Klassifizierung elektronischer Beweismittel für strafprozessuale Zwecke

Inauguraldissertation*

zur Erlangung der Doktorwürde der Juristischen Fakultät der Ruprecht-Karls-Universität Heidelberg

vorgelegt von

Claudia Warken

2018

Berichterstatter: Prof. Dr. Gerhard Dannecker
Prof. Dr. Kai Cornelius

* Es handelt sich um eine von der Juristischen Fakultät der Universität Heidelberg zum Druck freigegebene Dissertation.

Vorwort

Die Datenflut kommt!
Falsch. Sie ist längst da und hat ihren Scheitelpunkt noch lange nicht erreicht.

Geräte, die „smart“ sind, begleiten uns im privaten ebenso wie im öffentlichen Raum, und eine ganze Generation wird als „digital natives“ bezeichnet, um auszudrücken, dass die digitale Welt längst Realität geworden ist.
Alltag, Beruf, Freizeit – es gibt kaum noch einen Lebensbereich, der nicht in irgendeiner Form von der Digitalisierung erfasst wird, kaum eine Information, die sich nicht elektronisch darstellen lässt. Das Datenvolumen, das wir im Laufe des gesamten Jahres 2000 produzierten, wird heute im Laufe eines einzigen Tages erzeugt.[1]

Eine rechtsstaatliche Strafverfolgung braucht verlässliche Informationen. Sie ist zunehmend darauf angewiesen, diese in erheblichem Umfang und mit steigender Tendenz aus dem virtuellen Raum, aus dem Meer elektronischer Daten zu gewinnen, wobei nicht nur die Erlangung der Informationen unseren rechtsstaatlichen Prinzipien entsprechen muss, sondern auch ihre Verwertung.

Der Wandel von der analogen hin zur digitalisierten Gesellschaft findet in einer Geschwindigkeit statt, mit der kein Gesetzgeber Schritt halten kann. Als Folge fehlt es bereits jetzt in vielen Bereichen der digitalen Welt an Regelungen, die das, was unser Rechtssystem in der dinglichen Welt ausmacht, an die neuen Fragestellungen und Probleme anpassen.

---

1 Spehr, *Datenauswertung*, *Die Macht der Algorithmen*, FAZ.net, 16.09.2017

Dringende Fragen werden aktuell beispielsweise unter dem Stichwort „security by design“, im Datenschutzrecht oder im zivilrechtlichen Haftungsrecht diskutiert. Im Strafprozessrecht, das in besonderer Weise klare, eindeutige Normierungen verlangt, fallen die vorhandenen Regelungslücken noch erheblicher ins Gewicht. Ohne ihre Beseitigung kann eine handlungsfähige, effektive Strafverfolgung für die Zukunft nicht gewährleistet werden.

Es ist daher allerhöchste Zeit, die Lücken zu schließen.

Claudia Warken
Brüssel / Heidelberg, im Mai 2018

Inhaltsübersicht

Literaturverzeichnis

von Altenbockum, Jasper: *Bundestrojaner, Es bleibt nur der Lauschangriff,* FAZ.net, 23.06.2017, <http://www.faz.net/-gpg-8z3kv>, zuletzt aufgerufen am 04.01.2018

Apple Inc.: *Report on Government and Private Party Requests for Customer Information, January 1 – June 30, 2017,* <*https://images.apple.com/legal/privacy/transparency/requests-2017-H1-en.pdf*>, Download am 30.10.2017

Apple Inc.: *Report on Government and Private Party Requests for Customer Information, July 1 – December 31, 2016,* <https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf>, Download am 30.10.2017

ARD: *ARD/ZDF-Onlinestudie 2017: Neun von zehn Deutschen sind online. Bewegtbild insgesamt stagniert, während Streamingdienste zunehmen – im Vergleich zu klassischem Fernsehen jedoch eine geringe Rolle spielen*, Pressemitteilung vom 28.10.2017, <http://www.ard-zdf-onlinestudie.de/files/2017/Artikel/PM_ARD-ZDF-Onlinestudie_2017.pdf>, Download am 30.10.2017

ARD: *ARD/ZDF-Onlinestudie 2016: 84 Prozent der Deutschen sind online – mobile Geräte sowie Audios und Videos mit steigender Nutzung,* Pressemitteilung vom 12.10.2016, <http://www.ard-zdf-onlinestudie.de/fileadmin/Onlinestudie_2016/PM_ARD-ZDF-Onlinestudie_2016-final.pdf>, Download am 30.10.2017

Beer, Kristina: *Bundesländer bauen Ermittlungsbehörden gegen Cybercrime aus*, heise online, 30.08.2016, <https://www.heise.de/newsticker/meldung/Bundeslaender-bauen-Ermittlungsbehoerden-gegen-Cybercrime-aus-3307277.html>, zuletzt aufgerufen am 04.01.2018

Brodowski, Dominik: *Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick*, ZIS 2017, 11 ff., <http://zis-online.com/dat/artikel/2017_1_1080.pdf>, Download am 30.10.2017

Brodowski, Dominik: *Der „Grundsatz der Verfügbarkeit" von Daten zwischen Staat und Unternehmen,* ZIS 2012, 474 ff., <http://zis-online.com/dat/artikel/2012_8-9_703.pdf>, Download am 30.10.2017

Brodowski, Dominik: *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09,* JR 2009, 402 ff.

Bundesamt für Sicherheit in der Informationstechnik: *Verschlüsselung, Verschlüsselt kommunizieren*, <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/

verschluesselt_kommunizieren_node.html>, zuletzt aufgerufen am 04.01.2018

Bundesamt für Sicherheit in der Informationstechnik: *Das BSI, Historie*,<https://www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html>, zuletzt aufgerufen am 04.01.2018

Bundeskriminalamt, *Bericht zur Polizeilichen Kriminalstatistik 2016, Bericht der Innenministerkonferenz*, Version 1.0, April 2017, <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2016/pks2016ImkBericht.pdf__blob=publicationFile&v=5>, Download am 30.10.2017

Bundeskriminalamt: *Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft*, <https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zacEreichbarkeiten.pdf;jsessionid=299A99CED0B95B88F229B25D84FE595A.live0602?__blob=publicationFile&v=3>, Download am 30.10.2017

Bundesministerium des Inneren: *Cyber-Sicherheitsstrategie für Deutschland 2016*, <http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf>, Download am 30.10.2017

Bundesministerium für Wirtschaft und Technologie: *Strategiepapier zur Förderung der Einführung von IPv6*, November 2011, <http://www.post-und-telekommunikation.de/PuT/1Fundus/Dokumente/6._Nationaler_IT-Gipfel_2011_Muenchen/2011_6.IT-Gipfel_strategiepapier-zur-Foerderung_der-Einfuehrung-von-Ipv6-ag-2.pdf>, Download am 30.10.2017

Clopton, Zachary D.: *Data Institutionalism: A Reply to Andrew Woods*, Stanford Law Review Online, Volume 69, July 2016, S. 9 ff., <https://www.stanfordlawreview.org/online/data-institutionalism/>, zuletzt aufgerufen am 04.01.2018

Dettweiler, Marco: *Smart Home, Tausche Daten gegen Rabatt*, FAZ.net, 26.07.2017, <http://www.faz.net/aktuell/technik-motor/umwelt-technik/irobot-will-wohnungsplaene-von-roomba-nutzern-verkaufen-15122883.html>, zuletzt aufgerufen am 04.01.2018

Di Fabio, Udo: *Die algorithmische Person*, FAZ.net, 01.06.2016, http://www.faz.net/aktuell/feuilleton/debatten/der-staat-muss-die-grundrechte-in-der-digitalen-welt-sichern/>, zuletzt aufgerufen am 04.07.2016

Die Welt: *Das Land rüstet auf im Kampf gegen Cyber-Angriffe,* Presseartikel vom 16.08.2015, <https://www.welt.de/regionales/rheinland-pfalz-saarland/article145288691/das-Land-ruestet-auf-im-Kampf-gegen-Cyber-Angriffe. html>, zuletzt aufgerufen am 04.01.2018

Europäische Kommission: *Sicherheitsunion: Kommission erleichtert Zugang zu elektronischen Beweismitteln*, Pressemitteilung vom 17.04.2018, <http://europa.eu/rapid/press-release_IP-18-3343_de.htm>, zuletzt aufgerufen am 30.04.2018

Europäische Kommission: *Factsheet on EU resilience to cyber attacks*, September 2017, <http://europa.eu/rapid/attachment/IP-17-3193/en/Cyber security.en.pdf>, Download am 30.10.2017

Europäische Kommission: *Special Eurobarometer 464a, Cyber security, Factsheet Germany*, Juni 2017, <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79741>, Download am 30.10.2017

Europäische Kommission: *Report of the 17-18 January expert meeting*, 10.04.2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/e-evidence_report_17-18_january_2017_en.pdf>, Download am 30.10.2017

Europäische Kommission: *Report of the 28 February expert meeting*, 10.04.2017,<https://ec.europa.eu/hole-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/e-evidence_report_28_february_2017_en.pdf>, Download am 30.10.2017

Europäische Kommission: *Summary of Member States replies to the questionnaire on e-evidence*, 10.04.2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf>, Download am 30.10.2017

Europäische Kommission: *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 202/58/EG (Verordnung über die Privatsphäre und elektronische Kommunikation)*, 10.01.2017, <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42678>, Download am 30.10.2017

Europäische Kommission: *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 07.12.2016, ST 15072/1/16, <http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf>, Download am 30.10.2017

Europäische Kommission: *Europäisches Zentrum zur Bekämpfung der Cyberkriminalität: Eröffnung am 11. Januar*, Pressemitteilung vom 09.01.2013, <http://europa.eu/rapid/press-release_IP-13-13_de.htm>, zuletzt aufgerufen am 04.01.2018

Europäische Kommission / Hohe Vertreterin der Union für Aussen- und Sicherheitspolitik: *Gemeinsame Mitteilung an das Europäische Parlament und den Rat, Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen*, 13.09.2017, JOIN(2017) 450 final, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017_JC0450&from=EN>, Download am 30.10.2017

Europäische Kommission Services: *Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward,* 22.05.2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf>, Download am 30.10.2017

Europäische Kommission Services: *Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace,* 22.05.2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf>, Download am 30.10.2017

Europäischer Gerichtshof für Menschenrechte: *Factsheet – New technologies*, November 2017, <http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf>, Download am 06.12.2017

Europäischer Gerichtshof für Menschenrechte: *Factsheet – Personal Data Protection*, November 2017, <http://www.echr.coe.int/Documents/FS_Data_ENG.pdf>, Download am 06.12.2017

Europäischer Gerichtshof für Menschenrechte: *Guide on Article 8 of the European Convention on Human Rights*, 2017, <http://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>, Download am 06.12.2017

Europäisches Institut für Telekommunikationsnormen (ETSI): *Security*, Q2 2015, <http://www.etsi.org/images/files/ETSIClusterBrochures/clusters-security-Q22015.pdf>, Download am 30.10.2017

Europarat: *Chart of signatures and ratifications of Treaty 185, Status as of 04/01/2018*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>, zuletzt aufgerufen am 04.01.2018

Europarat: *Übereinkommen über Computerkriminalität*, 23.11.2001, Sammlung Europäischer Verträge - Nr. 185 („Cybercrime Convention"*)*, <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008157a>, Download am 30.10.2017

Europarat: *Explanatory Report to the Convention on Cybercrime,* 23.11.2001, *<http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>*, Download am 30.10.2017

Europarat, Budapest Convention on Cybercrime Convention Committee (T-CY): *Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY*, *Final report of the T-CY Cloud Evidence Group*, T-CY (2016)5, 16.09.2016, <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806 a495e>, Download am 30.10.2017

Europarat, Budapest Convention on Cybercrime Convention

Committee (T-CY): *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers*, *Background paper prepared by the T-CY Cloud Evidence Group*, T-CY (2016)2, 03.05.2016, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>, Download am 30.10.2017

European Informatics Data Exchange Framework for Courts and Evidence Project (EVIDENCE): *D9.2 Roadmap*, Version 1.5, <http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426.pdf>, Download am 30.10.2017

Europol: *Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade nat (GCN) to increase accountability online*, Pressemitteilung vom 17.10.2017, <https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online>, zuletzt aufgerufen am 04.01.2018

Europol: *The Internet Organized Crime Assessment (IOCTA) 2017,* <https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf>, Download am 30.10.2017

Europol: *EU forensic experts call for action on new cyber investigation standard*, Pressemitteilung vom 12.05.2017, <https://www.europol.europa.eu/newsroom/news/eu-forensic-experts-call-for-action-new-cyber-investigation-standard>, zuletzt aufgerufen am 04.01.2018

Europol: *Closing the online crime attribution gap: European law enforcement tackles Carrier-Grade NAT (CGN)*, Pressemitteilung vom 02.02.2017, <https://www.europol.europa.eu/newsroom/news/closing-online-crime-attribution-gap-european-law-enforcement-tackles-carrier-grade-nat-cgn>, zuletzt aufgerufen am 04.01.2018

Europol: *The Internet Organized Crime Assessment (IOCTA) 2016,* *<https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf*>, Download am 30.10.2017

Facebook: *Bericht über Regierungsanfragen, Deutschland, Juli 2016 – Dezember 2016,* *<https://govtrequests.facebook.com/country/Germany/2016-H2/*>, zuletzt aufgerufen am 04.01.2018

Generalstaatsanwaltschaft Bamberg: *Zentralstelle Cybercrime Bayern (ZCB)*, <https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/spezial_1.php>, zuletzt aufgerufen am 04.01.2018

Gercke, Björn: *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 ff.

Gollasch, Stefanie: *De Maizière will Ausspähen von Privat-Autos, Computern und Smart-TVs ermöglichen*, Redaktionsnetzwerk Deutschland, 30.11.2017, <http://www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-

Autos-Computern-und-Smart-Tvs-ermoeglichen>, zuletzt aufgerufen am 04.01.2018

Google: *Transparency Report, Requests for user information, Germany*, <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:DE&lu=user_requests_report_period>, zuletzt aufgerufen am 04.01.2018

Heller, Piotr: *Alexa, war es Mord?*, FAZ.net, 08.05.2017, <http://www.faz.net/aktuell/physik-mehr/internet-der-dinge-wenn-smarte-geraete-zu-zeugen-werden-15003037.html>, zuletzt aufgerufen am 04.01.2018

Hiéramente, Mayeul / **Pfister**, Andreas: *Datenerhebung beim Hersteller von Mobiltelefonen, Zum Erfordernis des Strukturwandels bei der strafprozessualen Datenerhebung*, StV 2017, 477 ff.

Hiéramente, Mayeul / **Fenina**, Patrick: *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 ff.

Hoffmann-Riem, Wolfgang: *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Band 130 (2005), 5 ff.

Hornung, Gerrit: *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 ff.

Internet and Jurisdiction Policy Network: *Data and Jurisdiction Policy Options, Cross Border Access to User Data*, November 2017 <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf>, Download am 04.01.2018

Jansen, Jonas: *Cyberattacken, Der große Kampf um das Internet*, FAZ.net, 02.03.2017, <http://www.faz.net/aktuell/wirtschaft/macht-im-internet/angst-vor-hackerangriffen-zur-bundestagswahl-2017-steigt-14901185.html?printPagedArticle=true#pageIndex_2>,zuletzt aufgerufen am 04.01.2018

Karg, Moritz: *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung*, DuD 2015, 85 ff.

Karpen, Ulrich: *Gesetzgebungslehre – neu evaluiert, Legistics – freshly evaluated*, 2. Aufl. 2008

Kaufmann, Annelie / **Tappert**, Wilhelm / **Vetter**, Joachim: *Kameras im Gericht: Mehr Transparenz oder Voyeurismus?*, Deutsche Richterzeitung 2017, 154 ff.

Kleinhans, Jan-Peter: *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?* , stiftung neue verantwortung e.V., Impulse, März 2015, <https://www.stiftung-nv.de/sites/default/files/impulse_die_cloud_im_rechtsfreien_raum.pdf>, Download am 30.10.2017

Koops, Bert-Jaap / **Goodwin**, Morag: *Cyberspace, the cloud and cross-border investigation – the limits and possibilities of international law*, Dezember 2014, <http://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf>, Download am 30.10.2017

Landeskriminalamt Baden-Württemberg: *Cybercrime und Digitale Spuren, Jahresbericht 2016,* <https://lka.polizei-bw.de/wp-content/uploads/sites/14/2017/06/Cybercrime_Digitale_Spuren.pdf>, Download am 30.10.2017

Landeskriminalamt Baden-Württemberg: *Cybercrime / Digitale Spuren, Jahresbericht 2015,* <*https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/pdf/2014_Cybercrime_und_Digitale_Spuren.pdf* >, Download am 30.10.2017

Landeskriminalamt Baden-Württemberg: *Die Geschichte des Landeskriminalamtes Baden-Württemberg im Überblick*, <http://www.polizei-bw.de/Dienststellen/LKA/Seiten/Historie.aspx>, zuletzt aufgerufen am 04.03.2017

Landeskriminalamt Nordrhein-Westfalen: *Das Cybercrime-Kompetenzzentrum beim LKA NRW (CCCC)*, <https://lka.polizei.nrw/artikel/das-cybercrime-kompetenzzentrum-beim-lka-nrw-cccc>, zuletzt aufgerufen am 04.01.2018

Leibholz / Rinck, *Grundgesetz*, 75. Lieferung 10.2017

Löwe / Rosenberg, *Die Strafprozessordnung und das Gerichtsverfassungsgesetz*, Großkommentar, 26. Aufl. 2014

Mason, Stephen: *Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now – But they Don`t Know it,* Computer and Telecommunications Law Review, 2017, Volume 23, Issue 8, S. 213 ff., <http://stephenmason.co.uk/wp-content/uploads/2017/12/Pages-from-2017_23_CTLR_issue_8_PrintNEWMASON.pdf>, Download am 04.01.2018

Mason, Stephen: *Draft Convention on Electronic Evidence*, Digital Evidence and Electronic Signature Law Review, Volume 13 (2016), Supplement, <http://journals.sas.ac.uk/deeslr/article/download/2321/2245>, Download am 30.10.2017

Meyer-Goßner, Lutz / **Schmitt**, Bertram: *Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmung*en, 59. Aufl. 2016

Microsoft Corporation: *Law Enforcement Requests Report, 2016 (Jul – Dec),* Landesauswahl Deutschland, <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/>, zuletzt aufgerufen am 04.01.2018

Microsoft Corporation: *Microsoft`s Cloud Infrastructure, Datacenters and Network Fact Sheet, June 2015,* <http://download.microsoft.com/

download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf>, Download am 30.10.2017

Osborne, Charlie: *FBI refuses to release Tor exploit details, evidence thrown out of court*, Zero Day online, 26.05.2016, <http://www.zdnet.com/article/fbi-refuses-to-release-tor-exploit-details-evidence-thrown-out-in-court/>, zuletzt aufgerufen am 04.01.2018

Payback GmbH: *Einwilligungserklärung seit September 2009,* <https://www.payback.de/pb/id/424758/>, zuletzt aufgerufen am 04.01.2018

Rat der Europäischen Union: *Schlussfolgerungen des Rates der Europäischen Union zur Verbesserung der Strafjustiz im Cyberspace*, 09.06.2016, ST 10007/16, <http://data.consilium.europa.eu/doc/document/ST-10007-2016-INIT/de/pdf>, Download am 30.10.2017

Reinbold, Fabian / **Schnack**, Thies*: US-Wahl und Daten-Ingenieure, Ich ganz allein habe Trump ins Amt gebracht*, Spiegel online, 06.12.2016, <http://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a1124439.html>, zuletzt aufgerufen am 04.01.2018

Schneider, Hans: *Gesetzgebung*, 1982

Sieber, Ulrich: *Straftaten und Strafverfolgung im Internet*, Verhandlungen des 69. Deutschen Juristentages, Band I, Gutachten Teil C, 2012

Sieber, Ulrich: *Kurzpräsentation des strafrechtlichen Gutachtens „Straftaten und Strafverfolgung im Internet“ auf dem 69. DJT in München am 19.9.2012*, <https://www.mpicc.de/files/pdf1/djt_sieber_kurzpraesentation.pdf>, Download am 30.10.2017

Sieber, Ulrich / **Neubert**, Carl-Wendelin: *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 ff.

Schwichtenberg, Simon: *Die "kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz*, DuD 2016, 605 ff.

Spehr, Michael: *Apps auf dem Smartphone, Gelinkt mit den Rechten*, FAZ.net, 30.11.2017, <http://www.faz.net/aktuell/technik-motor/digital/apps-auf-dem-smartphone-gelinkt-mit-den-rechten-15310250.html>, zuletzt aufgerufen am 04.01.2018

Spehr, Michael: *Datenauswertung, Die Macht der Algorithmen,* FAZ.net, 16.09.2017, <http://www.faz.net/aktuell/wirtschaft/me-convention-2017/daten-im-einzelhandel-macht-der-algorithmen-15191548.html>, zuletzt aufgerufen am 04.01.2018

Spehr, Michael: *Datenschutz und Privatsphäre, Jeder Schritt zählt, Was die Datenkraken interessiert: nicht die Adressen, nicht die E-Mails. Zu wissen, wie wir uns in der Welt bewegen, das ist die neue*

Digitalwährung der Netzspione, FAZ.net, 28.10.2016 <http://www.faz.net/aktuell/technik-motor/computer-internet/datenschutz-und-privatsphaere-jeder-schritt-zaehlt-14494871.html>, zuletzt aufgerufen am 04.01.2018

Svantesson, Dan Jerker B.: *Data categorisation and law enforcement access to cloud data*, 03.05.2017, <https://www.linkedin.com/pulse/data-categorisation-law-enforcement-access-cloud-svantesson?irgwc=1>, zuletzt aufgerufen am 30.10.2017

Svantesson, Dan Jerker B.: *Against ‚Against Data Exceptionalism'*, 2016 Masaryk University Journal of Law and Technology, S. 200 ff., <https://journals.muni.cz/mujlt/article/download/5925/6029>, Download am 30.10.2017

Svantesson, Dan Jerker B. / **van Zwieten**, Lodewijk: *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 ff.

Twitter Inc.: *Information requests, July to December, 2016*, <https://transparency.twitter.com/en/information-requests.html#information-requests-jul-dec-2016>, zuletzt aufgerufen am 04.01.2018

Vereinte Nationen, Vollversammlung: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22.05.2015, <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>, Download am 30.10.2017

Warken, Claudia: *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1, Beweissicherung im Zeitalter der digitalen Cloud*, NZWiSt 2017, 289 ff.

Warken, Claudia: *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, Beweisverwertung im Zeitalter der digitalen Cloud und daten-spezifische Regelungen in der StPO*, NZWiSt 2017, 329 ff.

Warken, Claudia: *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 3, Jenseits der StPO: Analogie, supra- und internationale Regelungen, praktische Lösungsansätze*, NZWiSt 2017, 417 ff.

Warken, Claudia: *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 4, Quo vadis, StPO? Warum es expliziter gesetzlicher Regelungen für den Umgang mit elektronischen Beweismitteln im Strafprozess bedarf und welche Rolle die Europäische Union dabei spielt*, NZWiSt 2017, 449 ff.

Wikipedia, Suchbegriff *ASCII*, <https://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Big Data*, <https://de.wikipedia.org/wiki/Big_Data>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Botnet*, <https://de.wikipedia.org/wiki/Botnet>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Cloud Computing*, <https://de.wikipedia.org/wiki/Cloud_Computing>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IMAP*, <https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IMEI,* <https://de.wikipedia.org/wiki/International_Mobile_Equipment_Identity>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IMSI*, <https://de.wikipedia.org/wiki/International_Mobile_Subscriber_Identity>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IMSI Catcher*, <https://de.wikipedia.org/wiki/IMSI-Catcher>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Internet*, <https://de.wikipedia.org/wiki/Internet>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IP-Telefonie*, <https://de.wikipedia.org/wiki/IP-Telefonie#Hintergrund-Technik_der_herk%C3%B6mmlichen_Telefonie>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *IPv4,* <https://de.wikipedia.org/wiki/IPv4>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Mobilfunk*, <https://de.wikipedia.org/wiki/Mobilfunk>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *OSI-Modell,* <https://de.wikipedia.org/wiki/OSI-Modell>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Quanteninformatik*, <https://de.wikipedia.org/wiki/Quanteninformatik#Quantencomputer>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Random Access Memory,* <https://de.wikipedia.org/wiki/Random-Access_Memory>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Ransomware*, <https://de.wikipedia.org/wiki/Ransomware>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *SIM Karte,* <https://de.wikipedia.org/wiki/SIM-Karte>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Smartphone*, <https://de.wikipedia.org/wiki/Smartphone>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Telefonbuch*, <https://de.wikipedia.org/wiki/

Telefonbuch>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *Vermittlungsstelle*, <https://de.wikipedia.org/wiki/Vermittlungsstelle #Manuelle_Vermittlung>, zuletzt aufgerufen am 04.01.2018

Wikipedia, Suchbegriff *World Wide Web, <https://de.wikipedia.org/wiki/World_Wide_Web*>, zuletzt aufgerufen am 04.01.2018

Wikipedia.org, Suchbegriff *Cambridge Analytica,* <https://en.wikipedia.org/wiki/Cambridge_Analytica>, zuletzt aufgerufen am 04.01.2018

Woods, Andrew K.: *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 ff., <https://www.stanfordlawreview. org/print/article/against-data-exceptionalism/>, zuletzt aufgerufen am 04.01.2018

Yahoo!: *Government Data Requests, July 1, 2016 – December 31, 2016*, <https://transparency.yahoo.com/government-data-requests?tid=35>, zuletzt aufgerufen am 04.01.2018

Ziegler, Peter-Michael: *Hessen forciert Bekämpfung der Internet-kriminalität*, heise online, 08.07.2008, <https://www.heise.de/newsticker/meldung/Hessen-forciert-Bekaempfung-der-Internetkriminalitaet-184888.html>, zuletzt aufgerufen am 04.01.2018

Zoetekouw, Mark: *Ignorantia Terrae Non Excusat, Discussion Paper for the Crossing Borders: Jurisdiction in Cyberspace conference – March 2016*,<https://www.eu2016.nl/binaries/eu2016/documenten/publicaties/2016/03/7/c---mzoetekouw---ignorantia-terrae-non-excusat---discussion-paper-for-the-crossing-borders---jurisdiction-in-cyberspace-conference-march-2016---final/c-mzoetekouw-ignorantia-terrae-non-excusat-discussion-paper-for-the-crossing-borders-jurisdiction-in-cyberspace-conference-march-2016-final.pdf>, Download am 26.02.2017

Abkürzungsverzeichnis

AAIS-Richtlinie
Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218 vom 14.08.2013, S. 8, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013L0040&rid=1>, Download am 30.10.2017

a.a.O.
am angegebenen Ort

Abs.
Absatz

a.F.
alte Fassung

AöR
Archiv des öffentlichen Rechts

Art.
Artikel

Bd.
Band

BDSG
Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 7 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097), <https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1509307940775>, Download am 30.10.2017

BGBl.
Bundesgesetzblatt

BGH
Bundesgerichtshof

BKA
Bundeskriminalamt

BSI
Bundesamt für Sicherheit in der Informationstechnik

BT-Ausschussdrucks.
Ausschussdrucksache des Bundestages

BT-Drucks.
Drucksache des Bundestages

BVerfG
Bundesverfassungsgericht

BVerfGE
Entscheidungen des Bundesverfassungsgerichts

ca.
circa

CR
Computer und Recht

Cybercrime-Konvention
Europarat: Übereinkommen über Computerkriminalität, 23.11.2001, Sammlung Europäischer Verträge - Nr. 185, <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008157a>, Download am 30.10.2017

DDoS
distributed denial of service

DJT
Deutscher Juristentag

DuD
Datenschutz und Datensicherheit

DS-GVO
Verordnung 2016/679/EU des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016, S. 1, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&qid=1493827937139&from=EN>, Download am 30.10.2017

DS-Richtlinie
Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002, S. 37, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=EN>, Download am 30.10.2017, geändert durch Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 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. L 105 vom 13.04.2006, S. 54, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0024&from=DE>, Download am 30.10.2017,

zuletzt geändert durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18.12.2009, S. 11, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0136&from=DE>, Download am 30.10.2017

DS-Richtlinie Strafjustiz
Richtlinie 2016/680/EU des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 04.05.2016, S. 89, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680&qid=1493828880226&from=EN>, Download am 30.10.2017

EEA-Richtlinie
Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 03.04.2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 01.05.2014, S. 1, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014L0041&from=DE>, Download am 30.10.2017

EGMR
Europäischer Gerichtshof für Menschenrechte

EMRK
Konvention zum Schutz der Menschenrechte und Grundfreiheiten in der Fassung der Bekanntmachung vom 17.05.2002 (BGBl. II S. 1054), <https://www.bgbl.de/xaver/bgbl/start.xavstartbk=Bundesanzeiger_BGBl&jumpTo=bgbl202s1054.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl202s1054.pdf%27%5D__1492948652923>, Download am 30.10.2017

etc.
et cetera, und so weiter

EU
Europäische Union

EuGH
Europäischer Gerichtshof

Europäische Beweisanordnung
Rahmenbeschluss 2008/978/JI des Rates vom 18.12.2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen, ABl. L 350 vom 29.12.2008, S. 72, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/

?uri=CELEX:32008F0978&rid=3>, Download am 30.10.2017

Europäische Sicherstellungsanordnung
Rahmenbeschluss 2003/577/JI des Rates vom 22.07.2003 über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union, ABl. EU L 196 vom 02.08.2003, S. 45, <http://eur-lex.europa. eu/legalcontent/DE/TXT/PDF/?uri=CELEX:32003F0577&rid=7>, Download am 30.10.2017

f.
folgend

ff.
fortfolgend

GG
Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 1 des Gesetzes vom 13.07.2017 (BGBl. I S. 2347), <http://www.gesetze-im-internet.de/gg/GG.pdf>, Download am 30.10.2017

GRC
Charta der Grundrechte der Europäischen Union, ABl. C 364 vom 18.12.2000, S. 1, <http://www.europarl.europa.eu/charter/pdf/text_de.pdf>, Download am 30.10.2017

HS
Halbsatz

IaaS
Infrastructure as a service, Infrastrukturbereitsstellung als Dienstleistung

IT
Informationstechnik

i.V.m.
in Verbindung mit

JKomG
Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22.03.2005, BGBl. I S. 837,<http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl105s0837.pdf>, Download am 30.10.2017

JR
Juristische Rundschau

LG
Landgericht

lit.
littera, Buchstabe

LKA
Landeskriminalamt

m.w.N.
mit weiteren Nachweisen

Nr.
Nummer

NZWiSt
Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht

PaaS
Platform as a service, Plattformbereitstellung als Dienstleistung

PKS
Polizeiliche Kriminalstatistik

OLG
Oberlandesgericht

OVG
Oberverwaltungsgericht

Rechtshilfeübereinkommen von 2000
Übereinkommen vom 29.05.2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedsstaaten der Europäischen Union, ABl. EG C 197 vom 12.07.2000, S. 3, <eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32000F0712(02)&>, Download am 30.10.2017

s.
siehe

S.
Satz, Seite

SaaS
Software as a service, Softwarebereitstellung als Dienstleistung

StraFo
Strafverteidiger Forum

StGB
Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 1 des Gesetzes vom 30.09.2017 (BGBl. I S. 3532), <http://www.gesetze-im-internet.de/stgb/StGB.pdf>, Download am 30.10.2017

StPO
Strafprozessordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 1 des

Gesetzes vom 27.08.2017 (BGBl. I S. 3295), <http://www.gesetze-im-internet.de/stpo/StPO.pdf>, Download am 30.10.2017

StV
Strafverteidiger

TKG
Telekommunikationsgesetz vom 25.07.1996 (BGBl. I S. 1120) in der Fassung der Bekanntmachung vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 1 des Gesetzes vom 27.06.2017 (BGBl. I S. 1963), <http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf>, Download am 30.10.2017

TKÜ
Telekommunikationsüberwachung

TMG
Telemediengesetz vom 26.02.2007 (BGBl. I S. 179, 251), zuletzt geändert durch Art. 1 des Gesetzes vom 28.09.2017 (BGBl. I S. 3530), <http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf>, Download am 30.10.2017

TOR-Netzwerk
The Onion Router, Anonymisierungsnetzwerk

vgl.
vergleiche

VPN
Virtual Private Network, virtuelles privates Kommunikationsnetz

Ziff.
Ziffer

ZIS
Zeitschrift für Internationale Strafrechtsdogmatik

A. Problemstellung und Ziel der Arbeit, Begrenzung des Untersuchungsgegenstandes und Methodik

I. Problemstellung

1. Zunehmende Bedeutung elektronischer Daten als Beweismittel für die Strafverfolgung[2]

Die Bedeutung elektronischer Daten als Beweismittel für die Strafverfolgung steigt stetig. Dies ist zum einen darauf zurückzuführen, dass sich mit dem technischen Fortschritt ganz neue Arten an Straftaten ergeben, deren Begehung zwingend in der virtuellen Umgebung des Internets oder zumindest innerhalb eines Informationssystems[3] erfolgt.[4] Zu denken ist in diesem Zusammenhang etwa an die Straftatbestände der Datenveränderung (§ 303a StGB) und der Computersabotage (§ 303b StGB), den im Jahr 2007 in das StGB eingefügten Straftatbestand des Abfangens von Daten (§ 202b StGB), zudem an den Ende 2015 neu eingeführten Straftatbestand der Datenhehlerei (§ 202d StGB).[5] Bei diesen Delikten stehen Angriffe gegen die Integrität, die Vertraulichkeit und die Verfügbarkeit von

---

2 Die unter diesem Punkt folgende Darstellung basiert im Wesentlichen auf der Veröffentlichung Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 1, NZWiSt 2017, 289 (289 ff.).

3 In Art. 2 a) der AAIS-Richtlinie wird der Begriff des Informationssystems definiert als „eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten“, wobei gemäß Art. 2 b) Computerdaten „jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann“ sind.
Vereinfacht dargestellt erfasst die Definition somit sowohl Computer als Einzelgeräte als auch, soweit sie miteinander in Verbindung stehen, alle Geräte in ihrer Gesamtheit und Computerdaten als solche.

4 Europol, *IOCTA 2017,* S. 18, spricht in diesem Zusammenhang von „cyber-dependent crimes“.

5 Aktuell wird zudem die Einführung des Straftatbestandes des Digitalen Hausfriedensbruches diskutiert, zu dem der Bundesrat durch Beschluss vom 23.09.2016 dem Deutschen Bundestag einen entsprechenden Gesetzesentwurf vorgelegt hat (BT-Drucks. 18/10182).

Informationssystemen im Mittelpunkt.[6]

Zum anderen führt die weite Verbreitung mobiler elektronischer Endnutzergeräte zu Daten, aus denen zum Beispiel unmittelbar auf einen bestimmten Aufenthaltsort oder eine bestimmte Tätigkeit etwa zur Tatzeit geschlossen werden kann: Mobilfunkgeräte senden selbst im Stand-by Modus permanent elektronische Signale, sogenannte Signalisierungsdaten, aus, um ihren Standort im Funknetz mitzuteilen. Dadurch können sie bei einem eingehenden Anruf möglichst schnell angesprochen werden. Daneben gibt es insbesondere für Smartphones eine Vielzahl von Programmen, die, ohne dass der Nutzer hiervon überhaupt Kenntnis erlangt, permanent aktuelle Informationen versenden. Bei Facebook beispielsweise ist standardmäßig vorgesehen, dass das einmal auf dem Gerät installierte Programm gleichsam im Minutentakt Standortdaten an das Unternehmen sendet.[7] Auch Google sieht vor, dass standardmäßig jedem Programm, das über den Google Playstore heruntergeladen und installiert wird, ein uneingeschränkter Internetzugang eingeräumt wird, sodass das Programm im Hintergrund und unbemerkt ständig Daten senden und empfangen kann.[8] Ein denkwürdiges Beispiel hierfür ist die Android-Taschenlampen-App, die 50 Millionen Mal auf Smartphones heruntergeladen wurde, bevor zufällig entdeckt wurde, dass sie – unter massivem Verstoß gegen die datenschutzrechtlichen Vorschriften - nicht nur als virtueller Licht-schalter fungierte, sondern sämtliche verfügbaren Daten über Nutzer und Gerät, vom Aufenthaltsort bis zur Seriennummer, an den Hersteller der Software zum Verkauf an Dritte übermittelte.[9]

Schließlich ist festzustellen, dass eine zunehmende Anzahl von klassischen Straftaten unter Zuhilfenahme des Tatwerkzeugs Internet verübt wird, sich also nicht nur die Vorbereitung oder Absprache einer

6 Sieber, *Gutachten zum 69. DJT*, S. 18; ihre Bedeutung ergibt sich anschaulich daraus, dass seit dem großen Hackerangriff im November 2016, bei dem aufgrund des Einsatzes der Botnet-Software „Mirai“ über 900.000 Kundenanschlüsse der Deutschen Telekom zeitweilig funktionsunfähig gesetzt wurden, die Gefahr vergleichbarer sogenannter Distributed-Denial-of-Service (DDoS) – Angriffe weiter gestiegen ist (vgl. Europol, *IOCTA 2017,* S. 26 f.).

7 Spehr, *Jeder Schritt zählt*.

8 Spehr, *Jeder Schritt zählt*.

9 Spehr, *Gelinkt mit den Rechten.*

solchen, sondern auch deren Begehung in den virtuellen Raum verschiebt[10] - beispielsweise beim bargeldlosen Zahlungsbetrug, bei der Unterstützung jeglicher Art von Internetstraftaten durch das Bereitstellen von Hilfsmitteln wie Schadprogrammen und entsprechenden online Diensten („crime as a service“)[11] oder beim Einsatz von Ransomware[12] zur Begehung einer Erpressungstat.[13]

Dies alles führt zu neuen Herausforderungen für die Strafverfolgungsbehörden, wie sie sich beispielsweise bei dem „Wannacry“-Ransomware-Angriff am 12.05.2017 gezeigt haben, dem binnen Stunden knapp 300.000 Betroffene in über 150 Ländern zum Opfer fielen.[14]

Umgekehrt eröffnet die Verfügbarkeit von Informationen im Netz und die kontinuierlich zunehmende Leistungsfähigkeit des Internets neue Überwachungs- und Kontrollmöglichkeiten, die die Verfolgung von Straftaten erheblich verbessern können.[15]

---

10 Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (242); Karg, *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung,* DuD 2015, 85; laut BKA, *Bericht zur Polizeilichen Kriminalstatistik 2016*, S. 15, stellten die Betrugsdelikte mit 72,5% aller Delikte, die unter Nutzung des Tatmittels Internet im Jahr 2016 begangen wurden, den Schwerpunkt dar.

11 Ausführlich dazu: Europol, *IOCTA 2017*, S. 50, 58 f.; laut Europol, *IOCTA 2017*, S. 27, kann etwa die Rechnerkapazität eines Botnetzes für einen 5-minütigen DDoS-Angriff auf die Server eines großen online-Händlers für ca. 5 US$ im Internet „gemietet“ werden.

12 Laut Wikipedia, Suchbegriff *Ransomware*, handelt es sich bei Ransomware um „Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden private Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf sie wird verhindert, um für die Entschlüsselung oder Freigabe ein ‚Lösegeld‘ zu fordern“, wobei das Lösegeld fast ausschließlich in elektronischer Währung wie Bitcoins verlangt wird (zu Letzterem: Europol, *IOCTA 2016,* S. 17). Vertiefend zu Ransomware-Angriffen: Europol, *IOCTA 2017,* S. 19 f.; LKA Baden-Württemberg, *Cybercrime und Digitale Spuren, Jahresbericht 2016*, S. 13 f.

13 Zu den genannten und weiteren Beispielen vgl. Europol, *IOCTA 2016,* S. 7. Sieber, *Gutachten zum 69. DJT*, S. 26, m.w.N., sieht den Schwerpunkt bei solchen Delikten, die unter den Begriffen Identitätsdiebstahl und Identitätsmissbrauch zusammengefasst werden.

14 Europol, *IOCTA 2017,* S. 19.

15 DS-Richtlinie Strafjustiz, Begründung Ziff. 3; Sieber, *Gutachten zum 69. DJT*, S. 10.

Insgesamt spielt somit die Auswertung elektronischer Daten für die Verfolgung sämtlicher Straftaten bereits heute eine große Rolle.[16] In der Praxis ist in den letzten Jahren europaweit zudem ein dramatischer Anstieg der Ermittlungs- und Anklagefälle aus dem Bereich der Internetkriminalität zu beobachten.[17] Spätestens seit der Veröffentlichung der sogenannten „NSA-Affäre“[18] im Sommer 2013 hat nicht nur die Presse „Cyber“ und die Gefahren des Internets als Topthemen für sich entdeckt, auch die Politik reagiert auf allen Ebenen mit Sicherheitsgesetzen[19] und Gründungen von operativen Spezialbehörden auf Landesebene[20] und Bundesebene[21].

16 Vgl. Rat der Europäischen Union, *Schlussfolgerungen vom 09.06.2016*, S. 1; Europäische Kommission, *Progress Report,* 07.12.2016, S. 1; EVIDENCE Project, *Roadmap*, S. 12; Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 17.

17 Europol, *IOCTA 2016*, S. 7; Zoetekouw, *Ignorantia Terrae Non Excusat,* S. 2. Laut Europäische Kommission, *Factsheet on EU resilience to cyber attacks*, September 2017, erfolgten 2016 in der EU täglich durchschnittlich über 4.000 Ransomware-Angriffe und in manchen Mitgliedstaaten stammen bereits die Hälfte aller Straftaten aus dem Bereich der Internetkriminalität.

18 Aus der Veröffentlichung geheimer Dokumente durch den ehemaligen Geheimdienstmitarbeiter Edward Snowden wurde publik, dass US-amerikanische und britische Geheimdienste umfänglich und weltweit die Telekommunikation und Internetnutzung - auch die deutscher Spitzenpolitiker - überwachten.

19 Etwa mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 24.07.2015, BGBl. I S. 1324.

20 Laut BKA, *Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft,* haben mittlerweile alle Bundesländer „Zentrale Ansprechstellen Cybercrime“ eingerichtet, die meistens beim jeweiligen Landeskriminalamt angesiedelt sind.
Vorreiter war laut Beer, *Bundesländer bauen Ermittlungsbehörden gegen Cybercrime aus*, und Ziegler, *Hessen forciert Bekämpfung der Internetkriminalität*, Hessen Ende 2007, gefolgt von beispielsweise Nordrhein-Westfalen 2011 (s. LKA Nordrhein-Westfalen, *Das Cybercrime-Kompetenzzentrum beim LKA NRW (CCCC)*), Baden-Württemberg 2013 (s. LKA Baden-Württemberg, *Die Geschichte des Landeskriminalamtes Baden-Württemberg im Überblick*), Rheinland-Pfalz 2014 (s. Die Welt, *Das Land rüstet auf im Kampf gegen Cyber-Angriffe*) und Bayern 2015 (s. Generalstaatsanwaltschaft Bamberg, *Zentralstelle Cybercrime Bayern (ZCB)*).

21 Etwa der German Competence Centre against Cyber Crime e.V. (G4C) mit Tätigkeitsaufnahme zum 01.01.2014, das Nationale Cyberabwehrzentrum in Bonn mit Tätigkeitsaufnahme am 01.04.2011, oder die Allianz für Cyber-Sicherheit (ACS), eine Kooperation des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) und verschiedener Landeskriminalämter mit Tätigkeitsaufnahme am 08.11.2012 (BSI, *Das BSI, Historie*).

Auch auf EU-Ebene[22] wird nach Strategien gesucht, um den Problemen Herr zu werden,[23] während die Wirtschaft „aufrüstet“ und Unternehmen, die professionellen Schutz vor Cyberangriffen anbieten, boomen[24]. Potentiell strafbare Handlungen wie der Einsatz von Ransomware, Wahlmanipulationen durch digitale Einflussnahme und computergesteuerte Angriffe auf wichtige Infrastruktureinrichtungen sind Themen, die erst seit einigen Monaten überhaupt in das Bewusstsein der Öffentlichkeit treten.

Mit der fortschreitenden Digitalisierung des Alltags in allen Lebensbereichen - Stichworte: selbstfahrende Fahrzeuge, medizinische Hilfsgeräte, Internet der Dinge etc. - und der jedem digitalen Gerät mit potentiellem Internetanschluss immanenten Manipulationsmöglichkeit von außen werden zunehmend auch Körperverletzungs- und Tötungsdelikte in den Blickpunkt rücken, deren eigentlicher Handlungsort nicht mehr mit dem Erfolgseintrittsort identisch sein wird.[25] Gleichzeitig steigt mit der zunehmenden Nutzung des Internets[26]

22 Europäisches Zentrum zur Bekämpfung der Cyberkriminalität, (englisch: European Cyber Crime Centre (EC3)), mit Tätigkeitsaufnahme am 11.01.2013 (Europäische Kommission, *Pressemitteilung vom 09.01.2013*).

23 Beispielsweise mit der am 09.11.2016 von der Bundesregierung verabschiedeten Cyber-Sicherheitsstrategie (Bundesministerium des Inneren, *Cyber-Sicherheitsstrategie für Deutschland 2016*).
Mit dem speziellen Problem der Hass- und Hetzkommentare im Internet beschäftigt sich das am 01.10.2017 in Kraft getretene Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 01.09.2017, BGBl. I S. 3352, durch das Facebook, Google und alle anderen großen Social-Media-Betreiber verpflichtet werden, entsprechende Kommentare schneller auf ihren Seiten zu löschen; zur weiteren Diskussion über eine solche gesetzliche Pflicht vgl. Kaufmann / Tappert / Vetter, *Kameras im Gericht: Mehr Transparenz oder Voyeurismus?*, Deutsche Richterzeitung 2017, 154 (154 f.); zur Diskussion über weitergehende Mitwirkungspflichten insbesondere der Industrie in Form der Offenlegung von Programmier-protokollen vgl. Gollasch, *De Maizière will Ausspähen von Privat-Autos, Computern und Smart-TVs ermöglichen*.

24 So hat sich beispielsweise der Aktienkurs der Symantec Corporation, einem weltweit führenden Anbieter speziell von Internetsicherheits-software, im Zeitraum vom 01.05.2014 bis 30.04.2017 von 14,36 € auf 29,30 € mehr als verdoppelt (Quelle: boerse.de, Aufruf am 01.05.2017, 12:07 Uhr).

25 Gedacht sei in diesem Zusammenhang beispielsweise an Manipulationen einer automatisierten Medikamentendosierung, wie sie heute in Krankenhäusern zunehmend üblich ist, oder an ferngesteuerte Eingriffe in die Steuerungstechnik eines autonom fahrenden Fahrzeugs.

26 Gemäß Europäische Kommission, *Sonderausgabe des Eurobarometers 464a (Factsheet Germany),* nutzen im Juni 2017 74% aller befragten Deutschen täglich das Internet, wobei der Computer (mit 89%) und das Smartphone (mit 79%) die meist genutzten Geräte für den Internet-

und der damit einhergehenden Vernetzung informationstechnischer Systeme deren Bedeutung für die Persönlichkeitsentfaltung des Einzelnen,[27] die mehr und mehr im und mit Mitteln des virtuellen Raumes stattfindet.

2. Fehlende konzeptionelle Einbindung des Beweismittels in der StPO

Der Bedeutung elektronischer Daten als potentielle strafprozessuale Beweismittel stehen der sehr begrenzte Umfang ihrer gesetzlichen Regelung und die geringe Regelungsdichte gegenüber. Bislang fehlt es an einer konzeptionellen Einbindung dieser Informationsträger im Strafverfahrensrecht; anstelle grundlegender, umfassender Normierungen sind dort lediglich punktuelle Einzelfallregelungen zu finden.
Diesbezüglich zeigt sich in den letzten Jahren ein verstärktes Problembewusstsein in der Rechtspolitik und Wissenschaft, das bislang nur zu vereinzelten Lückenschließungen geführt hat. Zudem lässt die aktuelle Entwicklung darauf schließen, dass mit weiteren Gesetzesinitiativen in diesem Bereich zu rechnen ist.

Parallel dazu ist die Entstehung eines Problembewusstseins auf Seiten der Prozessbeteiligten, namentlich der Strafgerichte, der Staatsanwaltschaft und der Strafverteidiger zu beobachten. Die Erlangung elektronischer Beweismittel, ihr Aussagegehalt und dessen Verifizierbarkeit werden zunehmend hinterfragt und bedürfen nicht selten der Einschaltung versierter Sachverständiger.

Ein weiteres Hauptproblem neben der Regelungsfragmentierung ist die derzeit vorherrschende Einteilung elektronischer Daten in Bestands-, Verkehrs- und Inhaltsdaten. Sie ist zum einen beschränkt auf Kommunikationsdaten und vernachlässigt dadurch den zunehmend wichtig werdenden Bereich aller sonstigen elektronischen Daten. Zum anderen entspricht diese Einteilung nicht (mehr) den verfassungs-

zugang waren. Laut ARD, *ARD/ZDF-Onlinestudie 2017*, verbringen derzeit rund 72% der deutschsprachigen Bevölkerung über 14 Jahre täglich im Schnitt knapp 2,5 Stunden online.

27 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 172 ff.; zustimmend Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“,* CR 2008, 299 (302).

rechtlichen Vorgaben, die an die Unterscheidung von Regelungsobjekten (hier: elektronische Daten) zu stellen sind. Schließlich zeigt sich ihre beschränkte Praxistauglichkeit dort, wo die bisherigen Annahmen auf ein dem technischen Fortschritt geschuldetes geändertes Kommunikationsverhalten der Internetnutzer und ein geändertes Dateninteresse der Dienstleister treffen.

Die herkömmliche Einteilung elektronischer Kommunikationsdaten, die sich auch innerhalb der EU-Mitgliedstaaten durchgesetzt hat, wird daher in Deutschland, aber auch auf EU-Ebene mehr und mehr in Frage gestellt und ihre Ablösung diskutiert.[28] Dabei gehen die Meinungen darüber auseinander, ob Ergänzungen des bisherigen Modells genügen oder ob ein völliger Neuansatz erforderlich ist.[29]

Es tut sich etwas, rechtlich und tatsächlich, im Hinblick auf elektronische Daten im Strafprozess und insbesondere im Hinblick auf ihre Kategorisierung für strafprozessuale Zwecke, wobei die Richtung, in die sich die Diskussion entwickeln wird, noch offen ist.

28 Vgl. Europäische Kommission Services, *Technical Document*, S. 18 f., unter Hinweis auf entsprechende Erkenntnisse aufgrund des unionsweit durchgeführten Expertenprozess zur Frage des grenzüberschreitenden Zugriffs auf elektronische Beweismittel im Strafermittlungsverfahren; Svantesson, *Data categorisation and law enforcement access to cloud data*.

29 Für eine Erweiterung des bisherigen Modells wohl: Europäische Kommission Services, *Technical Document*, S. 18 f.; für eine Neukonzeption u.a. Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679).

II. Ausgangspunkte und Ziel der Arbeit

1. Anforderungen an die Gesetzgebung

Jegliches staatliche Handeln tangiert in unterschiedlichem Ausmaß Rechte und Interessen des Einzelnen, wobei Maßnahmen im strafrechtlichen Ermittlungsverfahren generell jedenfalls das Grundrecht der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG des Betroffenen beeinträchtigen. Daneben sind häufig weitere Grundrechte wie das des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 Abs. 1 GG), der Freizügigkeit (Art. 11 Abs. 1 GG), der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG), des Eigentumsschutzes (Art. 14 Abs. 1 GG) sowie des Gleichheitsgrundsatzes (Art. 3 Abs. 1 GG) betroffen. Für jede strafprozessuale Handlung, die Grundrechte des Einzelnen beeinträchtigt, bedarf es einer expliziten Ermächtigungsgrundlage im Sinne eines förmlichen Gesetzes.[30] Dieses wiederum stellt im Idealfall das kodifizierte Ergebnis der abstrakten Abwägung widerstreitender Rechte und Interessen dar; im Strafrecht betrifft dies namentlich die grundrechtlich abgesicherten Positionen des Verdächtigen, die des Opfers und das Strafverfolgungsinteresse des Staates beziehungsweise der Allgemeinheit.[31]

Das vorrangige Ziel jeder strafprozessualen Ermittlungshandlung ist die Erlangung und Verwertung von be- und entlastenden Beweismitteln, die letztlich in einem gerichtlichen Strafprozess von Bedeutung sein können, sofern sie in ihrer Gesamtheit nicht bereits zuvor die Einstellung des Verfahrens rechtfertigen. Dabei unterliegen alle in der StPO normierten Eingriffsbefugnisse der verfassungsrechtlichen Anforderung, die in den Grundrechten konkretisierten Wertentscheidungen und die fundamentalen Ordnungsprinzipien des Grundgesetzes aufzugreifen und widerzuspiegeln;[32] die Gestaltungsfreiheit des Gesetzgebers besteht nur im Rahmen dieser verfassungs-

30 Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 138; Schneider, *Gesetzgebung*, S. 16; vgl. auch Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (8, 50).

31 Vgl. Meyer-Goßner / Schmitt, *StPO*, Einl Rn. 18.

32 Vgl. Hesselberger, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 34 f. (zitiert nach juris), m.w.N.

rechtlichen Vorgaben.[33]

Beispielsweise treten die Rechte des Opfers und der Allgemeinheit bei den persönlichen Beweismitteln (Zeugen- und Beschuldigtenvernehmung) nach der abstrakten verfassungsrechtlichen Wertung in allen Fällen hinter dem „nemo tenetur“-Grundsatz zurück: Weder der Verdächtige noch der Zeuge ist verpflichtet, zur Sache auszusagen, wenn er sich damit in die Gefahr begibt, selbst strafrechtlich verfolgt zu werden (§§ 136 Abs. 1 S. 2, 55 Abs. 1 StPO).[34]

Auch bei den Normen, die die Erlangung und Verwertung dinglicher Beweismittel zum Gegenstand haben, handelt es sich um Abwägungsergebnisse, in denen besondere Grundrechtsbeeinträchtigungen besondere Rechtsfolgen nach sich ziehen. Dies wird bei „Gegenständen“ deutlich, deren Erlangung sich im Allgemeinen nach § 94 StPO richtet. Aus verfassungsrechtlicher Sicht besonders sensible Gegenstände erfahren jedoch eine strafprozessuale Sonderbehandlung. Das gilt beispielsweise für Postsendungen (§ 99 StPO) ebenso wie für Mobilfunkendgeräte (§ 100i StPO), für Gegenstände, die den Schwangerschaftsabbruch einer Patientin betreffen (§ 108 Abs. 2 StPO), sowie für bestimmte Räume (§§ 102 f. StPO).

Selbst das gesprochene Wort ist de lege lata nicht gleich gesprochenes Wort: Die grundgesetzliche Werteordnung begründet die Differenzierung in den §§ 100a, 100c und 100f StPO, je nachdem, ob das gesprochene Wort im Rahmen einer Telekommunikation, innerhalb einer Wohnung oder außerhalb einer Wohnung abgehört wird.

Ein letztes, eindrückliches Beispiel verfassungsrechtlicher Wertungsvorgaben betrifft die Erlangung und Verwertung biometrischer Daten des Beschuldigten. Hier wird in der StPO nicht nur vom Wortlaut,

33 Hesselberger, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 34 (zitiert nach juris), m.w.N.; näher zum Entscheidungsspielraum des Gesetzgebers: Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 41.

34 Diese Gefahr ist bei der Beschuldigtenvernehmung hinsichtlich der konkret in Frage stehenden Tat evident und immanent, sodass sie für den Beschuldigten in § 136 Abs. 1 S. 2 StPO – anders als für den Zeugen in § 55 Abs. 1 StPO - nicht ausdrücklich erwähnt wird.

sondern insbesondere hinsichtlich der behördlichen Handlungsbefugnisse unterschieden zwischen der Lichtbildanfertigung, der Abnahme von Fingerabdrücken und der Durchführung von Messungen (§ 81b StPO), der körperlichen Untersuchung (§ 81a Abs. 1 StPO) sowie der Entnahme von Blutproben oder sonstigen Körperzellen (§ 81a Abs. 3 StPO).

Allen aufgezählten Normierungen ist gemein, dass sie das Ergebnis einer gesetzgeberischen Abwägung sind, die ihrerseits auf für den Gesetzgeber verbindlichen verfassungsrechtlichen Wertungsvorgaben beruht. Letztere beziehen sich einerseits auf die grundrechtsspezifischen Besonderheiten des jeweiligen Beweismittels, die sich vorrangig aus den Grundrechten des von der Ermittlungshandlung unmittelbar Betroffenen ergeben – Brief, Post- und Fernmeldegeheimnis, Recht auf körperliche Unversehrtheit etc. -, und andererseits auf die allgemeinen Rechtsgrundsätze, die auf alle Beweismittel Anwendung finden und nicht nur auf den unmittelbar Betroffenen, sondern auch auf die allgemeinen Opferrechte beziehungsweise Rechte und Interessen der Allgemeinheit Bezug nehmen. Solche allgemeinen Rechtsgrundsätze beinhalten etwa das Gebot der Sachgemäßheit, der Systemgemäßheit, der Folgerichtigkeit und der Angemessenheit.[35] Das Bundesverfassungsgericht fordert für die Gültigkeit der jeweiligen gesetzlichen Regelung insbesondere im Strafrecht zudem die Berücksichtigung der allgemeinen Grundsätze der Gleichheit, Verhältnismäßigkeit, Bestimmtheit und Klarheit.[36]

---

35 Vgl. Schneider, *Gesetzgebung*, S. 33 ff., m.w.N., wobei sich die Sachgemäßheit darauf beziehen soll, dass die gesetzliche Regelung nicht im Widerspruch zu elementaren Vorstellungen von Recht und Gesetz stehen dürfe, die Systemgemäßheit das Gebot der Einheit der Rechtsordnung postuliere, die Folgerichtigkeit insbesondere bei der „Gesetzgebung in Raten“ zu berücksichtigen sei und die Angemessenheit die Erforderlichkeit der Abwägung widerstreitender Interessen betone.

36 Vgl. Schneider, *Gesetzgebung*, S. 38 ff., m.w.N., wonach es an der Gleichheit fehle, „wenn ein einleuchtender (plausibler) Grund für eine gesetzliche Differenzierung fehlt und auch dem nachdenklichen Richter nicht einfällt“; der Gleichheitsgrundsatz verbiete, vergleichbare Sachverhalte ohne sachlich vertretbaren Grund verschieden zu behandeln, während die Verhältnismäßigkeit auf das Mittel-Zweck-Verhältnis abstelle und das Erfordernis der Bestimmtheit und Klarheit darauf abziele, dass der Regelungsgehalt vom betroffenen Kreis verstanden und von den Verwaltungsbehörden und Gerichten ohne Willkür gehandhabt werden könne.
Zu Klarheit, Bestimmtheit, Verständlichkeit, Widerspruchsfreiheit,

Die Berücksichtigung der spezifischen Besonderheiten eines bestimmten Regelungsobjektes darf nicht dazu führen, dass Einzelfallregelungen entstehen, die gegen das dem allgemeinen Gleichheitssatz entnommene Willkürverbot[37] verstoßen und daher per definitionem nicht die Anforderungen an ein förmliches Gesetz im Sinne des Art. 19 Abs. 1 S. 1 GG erfüllen.[38] Rechtssicherheit durch Vorhersehbarkeit der rechtlichen Handlungsfolgen, die Kontrollierbarkeit der Gesetzesanwendung und die Gleichheit des Rechts können nur durch die Allgemeinheit des gesetzlichen Inhaltes gewährleistet werden.[39] In der Gesetzgebungslehre wird wie folgt formuliert: „Die Allgemeinheit [einer Gesetzgebung, ohne die sie keine solche wäre] kommt in der abstrakten, auf typische Grundmerkmale abgestellten Fassung des Gesetzes zum Ausdruck. Es werden Kategorien von Personen, Reihen von Fällen und Lagen geordnet.“ Und weiter: „Generalität des Gesetzes ist nicht im absoluten Sinn zu verstehen; es genügt, daß innerhalb eines nach typischen Kennzeichen bestimmten Kreises von Personen oder Sachverhalten, alle Fälle erfasst werden.“[40]

Die Herausforderung liegt darin, durch die Bestimmung geeigneter Regelungsobjekt-Kategorien die richtige Balance für das Zusammenspiel des allgemeinen Gleichheitsgrundsatzes und der rechtlichen Besonderheit der jeweiligen Kategorie im verfassungsrechtlichen Wertekanon zu finden. Die Unterscheidung zwischen einer unzulässigen Einzelfallregelung und einem den Gleichheitsgrundsatz beachtenden Gesetz erfolgt durch die Prüfung, „ob das Gesetz vergleichbare Fälle nicht trifft und nicht treffen will, die

---

Folgerichtigkeit, Vollständigkeit und Systemgemäßheit als maßgebliche Kriterien eines ‚guten Gesetzes‘ im Sinne der modernen Gesetzgebungslehre vgl. Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 37 ff.; ähnlich Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (68), der zur Legitimationssicherung staatlicher Herrschaft die Berücksichtigung unter anderem folgender Faktoren empfiehlt: Input-Richtigkeit (Verarbeitung aller rechtserheblichen Tatsachen und Wertungen), Organisationsrichtigkeit (insbesondere Zuständigkeit), Verfahrensrichtigkeit, Kohärenz und Erfolgskontrolle.

37 Hesselberger, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 38 (zitiert nach juris), m.w.N.

38 Schneider, *Gesetzgebung*, S. 16, 21; Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 13, 199.

39 Schneider, *Gesetzgebung*, S. 21 f.

40 Schneider, *Gesetzgebung*, S. 22.

vernünftigerweise in gleicher Weise erfasst werden sollten“,[41] oder, mit den Worten des Bundesverfassungsgerichts: ob wesentliches Gleiches ohne sachlichen Grund ungleich beziehungsweise wesentliches Ungleiches ohne sachlichen Grund gleich behandelt wird.[42] Damit kommt der Kategorisierung, der Trennung zwischen wesentlich Gleichem und wesentlich Ungleichem, eine herausragende Bedeutung für die Gesetzgebung zu.

Die Feststellung typischer tatsächlicher Grundmerkmale als wesentliches Zuordnungskriterium zu einer Gruppe von Regelungsobjekten und damit eine Klassifizierung orientiert sich an Kriterien, denen „aus Erwägungen der Gerechtigkeit und Zweckmäßigkeit auch für das Recht unterschiedliche Bedeutung zukommt“:[43] Eine Postsendung erfährt ihre rechtliche Besonderheit aus ihrer besonderen Bedeutung für die Entfaltung der Persönlichkeit im Umgang mit anderen, die Art. 10 Abs. 1 GG explizit aufnimmt, und nicht, weil es sich um den Gegenstand eines bestimmten Formats, eines bestimmten Gewichtes oder eines bestimmten Materials handelt; die besondere Schutzwürdigkeit der Wohnung und ihre Kodifizierung in Art. 13 Abs. 1 GG ist auf die Anerkennung des Schutzes der Privatsphäre zurückzuführen und nicht auf bestimmte bauliche Eigenarten einer Immobilie. Bei den biometrischen Daten steht neben der allgemeinen Handlungsfreiheit vor allem das Recht auf körperliche Unversehrtheit im Fokus, auf das Art. 2 Abs. 2 GG Bezug nimmt.

An diesem letztgenannten Beispiel zeigt sich sehr deutlich, dass die Kategorisierung nach typischen Kennzeichen nicht notwendig die Heranziehung unterschiedlicher Rechte erfordert. Vielmehr kann es sachgerecht sein, die Kategorisierung danach vorzunehmen, wie stark ein einzelnes Recht durch unterschiedliche Maßnahmen beeinträchtigt wird. Im Hinblick auf das Recht auf körperliche Unversehrtheit gibt es graduelle Unterschiede, die zu dem Schluss führen, dass etwa die Abnahme eines Fingerabdrucks rechtlich anders zu gewichten ist als die Entnahme von Körperzellen. Die Menge aller biometrischen Daten,

41 Schneider, *Gesetzgebung*, S. 26.
42 Burghart, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 27 (zitiert nach juris), m.w.N.
43 BVerfG, Urteil vom 18.12.1953, 1 BvL 106/53, zugleich BVerfGE 3, 225, Rn. 37 (zitiert nach juris).

deren Erlangung einheitlich das Recht auf körperliche Unversehrtheit berührt, ist offensichtlich im Hinblick auf ihre jeweilige Schutzwürdigkeit heterogen – und darauf fußt die entsprechende Gesetzgebung.

Durch die Kategorisierung werden konkrete Klassen geschaffen, über die quasi vorab eine jedenfalls relative Aussage für die vorzunehmende Abwägung getroffen werden kann; sie erleichtert dadurch den eigentlichen gesetzgeberischen Abwägungsprozess. Dieses Prinzip kommt nicht nur in der StPO, sondern auch in anderen Gesetzeswerken häufig zur Anwendung. Dabei ist es nicht zwingend, dass, wie bei den biometrischen Daten, die einzelnen Klassen zueinander in ein Schutzwürdigkeitsverhältnis gesetzt werden können. Für gesetzgeberische Zwecke kann es genügen, bestimmte Klassen innerhalb einer Gesamtmenge zu identifizieren, zu deren gegenseitigem Verhältnis zwar keine Aussage getroffen werden kann, wohl aber eine besondere Schutzwürdigkeit der jeweiligen Klasse im Verhältnis zur Grundmenge feststellbar ist.[44]

Zusammenfassend lässt sich festhalten, dass strafrechtliche Ermittlungsbefugnisse gesetzlicher Eingriffsbefugnisse bedürfen. Diese stellen das abstrakte, allgemeingültige Ergebnis einer Abwägung dar, die grundrechtliche Spezifika des Regelungsobjektes ebenso berücksichtigt wie allgemeine Grundsätze der verfassungsrechtlichen Ordnung. Die spezifischen Merkmale beurteilen sich nach der grundrechtlichen Schutzwürdigkeit, die sich aus dem Zusammenspiel mehrerer Grundrechte oder der unterschiedlichen Schutzwürdigkeit im Rahmen lediglich eines Grundrechts ergeben kann. Eine entsprechende Kategorisierung hat mindestens eine relative Aussagekraft und stellt somit ein Instrument dar, das die vorzunehmende gesetzgeberische Abwägung in allgemeingültiger Form teilweise vorwegnimmt.

---

44 Diese Konstellation liegt beispielsweise bei der Grundmenge „Gegenstände“ vor, die einzelne, besonders schutzwürdige Klassen beinhaltet, ohne dass eine Aussage zu deren Verhältnis zueinander getroffen werden könnte: aus der Kategorisierung „Postsendungen“ und „Wohnungen“ ergibt sich eine besondere Relevanz im Verhältnis zu sonstigen Gegenständen, wobei offen bleibt, wie sich die beiden Kategorien zueinander verhalten.

2. Anforderungen an die Regelung elektronischer Beweismittel in der StPO

Zur Einführung in die Thematik werden zunächst die wesentlichen technischen Besonderheiten elektronischer Beweismittel dargestellt. Dies ist erforderlich, um überhaupt eine sinnvolle juristische Betrachtung zu ermöglichen.

Anschließend wird untersucht, inwieweit die vorhandenen gesetzlichen Normierungen in der StPO und den einschlägigen supranationalen Regelungen zum Umgang mit elektronischen Beweismitteln den vorgenannten Anforderungen entsprechen.

Dabei wird sich zeigen, dass die aktuelle Kategorisierung elektronischer Daten und insbesondere die Klassifizierung elektronischer Kommunikationsdaten als Bestands-, Verkehrs- und Inhaltsdaten nicht den verfassungsrechtlichen Vorgaben und denen der modernen Gesetzgebungslehre entspricht. Letzteres liegt vor allem daran, dass sich die Kategorisierung an den tatsächlichen Bedürfnissen der Telekommunikationsanbieter in der Vergangenheit orientiert hat. Selbst wenn die ursprüngliche Klassifizierung zunächst noch mit der verfassungsrechtlichen Werteordnung in Einklang zu bringen war, gilt dies aufgrund der zwischenzeitlichen technischen und gesellschaftlichen Veränderungen, die seit der Einführung der Begriffe stattgefunden haben, heute nicht mehr.

Die dadurch begründeten Zweifel an der Verfassungsmäßigkeit einzelner Regelungen zu elektronischen Beweismitteln im Strafprozess werden im Folgenden herausgearbeitet und führen zu der Schlussfolgerung, dass wegen der strafverfahrensrechtlichen Bedeutsamkeit dieses Beweismittels eine umfassende Regelungspflicht für den Gesetzgeber besteht.

Der Exkurs zur Lage in den übrigen EU-Mitgliedstaaten soll schließlich verdeutlichen, dass es sich nicht um ein singuläres Problem des deutschen Strafprozessrechts handelt, sondern aufgrund der

verbreiteten identischen Datenkategorisierung in allen Mitgliedstaaten vergleichbare Probleme auftreten.

Ein weiteres Ziel dieser Arbeit ist sodann die Analyse möglicher Regelungsalternativen. In diesem Zusammenhang wird der theoretische Ansatz, alle elektronischen Daten einheitlich zu behandeln, aus rechtlichen und tatsächlichen Gründen verworfen. Die denkbare Alternative, jeden Datensatz gesondert zu betrachten, ist aufgrund der Vielzahl der zur Verfügung stehenden Daten nicht umsetzbar und eine Abstrahierung daher unumgänglich.

Damit rückt die Frage in den Fokus, wie elektronische Beweismittel sachgerecht und unter Berücksichtigung der genannten verfassungsrechtlichen Vorgaben kategorisiert werden können. Zur Beantwortung dieser Frage werden verschiedene Kriterien, die derzeit in der Literatur diskutiert werden – die Rechtsprechung folgt der herkömmlichen Einteilung, ohne die zugrundeliegenden Kriterien in Frage zu stellen – auf ihre Geeignetheit hin geprüft, als rechtlich relevante Unterscheidungskriterien eine Kategorisierung elektronischer Daten zu ermöglichen, die deren typische Grundmerkmale widerspiegelt.

Im Ergebnis wird sich zeigen, dass bei elektronischen Daten die Differenzierung innerhalb eines großen, alle elektronische Daten umfassenden Schutzbereiches vorzunehmen ist und keines der bislang diskutierten Kriterien eine zufriedenstellende Lösung bietet.
Aus der Analyse der einschlägigen datenspezifischen Grundrechte, namentlich des Fernmeldegeheimnisses, des Rechts auf informationelle Selbstbestimmung und des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme, die ausführlich dargestellt und entfaltet werden, wird sich ergeben, dass letztlich auf die berechtigte Erwartungshaltung des Datenberechtigten in Bezug auf die Vertraulichkeitswahrung abgestellt werden muss. Die Erwartungshaltung bestimmt sich maßgeblich danach, wem der Datenberechtigte die Kenntnisnahme eines konkreten Datensatzes gestattet.

Mit diesem Kriterium lässt sich eine Kategorisierung in fünf Klassen vornehmen, die ihrerseits erforderlich ist, um sinnvoll und im Einklang mit der modernen Gesetzgebungslehre strafprozessuale Eingriffsbefugnisse im Hinblick auf elektronische Daten zu entwickeln. Diese Klassen werden (mit steigender Schutzwürdigkeit) bezeichnet als unbeschränkt zugängliche Daten, beschränkt zugängliche Daten, vertrauliche Daten, geheime Daten und Kernbereichsdaten.

Die grundrechtsorientierte Herausarbeitung des maßgeblichen Kriteriums und die daraus folgende Ableitung von fünf konkreten Kategorien erlaubt die Ablösung der bisherigen Kategorisierung, die weder praktikabel noch grundrechtskonform ist. Zum leichteren Verständnis werden ausgewählte Zuordnungsbeispiele im herkömmlichen und im neuen Klassifikationsmodell gegenübergestellt.

Ein Überblick über die Klassifikation analoger, also nicht-elektronischer Daten wird zeigen, dass für diese die vorgeschlagene Einteilung im Wesentlichen bereits angewandt wird, auch wenn es an einer expliziten, namentlichen Unterscheidung fehlt und verfassungsrechtliche Besonderheiten einzelner Beweismittel einer direkte Übertragung der jeweiligen Differenzierungen auf elektronische Daten entgegenstehen.
Der Befund bestätigt die Stimmigkeit des neuen Modells im verfassungsrechtlichen Rahmen und die Kohärenz der jeweiligen Regelungskomplexe.

Zur Verdeutlichung der Tauglichkeit des neuen Modells für eine umfassende Neuregelung elektronische Daten in der StPO wird sodann ein Musterentwurf, der auf der vorgeschlagenen Neuklassifizierung beruht und gleichzeitig die genannten allgemeinen inhaltlichen Anforderungen erfüllt, entwickelt und erläutert.

Im abschließenden Ausblick werden Einzelfragen wie besondere Problemkonstellationen und die Übertragbarkeit der Neuklassifikation auf andere Rechtsordnungen, namentlich auf EU-Ebene, angerissen.

Jenseits der Schaffung eines konkreten Abwägungsinstrumentes in Form der Neuklassifikation unterstützt diese Arbeit argumentativ Überlegungen einer konzeptionellen Überarbeitung der StPO im Hinblick auf elektronische Beweismittel und, da eine neue Begriffsverwendung vorgeschlagen wird, Verbesserungsbestrebungen für die internationale Kooperation, die derzeit unter anderem daran leidet, dass elektronische Daten zwar mit einheitlicher Bezeichnung, aber unterschiedlichem Bedeutungsinhalt gruppiert werden.

Obwohl sich die Problematik, die sich aus der althergebrachten Kategorisierung ergibt, nicht nur in Deutschland, sondern in vergleichbarer Art und Weise auch in den EU-Mitgliedstaaten und weiteren westlichen Ländern wiederfindet und der Ruf nach einer Neuklassifizierung oder jedenfalls einer Erweiterung des bisherigen Modells in der internationalen Literatur zunimmt,[45] haben die Recherchen bislang keinen Hinweis darauf gebracht, dass bereits eine konkrete Neuklassifikation elektronischer Daten vorgeschlagen worden ist.[46] Insofern will diese Arbeit – last but not least - einen konstruktiven Beitrag zur erforderlichen und noch in den Anfängen steckenden wissenschaftlichen Diskussion darstellen.

45 Vgl. Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679); Svantesson, *Data categorisation and law enforcement access to cloud* data; Europäische Kommission, *Report on the 17 / 18 January 2017 expert meeting*, S. 1; Europäische Kommission Services, *Technical Document*, S. 18 f.

46 Stand: 30.04.2018.

III. Begrenzung des Untersuchungsgegenstandes

Die Neuklassifikation bezieht sich auf sämtliche elektronischen Daten, die als Beweismittel im Strafprozess in Betracht kommen.

Der Begriff elektronischer Daten wird dabei im Sinne des Art. 2 b) der AAIS-Richtlinie als „jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form“ verstanden. Das schließt zum einen originär digitale Daten, die innerhalb eines Computersystems entstanden sind, und zum anderen auch ursprünglich nicht-elektronische und erst später digitalisierte Daten ein.[47]

Die vorgeschlagene Klassifikation macht – aus rechtlichen Gründen, die im Einzelnen dargelegt werden - keinen Unterschied zwischen gespeicherten und Echtzeit-Daten.

Zudem berücksichtigt sie neben Kommunikationsdaten auch sämtliche Nicht-Kommunikationsdaten, sodass beispielsweise auch die Daten, die im Zusammenhang mit dem Internet der Dinge zur Verfügung stehen, umfasst werden.

Schließlich ist der Untersuchungsgegenstand dieser Arbeit auf elektronische Daten mit ausschließlich strafprozessualer Relevanz begrenzt. Damit bleibt offen, ob die Anwendung der vorgeschlagenen Klassifizierung beispielsweise auf weitere gerichtliche Zweige oder die präventionsorientierte oder nachrichtendienstliche Tätigkeit staatlicher Stellen übertragbar ist.

Auch wenn sich diese Arbeit ausdrücklich auf die deutsche Rechtsordnung bezieht, sind ihre Kernaussagen auf vergleichbare Rechtssysteme, wie sie sich in den Mitgliedstaaten der EU finden, übertragbar.

47 Die Begriffsbestimmung folgt EVIDENCE Project, *Roadmap*, S. 23.

IV. Methodik

Dem einleitenden Teil der Arbeit (Teil A) folgen sieben Hauptblöcke mit unterschiedlichen Themenschwerpunkten: die technischen Besonderheiten elektronischer Beweismittel (B), die daraus resultierende Erforderlichkeit spezieller strafprozessualer Regelungen und die derzeitigen in Deutschland relevanten gesetzlichen Regelungen nebst den ihnen zugrundeliegenden Datengruppierungen (C) - Teil C wird zudem ergänzt durch einen Exkurs zur Rechtslage in den anderen Mitgliedstaaten der Europäischen Union -, sodann, als Herzstück der Arbeit, die Entwicklung einer Neuklassifizierung elektronischer Daten für strafprozessuale Zwecke (D) sowie ihre Gegenüberstellung mit den Klassifikationen analoger Daten (E), schließlich die Präsentation eines legislativen Musterentwurfes (F) sowie eines abschließenden Fazits (G) und Ausblicks (H).

Die Darstellung der Besonderheiten elektronischer Beweismittel, die, wie sich zeigen wird, allesamt auf ihrer Unkörperlichkeit beruhen, erfolgt mittels einer technikbetonten empirischen Analyse ihrer Charakteristika, die sie von herkömmlichen Beweismitteln in unterschiedlicher Art und Weise unterscheiden. Ein Grundverständnis darüber, was elektronische Daten ausmacht und wie bestimmte technische Vorgänge ablaufen, ist unabdingbare Voraussetzung für ihre sinnvolle juristische Behandlung.

(Grund-)rechtsdogmatisch und unter Anwendung fundamentaler Rechtsprinzipien wie dem Unmittelbarkeitsgrundsatz wird sodann untersucht, ob es aufgrund der dargestellten technischen Besonderheiten überhaupt gesonderter Regelungen für elektronische Beweismittel bedarf. In diesem Zusammenhang spielen auch rechtspolitische Überlegungen eine Rolle, die jedoch, wie sich zeigen wird, keinen entscheidenden Einfluss auf das letztlich bejahende Untersuchungsergebnis haben.
Rein rechtsdogmatisch gestaltet sich im Anschluss die Untersuchung der in Deutschland geltenden einschlägigen Regelungen der StPO und der relevanten Normierungen im internationalen Kontext.

Die Methode der empirischen Analyse kommt im Exkurs zur Lage in den anderen EU-Mitgliedstaaten zur Anwendung.

Die Entwicklung einer Neuklassifikation basiert zunächst auf einer rechtsdogmatischen Darstellung des bisherigen Klassifikationsmodells, das hinsichtlich Kommunikationsdaten zwischen Bestands-, Verkehrs- und Inhaltsdaten unterscheidet. Die anschließende kritische Auseinandersetzung mit der herkömmlichen Dateneinteilung beruht vorwiegend auf einer empirischen Analyse ihres Entstehungskontextes.

Vorüberlegungen zur Neuklassifizierung und die Entwicklung geeigneter Unterscheidungskriterien werden im Wesentlichen rechtsdogmatisch begründet. Ganz im Sinne der modernen Gesetzgebungslehre liegt der Fokus der Kriterienentwicklung auf den datenspezifischen Grundrechten, namentlich dem Fernmeldegeheimnis, dem Recht auf informationelle Selbstbestimmung und dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, die ausführlich dargestellt werden.

Die Anwendung der Kriterien, die unmittelbar zur vorgestellten Neuklassifikation von unbeschränkt zugänglichen Daten, beschränkt zugänglichen Daten, vertraulichen Daten, geheimen Daten und Kernbereichsdaten führt, ist ausschließlich rechtsdogmatisch-deduktiv begründet.

Sodann kommen die Methoden der Rechtsvergleichung und der Rechtspolitik zur Anwendung, wenn die herkömmliche Datenklassifizierung der neu vorgeschlagenen gegenübergestellt und Anwendungsbeispiele für konkrete Datensätze dargelegt werden.

Der anschließende Vergleich mit Kategorisierungen analoger Daten bedient sich rechtsvergleichender und rechtsdogmatischer Methoden, um zu zeigen, dass die vorgeschlagene Unterscheidung vom Prinzip her auf fast alle Daten, analoge wie elektronische, Anwendung findet, auch wenn aufgrund grundrechtsspezifischer Besonderheiten die

konkrete rechtliche Ausgestaltung im Detail unterschiedlich ausfällt.

Die abschließenden Teile dieser Arbeit, der Musterentwurf einer gesetzlichen Neuregelung, das Fazit und der Ausblick, sind rechtspolitischer Natur.

B. Technische Besonderheiten elektronischer Beweismittel[48]

Als herkömmliche Beweismittel sind im deutschen Strafprozessrecht Zeugen, Sachverständige und Augenschein, Urkunden und andere Schriftstücke sowie in gewissem Rahmen die Beschuldigtenaussage anerkannt[49] und explizit gesetzlich geregelt,[50] um den jeweiligen Besonderheiten Rechnung zu tragen. Elektronische Daten werden in diesem Kanon nicht ausdrücklich erwähnt. Sie weisen aber ebenfalls Besonderheiten auf, die im Folgenden näher dargestellt werden sollen. Ein technisches Grundverständnis ist unabdingbar, um die rechtlich relevanten typischen Merkmale elektronischer Daten herauszuarbeiten und dadurch die bestehenden Regelungslücken und verfahrensrechtlichen Unzulänglichkeiten zu erkennen und sie sinnvoll zu beheben.

Als herausragendes Wesensmerkmal elektronischer Daten ist ihre fehlende Körperlichkeit zu nennen.[51] Beim heutigen Stand der Technik stellen elektronische Daten nichts anderes als eine Notation mit zwei Variablen, 0 und 1, genannt Bits oder Qubits, dar.[52] Sie sind, anders als Datenträger oder Hilfsmittel für den Datentransfer, nicht fassbar und lassen sich je nach Übertragungsart annähernd mit Lichtgeschwindigkeit übertragen oder verschieben. Die jeweilige Sensibilität eines Datensatzes im Hinblick auf die Persönlichkeitsrechte des Betroffenen ist der 0 - 1 Notation nicht anzusehen. Aus der fehlenden

---

48 Die unter diesem Punkt folgende Darstellung basiert im Wesentlichen auf den Veröffentlichungen Warken, E*lektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 1, NZWiSt 2017, 289 (291, 294 ff.) und Teil 2, NZWiSt 2017, 329 (329 ff.).

49 Vgl. zur Übersicht über die herkömmlichen Beweismittel: Meyer-Goßner / Schmitt, *StPO*, Einl Rn. 49.

50 Vgl. §§ 48 ff. StPO zum Zeugen, §§ 72 ff. StPO zum Sachverständigen und Augenschein, §§ 249 ff. StPO für Urkunden und andere Schriftstücke sowie §§ 136, 163a Abs. 1, 243 Abs. 3 StPO zur Beschuldigtenaussage.

51 Zur herausragenden Bedeutung der immateriellen Eigenschaft von Daten als wesentliches Unterscheidungsmerkmal zu herkömmlichen Beweismitteln vgl. auch Sieber, *Gutachten zum 69. DJT*, S. 153.

52 Vgl. Europol, *IOCTA 2016*, S. 64, zur näheren Erläuterung.
Während ein Bit entweder den Wert 0 oder den Wert 1 darstellt, kann sich ein Qubit darüber hinaus gleichzeitig auf beide Werte beziehen. Die sich daraus ergebende erweiterte Möglichkeit der Datenverarbeitung bezeichnet man als „Quanteninformatik“ (vgl. Wikipedia, Suchbegriff *Quanteninformatik*).

Körperlichkeit ergeben sich Besonderheiten, die zum einen ihre Erlangung (dazu unter I.) und zum anderen ihre Verwertung (II.) betreffen.

I. Erlangung eines Datensatzes

1. Verschiedene Arten der Übermittlung

Elektronische Daten können einerseits durch elektronische Übermittlung, über einen mobilen Datenträger oder bereits visualisiert, beispielsweise als Dokument oder in Bildform, an die Ermittlungsbehörde gesandt werden. Eine Übergabe im Sinne von Gewahrsamsübertragung von einer Person auf eine andere ist hingegen aufgrund der Unkörperlichkeit eines Datensatzes nicht möglich; der Empfänger erhält vielmehr eine Kopie oder ein Abbild eines bestehenden Datensatzes.

Die elektronische Übermittlung erfolgt technisch entweder durch „Anzapfen der Leitung“, also durch ein meist verdeckt durchgeführtes Ausleiten des Datenstromes zur Strafverfolgungsbehörde, oder durch ein von der Strafverfolgungsbehörde oder vom Dateninhaber aktiv gesteuertes, zielgerichtetes Übersenden, das einen digitalen Zugang zum Speichermedium voraussetzt.

Als mobile Datenträger kommen Geräte wie Laptops oder Smartphones ebenso in Betracht wie Teile solcher Geräte (interne Festplatten, SIM-Karten etc.) oder sonstige Speichermedien (externe Festplatten, USB-Sticks, CDs, DVDs etc.).[53]

Die Übermittlung bereits visualisierter elektronischer Daten kann auf elektronischem Weg (etwa durch Übersendung einer Text- oder Bilddatei per E-Mail) oder klassisch in Papierform erfolgen. Dabei ist zu beachten, dass bei der Übermittlung in Papierform das eigentliche Beweismittel nunmehr das entsprechende Dokument oder das entsprechende Bild ist, nicht mehr der ursprüngliche elektronische Datensatz als solcher. Diese Unterscheidung ist unter anderem deshalb zu wahren, weil die ursprünglich anhängenden Metadaten des

53 Gemäß LKA Baden-Württemberg, *Cybercrime und Digitale Spuren, Jahresbericht 2016*, S. 26, setzte sich im Jahr 2016 die Gesamtmenge an asservierten mobilen Datenträgern in Baden-Württemberg wie folgt zusammen: 48% Mobiltelefone und SIM-Karten, 12% PCs, 3% Tablets und 37% sonstige Datenträger.

Datensatzes bei der Visualisierung grundsätzlich nicht berücksichtigt werden.[54]

Dateninhaber kann in allen Fällen sowohl der Verdächtige als auch jeder beliebige Dritte, etwa eine einzelne natürliche Person oder ein Großunternehmen wie Anbieter elektronischer Informations- oder Kommunikationsdienstleistungen, sein.

Die zielgerichtete Datenübermittlung durch den ursprünglichen Dateninhaber erfolgt in der Praxis teilweise aus einem gänzlich selbstbestimmten Entschluss heraus,[55] teilweise wird der Entschluss von der Strafverfolgungsbehörde durch eine entsprechende Anfrage initiiert. Je nach den Umständen des Einzelfalles verbleibt die Entscheidung, ob und was übersandt wird, beim Dateninhaber[56] oder es besteht eine gesetzliche Verpflichtung zur Datenübermittlung.[57]

2. Grundsätzliches Verbleiben der Originaldaten beim Dateninhaber

Anders als bei allen anderen dinglichen Beweismitteln, die die Strafverfolgungsbehörden erlangen können, ist bei elektronischen Daten zu berücksichtigen, dass ihre Erlangung nicht zwingend einen Gewahrsamswechsel voraussetzt, sondern technisch eine Datensicherung, also ein Kopiervorgang auf ein Speichermedium der

---

54 Bereits einfache elektronische Dokumente oder Bildaufnahmen verfügen über eine Vielzahl von Hintergrundinformationen, wie zum Beispiel zum Autor, zum Zeitpunkt der Erstellung, der letzten Änderung oder des letzten Zugriffs, zu Zugriffsberechtigungen oder zum Dateiformat. Diese Informationen werden bei der visualisierten Darstellung grundsätzlich nicht mitübertragen.

55 Ein solch freiwilliger Entschluss kann zum Beispiel regelmäßig bei der Datenübermittlung im Zusammenhang mit einer Strafanzeige unterstellt werden.

56 Diese Fallgestaltung ist vergleichbar mit der Informationserlangung im Rahmen der informatorischen Befragung. Sie spielt in der Praxis im Verhältnis zu den US-amerikanischen Internet Service Providern eine große Rolle, denen es nach US-amerikanischem Recht gestattet ist, Bestandsdaten („subscriber data“) und Verkehrsdaten („traffic data“) auf freiwilliger Basis an ausländische Strafverfolgungsbehörden direkt zu übermitteln. Nach Auskunft von Apple Inc., *Report on Government Information Requests, 2017 H1*, gingen im ersten Halbjahr 2017 allein aus Deutschland 12.677 solcher Anfragen bei dem Unternehmen ein, wovon 9.312, mithin 73%, beauskunftet wurden.

57 Beispielsweise gemäß § 100g StPO für Verkehrsdaten oder § 100j StPO für Bestandsdaten.

Behörde erfolgt.[58] Grundsätzlich verbleiben daher die betreffenden Datensätze im Original bei dem oder den bisherigen Dateninhaber(n).[59] Gleichzeitig weist die Kopie alle Merkmal des Originals auf, beide Datensätze sind bei korrektem Sicherungsvorgehen völlig identisch und weisen insbesondere übereinstimmende Informationen zu ihrem Entstehungszeitpunkt und ihrer Urheberschaft auf.[60] Dies gilt für die Kopie eines Schriftstückes nicht, was im Strafverfahren folgerichtig dazu führt, dass einer Kopie grundsätzlich ein anderer Beweiswert zukommt als dem Originalschriftstück.

3. Grundsätzliche Ortsungebundenheit der Zugriffshandlung

Ebenfalls abweichend von den herkömmlichen Beweismitteln muss die Sicherstellung nicht zwingend „vor Ort“, also am Ort der physikalischen Speicherung erfolgen, sondern kann bei entsprechenden technischen Voraussetzungen grundsätzlich von überall her erfolgen.[61]

4. Unterschiedliche Speicher- und Datenverarbeitungsorte (insbesondere: Cloud)

Der Raum, in dem Internetkriminalität und damit die Entstehung beweisrelevanter elektronischer Daten stattfindet, der virtuelle „cyber space“, ist für sich gesehen materiell nicht existent und a-territorial.[62] Der tatsächliche Speicher- und Verarbeitungsort elektronischer Daten

---

58 Art. 19 Abs. 3 der Cybercrime-Konvention differenziert in dieser Hinsicht sehr genau zwischen der Beschlagnahme eines Computersystems oder eines Teiles davon oder eines Computerdatenträgers, der Anfertigung oder Zurückbehaltung einer Kopie der Computerdaten und der Unzugänglichmachung oder Entfernung der Computerdaten aus dem Computersystem.

59 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations*, S. 17; Mason, *Draft Convention on Electronic Evidence*, S. 7 Ziff. 10 i.V.m. S. 3 Art. 5 Abs. 1, formuliert folgerichtig, dass jegliche körperliche Manifestation eines Datensatzes, beispielsweise ein Ausdruck, immer eine bloße Kopie darstelle: „There can be no original“.

60 Die Identität beider Datensätze schließt nicht aus, dass hinsichtlich der Kopie weitere Metadaten anfallen, etwa über den Zeitpunkt der Erstellung der Kopie.

61 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations*, S. 18.

62 Zoetekouw, *Ignorantia Terrae Non Excusat,* S. 6; Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 1, zitiert nach juris).

verliert sowohl in sozialer als auch in technischer Hinsicht zunehmend an Bedeutung.[63] Jedenfalls in der westlichen Welt ist es dem Durchschnittsnutzer in der Regel gleichgültig, wo sich der physikalische Speicher- und Verarbeitungsort seiner Daten befindet.

Dies erklärt die stetig wachsende Verbreitung der sogenannten Cloud-Dienste,[64] deren technischer Ansatz darin liegt, IT-Infrastrukturen über ein Rechnernetz zur Verfügung zu stellen.[65] „Cloud Computing“ kann, vereinfacht dargestellt, als Gesamtbegriff für ausgelagerte Datenverarbeitungsdienste im weitesten Sinne verstanden werden,[66] wobei sich die Dienste auf die Bereitstellung von Software („software as a service“ (SaaS)), von Plattformen („platform as a service“ (PaaS)) und / oder von Infrastruktur („infrastructure as a service“ (IaaS)) beziehen können.[67]

Letztgenannter Dienst umfasst die physikalische Bereitstellung von Speichern, Servern und der damit zusammenhängenden Infrastruktur solcher Rechenzentren, die über das Internet zugänglich sind.[68] PaaS

---

63 Zoetekouw, *Ignorantia Terrae Non Excusat,* S. 6.

64 Europol, *IOCTA 2016*, S. 52; LKA Baden-Württemberg, *Cybercrime und Digitale Spuren, Jahresbericht 2016,* S. 28; Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (243); Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S. 6; Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (739).
Nach Woods (a.a.O., S. 740 f., m.w.N.) ist Schätzungen zufolge davon auszugehen, dass im Jahr 2011 ca. 7% aller elektronischer Daten auf Cloud-Servern gespeichert wurden, während es 2016 bereits 36% aller elektronischen Daten gewesen sein sollen.

65 Wikipedia, Suchbegriff *Cloud Computing.*

66 Wie Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2, zitiert nach juris), zutreffend feststellen, gibt es keine allgemeingültige Definition des Begriffes „Cloud Computing“, zumal es sich „weniger [um] ein bestimmtes technisches Konstrukt als vielmehr eine Idee, […] ein Dienstleistungskonzept“ handele (Hiéramente / Fenina, a.a.O.).

67 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 15, 21, m.w.N.; Wikipedia, Suchbegriff *Cloud Computing,* m.w.N.
Laut Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S. 3, waren jedenfalls im Jahr 2012 unter den 10 größten IaaS-, PaaS- oder SaaS-Anbietern jeweils mindestens 9 US-amerikanische Unternehmen. Die Zahl bestätigt die praktische Relevanz dieser Dienstleister für die europäischen Strafverfolgungsbehörden.

68 Vgl. Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2 f. zitiert nach juris), m.w.N.

hingegen erlaubt dem Nutzer den Zugriff auf ein dezentral, aus Sicht des Nutzers extern installiertes Programm.[69] Die zugrundeliegende Idee ist es, auf diese Art einer Vielzahl von Nutzern Zugang zu einer einzelnen Software-Applikation zu gewähren, sodass zum Beispiel eine offene Kommunikation unter allen Nutzern der Plattform stattfinden kann.[70] Durch den dem Verbraucher zugänglichsten und insgesamt am meisten verbreiteten Dienst,[71] dem SaaS, werden dem Nutzer möglichst nutzerfreundliche, vollständige Anwendungen zur direkten Nutzung zur Verfügung gestellt.[72] Dies betrifft vor allem Dienste, die ursprünglich lokal, auf dem Endgerät des Nutzers, ausgeführt wurden, beispielsweise die Speicherung, Verwaltung und Bearbeitung von Dokumenten, E-Mails, Adressen, Terminen, Bildern etc.

Die strafprozessual relevante externe Datenspeicherung als Dienstleistung findet in diesem Schema zumeist im SaaS-Bereich statt[73] und verdrängt zunehmend die Datenspeicherung auf dem Nutzerendgerät, das dadurch mehr und mehr zum bloßen Zugangsinstrument für den Abruf dezentral gelagerter Daten wird.[74]

Häufig verfügt der Cloud-Anbieter, dessen sich der Nutzer beispielsweise zur Speicherung seiner Daten bedient, nicht nur über ein einzelnes Speichermedium, sondern über mehrere,[75] was dazu führt,

---

69 Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2, zitiert nach juris).

70 Der Begriff der Kommunikation ist in diesem Zusammenhang sehr weit zu verstehen. Er umfasst den bloßen sozialen Austausch etwa in klassischen „Chaträumen“ oder auf Ratgeberseiten zu allen erdenklichen Themen und ebenso Verhandlungen, die in einem Vertragsabschluss enden können (wie beispielsweise auf der „ebay“-Seite).

71 Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 3, zitiert nach juris).

72 Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 3, zitiert nach juris).

73 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 15, 21.

74 Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 1 f., zitiert nach juris), m.w.N.

75 Beispielhaft sei auf Microsoft verwiesen; das Unternehmen hatte nach eigenen Angaben im Juni 2015 für seine Cloud-Dienstleistungen über 1 Millionen Server in über 100 weltweit verteilten Datenzentren in Betrieb (Microsoft Corporation, *Datacenters and Network Fact Sheet)*.

dass Algorithmen den Speicherort – oft grenzüberschreitend - ohne konkrete menschliche Steuerung bestimmen.[76] Dies geschieht teilweise mit stetiger Ortsänderung,[77] teilweise in solcher Art und Weise, dass selbst eine nachträgliche Lokalisation nur mit erheblichem Aufwand möglich ist.[78] Zudem erfolgt ein Datenverarbeitungsprozess oder die Speicherung eines elektronischen Dokuments nicht mehr zwingend als Gesamtheit an einem Ort, sondern aus sicherheitsrelevanten und / oder wirtschaftlichen Gründen zeitgleich und bildlich gesprochen in vielen Einzelteilen auf einer Vielzahl von Rechnern, die im virtuellen Netzwerk der Cloud weltweit verteilt sein können.[79]

Während das automatisch gesteuerte Verschieben des Speicherplatzes und das Datensplitting für den Durchschnittsnutzer keine Rolle spielen – im Normalfall kann der Endnutzer den Datentransfer weder nachvollziehen noch beeinflussen –[80] eröffnen sich dem fachkundigen „Cyber-Kriminellen“ dadurch willkommene Möglichkeiten, beispielsweise seinen Aufenthaltsort, seine Daten und seine Netzwerke beziehungsweise Infrastruktur zu verschleiern.[81] Darauf kann er auch durch den Einsatz sogenannter Botnetze, bei denen zeitgleich und ohne Einverständnis der Berechtigten auf die Rechnerkapazitäten einer

76 Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S. 4; Zoetekouw, *Ignorantia Terrae Non Excusat,* S. 6; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (678).

77 Sieber, *Gutachten zum 69. DJT*, S. 36; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (674).

78 Sieber, *Gutachten zum 69. DJT*, S. 36; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (680); Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 7 f.

79 Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S. 4; Zoetekouw, *Ignorantia Terrae Non Excusat*, S. 6; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (680).

80 So auch Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2, zitiert nach juris).

81 Zoetekouw, *Ignorantia Terrae Non Excusat*, S. 6.

Vielzahl von miteinander verknüpften Rechnern zurückgegriffen wird,[82] hinwirken.[83]

Erschwerend kommt hinzu, dass in vielen Fällen gleichzeitig mehrere Cloud-Dienstleister auf verschiedenen Leistungsebenen in Anspruch genommen werden,[84] was zu entsprechender Unübersichtlichkeit führt.[85]

5. Zeitfaktor

Elektronische Daten können, anders als alle herkömmlichen Beweismittel, mit annähernd Lichtgeschwindigkeit und jedenfalls in Sekundenschnelle von einem Ort auf der Welt zu einem anderen versandt werden.[86] Dies kann durch im Wortsinne einen Klick geschehen, also ohne nennenswerten finanziellen oder organisatorischen Aufwand.
Dasselbe gilt für ihre Löschung, wobei sie in den seltensten Fällen wirklich zur absoluten Unwiederbringlichkeit führt, sondern mehr oder weniger technischer Aufwand erforderlich ist, um die Daten wiederherzustellen.[87] Eine echte Löschung gespeicherter Daten ist Dienstleistern aller Art häufig aus Datenschutzgründen vorgeschrieben,[88] eine längerfristige Speicherung darf nur unter engen

82 Wikipedia, Suchbegriff *Botnet.*
83 Sieber, *Gutachten zum 69. DJT*, S. 36.
84 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 23; Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2, zitiert nach juris), m.w.N.
85 Laut Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S. 1, sei es „extrem unwahrscheinlich“, dass sich der angefragte Dienstleister und der relevante Server, auf denen bestimmte Nutzerdaten liegen, in derselben Jurisdiktion befänden.
86 Ausführlich dazu: Sieber, *Gutachten zum 69. DJT*, S. 35 f.
87 Für die endgültige Löschung elektronischer Daten bedarf es in der Regel einigen Aufwandes, etwa der mehrfachen Überschreibung des gesamten Speichermediums.
88 Die DS-GVO, die gemäß ihrem Art. 99 Abs. 2 ab dem 25.05.2018 Anwendung finden wird, betont unter den Begründungen Ziff. 65 f., 68 ausdrücklich das Recht des Betroffenen auf Löschung seiner Daten und statuiert in Art. 17 unter bestimmten Umständen explizit ein „Recht auf Vergessenwerden“.
Auch die DS-Richtlinie Strafjustiz, die nach ihrem Art. 63 Abs. 1 bis zum 06.05.2018 in nationales Recht umzusetzen ist, sieht in Art. 16 Abs. 2 ein

gesetzlichen Voraussetzungen und für einen konkreten Zeitraum erfolgen.[89] Das gilt nicht nur im Herrschaftsbereich der StPO, sondern in vielen Ländern, insbesondere in allen EU-Mitgliedstaaten.[90]

6. Anonymität im Netz

Die technische Struktur des Internets erlaubt es dem Nutzer, gänzlich anonym Seiten aufzurufen, Inhalte herunterzuladen oder an der öffentlichen Kommunikation teilzunehmen.[91] Durch die freie Wahl eines Nutzernamens oder einer E-Mail-Adresse, die lediglich durch die (Noch-)Verfügbarkeit der Zeichenkette eingeschränkt ist, und die faktische Möglichkeit, Endgeräte mit dazugehörigem Datenvolumen als Prepaid-Option ohne Identifikationserfordernis zu erwerben,[92] können selbst individuelle Nachrichten so versandt werden, dass für den Empfänger nicht ersichtlich ist, von wem sie stammen.
Eine eindeutige Identifizierung des Handelnden ist auch grundsätzlich nicht möglich: Zwar bedarf es zur ordnungsgemäßen Nachrichten-

---

Recht auf Löschung personenbezogener Daten vor.

89 Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 1 f., zitiert nach juris).

90 Der EuGH hat in mehreren Entscheidungen die Bedeutung des Datenschutzes betont und einer anlassunabhängigen Datenspeicherung („Vorratsdatenspeicherung“) auch in zeitlicher Hinsicht äußerst enge Grenzen gesetzt – vgl. EuGH, Urteil vom 08.04.2014 („Digital Rights Ireland“), C-293/12 und C-594/12, durch das die DS-Richtlinie vom 15. 03.2006 für unwirksam erklärt wurde; EuGH, Urteil vom 21.12.2016 („Tele2 / Watson“), C-203/15 und C-698/15, zu den strikten Anforderungen für die Zulässigkeit einer Vorratsdatenspeicherung.

91 Sieber, *Gutachten zum 69. DJT*, S. 36 f., m.w.N., spricht von „scheinbar völliger Anonymität“, und stellt fest, dass „die Rückverfolgung von Verdächtigen […] oft mit besonderen Schwierigkeiten verbunden“ sei und auch die eindeutige Zuordnung etwa einer IP-Adresse zu einem bestimmten Computersystem noch keinen Aufschluss darüber gebe, welche Person das Computersystem tatsächlich genutzt habe; zu weiteren Anonymisierungsmöglichkeiten vgl. Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (242).
Zur Bedeutung der Anonymität im Internet im Zusammenhang mit der Meinungsfreiheit: Vollversammlung der Vereinten Nationen, *Bericht des Sonderberichterstatters David Kaye*, 22.05.2015, S. 4 ff.

92 Gemäß § 111 Abs. 1 S. 3 TKG bedarf es in Deutschland zwar offiziell der Vorlage eines Identitätsnachweises für den Erwerb sogenannter Prepaid-Karten für Mobiltelefone. Dies betrifft jedoch nur Telekommunikations-dienstleistungen im Sinne des TKG. Zudem darf nach eigener Erfahrung bezweifelt werden, dass in allen Verkaufsstellen solcher Karten die Identitätsfeststellung mit der erforderlichen Sorgfalt durchgeführt wird.

übermittlung aus technischen Gründen einer eindeutigen Absender- und Empfangsadresse, die derzeit standardmäßig über die IP-Adressen als Zahlenfolge angegeben werden.[93] Die IP-Adresse führt aber lediglich zu einer Internetanschlussstelle, die von jeder Person, der die Zugangsdaten bekannt sind, genutzt werden kann.[94]

Eine besondere Herausforderung stellt die in den letzten wenigen Jahren[95] von den Dienstleistern praktizierte Mehrfachvergabe sogenannter dynamischer IP-Adressen dar: Während in den Anfangszeiten des Internets eine so geringe Anzahl an internetfähigen Geräten vorhanden war, dass jedem Gerät eine permanente IP-Adresse zugeordnet werden konnte, führte die schnell wachsende Verbreitung solcher Geräte vor etwa 10 Jahren zu einer Knappheit verfügbarer Adressen. Mit Ausnahme derjenigen Geräte, die, wie beispielsweise Server der öffentlichen Telekommunikation, technisch auf eine dauerhafte, statische IP-Adresse angewiesen sind, wurden die Geräte sodann zunehmend mit dynamischen IP-Adressen versehen, die lediglich für den jeweils konkreten Telekommunikationsvorgang Gültigkeit haben. Auf diese Weise stand zunächst wieder eine hinreichende Anzahl an IP-Adressen zur Verfügung, da nicht alle Geräte gleichzeitig im Netz angemeldet waren.

Aufgrund der stetigen Zunahme der Anzahl internetfähiger Geräte und der Verbreitung von Nutzungsfunktionen, die zum einen häufiger und zum anderen jeweils länger andauernd (wenn nicht gar permanent) eine Internetverbindung erfordern, zeichnet sich aktuell erneut eine

93 Beim derzeit als Standard verwendeten Internet Protocol Version 4 (IPv4) setzt sich die IP-Adresse aus 4 Böcken zusammen, wobei jedem Block ein Zahlenwert zwischen 0 und 255 zugewiesen wird (vgl. Wikipedia, Suchbegriff *IPv4*).

94 In großer Anzahl geschieht dies in der Praxis etwa bei öffentlichen „Hot Spots“ oder den „Free W-Lan“-Räumen, die Infrastruktureinrichtungen wie Cafés, Einkaufsläden und Sporteinrichtungen zunehmend anbieten. Dass auch bei gleichzeitiger Nutzung einer einzigen IP-Adresse durch mehrere Nutzer mit gleicher Geräteart alle Datenströme das jeweils korrekte Gerät erreichen, liegt an weiteren übertragenen Metadaten (beispielsweise der individuellen Gerätenummer IMEI), die die Geräte zur eindeutigen Identifizierung aussenden.

95 Die zugrundeliegende technische Idee wurde im Juni 2011 als sogenannter Request for Comments Nr. 6264 (RFC 6264) erstmals publiziert und erst im Anschluss daran zur konkreten Anwendung weiterentwickelt.

Knappheit verfügbarer IP-Adressen ab.[96] Die Dienstleister, die die dynamischen IP-Adressen vergeben, sind daher dazu übergegangen, zeitgleich eine einzige Adresse mehreren Anschlüssen zuzuordnen. Dies geschieht im Rahmen der sogenannten Carrier-Grade-Network Address Translation (CGN),[97] wodurch einer einzigen IP-Adresse gleichzeitig bis zu mehrere Tausend Anschlüsse zugeordnet werden.[98]

96 Nach derzeitiger Prognose dürfte eine solche Knappheit mit Umstellung aller Adressen-Vergeber auf die IPv6-Technik in Zukunft ausgeschlossen sein (vgl. Europol, *Pressemitteilung vom 02.02.2017;* Bundesministerium für Wirtschaft und Technologie, *Strategiepapier zur Förderung der Einführung von IPv6*, S. 5). Wegen der erheblichen Kosten erfolgt die Umstellung jedoch nur sehr schleppend und wird flächendeckend vermutlich erst „in einigen Jahren“ abgeschlossen sein (Bundesministerium für Wirtschaft und Technologie, *Strategiepapier zur Förderung der Einführung von IPv6*, S. 13).

97 Die korrekte Datenstromzuordnung erfolgt anhand weiterer Metadaten, die den Ermittlungsbehörden grundsätzlich nicht bekannt sind.

98 Europol, *Pressemitteilung vom 02.02.2017*; laut Europol, *Pressemitteilung vom 17.10.2017*, nutzen derzeit 90% der Mobilfunknetz-Betreiber und 50% der Festnetz-Betreiber die CGN-Technologie.

II. Verwertung eines Datensatzes

1. Dechiffrierung der 0 - 1 Notation (insbesondere: OSI-7-Schichten Modell)

Jeder elektronische Datensatz muss, bevor er einer nicht-automatisierten Bewertung zugänglich ist, von der 0 – 1 Notation dechiffriert werden. Erst nach diesem Vorgang, der gegebenenfalls mehrstufig sein kann, ist ein Datensatz verwertbar.[99]

Die Dechiffrierung geschieht üblicherweise durch Protokolle, also Software, die auf unterschiedlichen Ebenen ablaufen. Dabei wird der Dateninhalt häufig mehrfach chiffriert und dechiffriert. Bei Zugrundelegung des OSI-7-Schichten Modells,[100] das als Referenzmodell für Netzwerkkommunikation anerkannt ist, unterliegt beispielsweise die externe Speicherung eines Nutzer-Dokumentes in vereinfachter Darstellung folgenden Umwandlungsprozessen:

Auf der Anwendungsschicht erfolgt die Eingabe des Bildes oder des gesprochenen oder geschriebenen Textes über ein Anwenderprogramm, also beispielsweise über ein Textverarbeitungsprogramm (Microsoft Word, Open Office etc.), über ein E-Mail-Programm oder über einen Webbrowser.
Diese Klardaten werden sodann erstmals umgewandelt für die weiterverarbeitende Darstellungsschicht in eine systemunabhängige Datendarstellung, beispielsweise im ASCII-Code, in dem jedem Zeichen ein Bitmuster aus 7 beziehungsweise 8 Bits zugeordnet wird.[101]
Die folgende Sitzungsschicht sorgt für den störungsfreien Ablauf der Prozesskommunikation, also für einen organisierten und synchronisierten Datenaustausch.
Sie wird ergänzt von der Transportschicht, die den eigentlichen

---

99 Die Verwertung als Beweismittel erfolgt im deutschen Strafprozess derzeit normalerweise mittels eines Ausdrucks im Wege des Urkundenbeweises bei verlesbaren Inhalten oder mittels eines Augenscheinbeweises (vgl. Sieber, *Gutachten zum 69. DJT*, S. 67, m.w.N.).

100 Zu allen folgenden Ausführungen zum OSI-7-Schichten Modell siehe Wikipedia, Suchbegriff *OSI Schichtmodell.*

101 Wikipedia, Suchbegriff *ASCII.*

Datenstrom durch Erstellung von Datenpaketen regelt.
Auf der Vermittlungsschicht werden die Datenpakete sodann fragmentiert, um über verschiedene Netzwerkknoten als Gesamtheit zum Empfänger zu gelangen. Auf dieser Schicht kommt das Internet Protokoll, IP, zum Einsatz, hier werden die IP-Adressen relevant.
Ziel der Sicherungsschicht ist die fehlerfreie Datenübertragung, was unter anderem durch die Aufteilung des Bitdatenstromes und dem Hinzufügen von Prüfsummen gewährleistet werden soll; fehlerhafte Blöcke können dadurch beim Empfänger erkannt werden.
Die unterste Schicht im Modell ist die Bitübertragungsschicht, die mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung stellt, um tatsächliche Verbindungen zu aktivieren beziehungsweise zu deaktivieren und dadurch Bits als elektrische oder optische Signale, elektromagnetische Wellen oder Schall zu übertragen.
Im Anschluss an die Bitübertragung laufen die Prozesse sodann in umgekehrter Reihenfolge, um bei Empfänger wieder in benutzerfreundlicher Form zur Verfügung zu stehen. Handelt es sich beim Empfänger um den zur Speicherung verpflichteten Dienstleister, bedarf es nunmehr intern der Umwandlung der empfangenen Daten in eine speicherfähige 0 – 1 Notation.

Das Modell ist im Grundsatz auf alle Arten von Netzwerk-Kommunikation anwendbar, insbesondere auch auf mündliche Kommunikation, wo das gesprochene Wort letztlich auch in ein 0 - 1 Signal umgewandelt, als solches übertragen und schließlich beim Empfänger als Ton wiedergegeben wird. In der Telekommunikation stellt die Übertragung des gesprochenen Wortes über das Internet (englisch: „Voice over IP“, „VoIP“) mittlerweile die Standardübertragungstechnik dar.

2. Unterschiedliche Datenformate

Die Ermittlungsbehörden erhalten elektronische Datensätze in ganz unterschiedlichen Formaten, je nachdem, ob es sich bei den Datenquellen beispielsweise um Hauscomputer, Mobilfunkgeräte,

Telekommunikationsüberwachungstechnik, Basisstationen der Telekommunikationsbetreiber, Videoüberwachungskameras, Buchhaltungssysteme, medizinische, technische oder chemische Laborapparate, Bankkonten, soziale Netzwerke, Streamingdienste oder Internetplattformen handelt.[102] Zudem werden auch innerhalb einer Datenquelle nicht zwingend einheitliche Datenformate verwendet.[103]

Hinzu kommt, dass elektronische Daten als Sammelbegriff originär digitale Daten[104] ebenso umfassen wie ursprünglich analoge und sodann digitalisierte Daten[105] sowie digitalisierte Nicht-Daten[106].[107] Selbst Daten, die von einer deutschen Behörde an eine andere übermittelt werden, sind teilweise nicht direkt nutzbar, weil der Bund und die Bundesländer für manche Bereiche ihre eigene, nicht mit anderen kompatible IT-Infrastruktur aufgebaut haben.

Daneben liegen zu bestimmten Datenpaketen häufig automatisiert erzeugte Metadaten vor, die als solche zunächst nicht sichtbar sind. Das gilt beispielsweise schon bei Aufnahmen mit einer herkömmlichen Digitalkamera, bei der zu den eigentlichen Bilddaten in der Standardeinstellung auch Kameratyp, Aufnahmedatum und Aufnahmeort als Metadaten gespeichert werden.

Schließlich kann aus den Resten eines bereits gelöschten Datensatzes dieser mit entsprechenden technischen Hilfsmitteln häufig rekonstruiert werden, solange er nicht vollständig vernichtet oder

---

102 Im Hinblick auf die Telekommunikationsdienstleister wäre daran zu denken, eine Standardisierung über das Europäische Institut für Telekommunikationsnormen (ETSI) zu erreichen. Dessen Ziel ist die Schaffung weltweit anerkannter Standards für die Informations- und Kommunikationstechnologien, wobei das Institut einen Cluster „Security“ hat, der sich speziell mit technischen Aspekten der Telekommunikationsüberwachung („lawful interception“) und der Datenspeicherung („retained data“) befasst (vgl. ETSI, *Security*, S. 3).

103 Allein ein Smartphone arbeitet mit unterschiedlichen Datenformaten für SMS-Nachrichten, E-Mails, Anruflisten, Bilder, Videos, Kalendereinträge, Adressbucheinträge, Passwörter etc.

104 Wie beispielsweise die Metadaten einer konkreten Internetnutzung oder die Verbindungsmerkmale eines Mobilfunkanrufes.

105 Wie beispielsweise ein eingescanntes Dokument.

106 Wie beispielsweise die Digitalaufnahme eines Gegenstandes (zum Beispiel der Tatwaffe), der als solches nicht unter die Bezeichnung „Daten“ fällt.

107 Vgl. EVIDENCE Project, *Roadmap*, S. 23.

beseitigt wurde.

3. Bewusste Verschlüsselung

Im Zusammenhang mit der zur Visualisierung ohnehin erforderlichen Dechiffrierung elektronischer Daten weisen diese zunehmend das Merkmal auf, dass ihr Inhalt aus Sicherheitsgründen oder zur Verschleierung einer Straftat ganz gezielt standardmäßig anonymisiert oder verschlüsselt wird.[108]

Um eine Entschlüsselung vorzunehmen, bedarf es entweder des Schlüssels,[109] des Zugriffes auf das Gerät, in das die Klardaten vom Absender vor ihrer Verschlüsselung eingegeben beziehungsweise nach ihrer Entschlüsselung beim Empfänger ausgegeben werden, oder des Ausprobierens möglichst vieler Lösungsmöglichkeiten.[110] In Abhängigkeit vom gewählten Ansatz sind enorme Rechnerkapazitäten erforderlich, um etwa ein Passwort zu dechiffrieren.

---

108 Europol, *IOCTA* 2017, S. 63; laut Europol, *IOCTA 2016*, S. 46, werden vor allem IP-Adressen durch die Nutzung von Proxies, TOR-Netzwerken und VPN-Verbindungen anonymisiert, während die Verschlüsselung auf alle Arten von Daten Anwendung findet und viele kommerzielle Kommunikationsplattformen sie standardmäßig anwenden.
Zur Bedeutung der Verschlüsselung aus Sicherheitsgründen vgl. Europäische Kommission / Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, *Gemeinsame Mitteilung*, 13.09.2017, S. 12: „Eine leistungsstarke Verschlüsselung ist die Grundlage sicherer digitaler Identifizierungssysteme, die für eine wirksame Cybersicherheit von zentraler Bedeutung sind“; Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (242).

109 Bei der weitverbreiteten Gruppe der asymmetrischen Verschlüsselungstechnik, wie sie beispielsweise WhatsApp seinen Nutzern standardmäßig als Ende-zu-Ende Verschlüsselung anbietet, wird bildlich übertragen nicht nur ein Schlüssel, sondern vielmehr ein Schlüsselpaar verwendet: der öffentliche Schlüssel, der allen Kommunikationspartnern zur Verschlüsselung ihrer Nachricht frei zugänglich bereitgestellt wird, und der private Schlüssel, der allein beim Berechtigten verbleibt und zur Entschlüsselung dient. Stark vereinfacht dargestellt, wird bei der Ende-zu-Ende Verschlüsselung ein Zeichensatz durch eine mathematische Funktion, den Verschlüsselungsalgorithmus, nach Angaben des Schlüssels verschlüsselt und durch Anwendung der Umkehrfunktion wieder entschlüsselt.

110 Die sogenannte Brute-Force Methode, gegebenenfalls unter Verwendung von Wörterbüchern, findet insbesondere dann Anwendung, wenn es darum geht, ein einzelnes Passwort zu dechiffrieren. Dies kann automatisiert geschehen und erfordert mit zunehmender Passwortlänge und der Verwendung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen exponentiell steigende Rechnerleistungsfähigkeiten.

4. Manipulationsanfälligkeit elektronischer Daten

Wie soeben dargelegt, können einfache Programmierfehler auf verschiedenen Stufen der Datenverarbeitung und insbesondere auf dem Übertragungsweg auftreten. Das unterscheidet sie wesentlich von den herkömmlichen Beweismitteln, denen diese Gefahr nicht immanent ist, weil sie während ihres Transportes keinem Verarbeitungsprozess unterliegen. Zur Klarstellung: selbstverständlich können auch Augenscheinsobjekte und Schriftstücke verarbeitet oder verändert werden, ihre Beweiskraft bezieht sich aber grundsätzlich nur auf einen bestimmten Zustand oder eine bestimmte Form zu einem konkreten Zeitpunkt; ein Hin- und Herwechseln der äußerlichen Erscheinungsform hat unmittelbar Einfluss auf ihren Beweisinhalt.

Außerdem ist zu berücksichtigen, dass die Visualisierung eines elektronischen Datensatzes, also etwa der Ausdruck eines Bildes oder eines Textverlaufes, die Metadaten nicht erfasst. Sie müssen gesondert visualisiert und eindeutig mit dem visualisierten Kerndatensatz verknüpft werden.

Daneben weisen elektronische Daten im Vergleich zur Zeugenaussage, zur Inaugenscheinnahme von Bildern und sonstigen Objekten und zu Schriftstücken im Allgemeinen eine erhöhte Manipulations- oder Datenverlustanfälligkeit auf.[111]
Das liegt zum einen daran, dass die Veränderung einschließlich der Löschung eines Datensatzes bei entsprechender technischer Zugangsmöglichkeit grundsätzlich von überall aus erfolgen kann; es ist nicht erforderlich (und wenn es um eine Speicherung auf Großrechnern beziehungsweise um gesplittete Datensicherung geht: noch nicht einmal sinnvoll), sich zum Speicherort zu begeben, um einen Datensatz zu verändern.

111 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 7; Europäische Kommission, *Progress Report,* 07.12.2016, S. 11; EVIDENCE Project, *Roadmap*, S. 15; BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 240.

Zum anderen erfordert eine Datenmanipulation, wenn man von dem Erwerb eines entsprechenden Werkzeugs, also eines Rechners mit dem notwendigen Hardware- und Software-Zubehör, absieht, keinen großen finanziellen oder faktischen Aufwand. Zum Teil genügt es sogar, für die dauerhafte Löschung die Stromzufuhr für einen Moment zu unterbinden,[112] was im wahrsten Sinne des Wortes mit einem Handgriff erfolgen kann.

Desweiteren kann selbst eine unbewusste Datenveränderung oder -löschung häufig in einer Art und Weise erfolgen, dass, anders als bei Veränderungen von Gegenständen, weder der Änderungsvorgang noch die Änderung an sich im Nachhinein nachvollzogen werden können. Das betrifft auch die Fälle, in denen die Strafermittlungsbehörden selbst und unmittelbar auf die elektronischen Rohdaten Zugriff haben und die Dechiffrierung unter ihrer Regie erfolgt. Aus technischer Sicht ist es beispielsweise sehr schwierig, nachzuweisen, dass ein aus der Cloud heruntergeladener Datensatz absolut identisch mit demjenigen ist, der ursprünglich dort abgelegt wurde.[113] Dies liegt unter anderem an der häufig automatisierten, gesplitteten und dynamischen Speicherung,[114] die Änderungsmöglichkeiten schafft, die weit über das hinausgehen, was unter der Erforderlichkeit der Dechiffrierung bereits als problematisch beschrieben wurde.

Schließlich ist zu berücksichtigen, dass, wie bereits geschildert, bei der Sicherung der Daten grundsätzlich der Original-Datensatz beim ursprünglichen Dateninhaber verbleibt. Es kann nicht ausgeschlossen werden, dass dieser seinen Datensatz bewusst verändert und sodann im Ermittlungsverfahren präsentiert, um Einfluss auf die Beweisführung zu nehmen.

112 Das betrifft etwa alle Daten, die im Arbeitsspeicher (RAM) temporär abgelegt werden (s. Wikipedia, Suchbegriff *Random Access Memory*).
113 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 23.
114 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 24.

5. Big Data

Der Begriff Big Data folgt keiner klaren Definition, wird aber für gewöhnlich auf das Phänomen der massenhaften Datenverfügbarkeit bezogen, die sich aus der Menge der vorhandenen elektronischen Daten, ihrer Generierungs- und Übermittlungsgeschwindigkeit sowie ihrer Herkunftsbereiche ergibt.[115]

Die Masse der vorhandenen Daten resultiert zum einen aus der Vielzahl an unterschiedlichen Datenquellen, die bereits beispielhaft aufgezeigt wurden.

Auch dringt die elektronische Datenverarbeitung stetig in immer weitere Lebensbereiche des Alltags vor. Erinnert sei in diesem Zusammenhang für den Bereich des Privatlebens etwa an schriftliche Korrespondenz, die, falls sie nicht ohnehin papierlos erfolgt, in der Regel jedenfalls beim Verfassen eines Schriftstückes am Computer geschieht, elektronische Fotografie- und Videoaufnahmen, Internet-telefonie und Teilnahme an sozialen Medien, die Nutzung von Multimedia-Streamingdiensten, online-Banking, Navigationssysteme im Auto, bargeldloses Bezahlen, personalisierte Ratgeber im Gesundheits-bereich und Kleinrechner wie kommunizierende Fitnessbänder oder Multifunktionsuhren. Berufsbezogen werden nicht nur sämtliche Personal-, Firmen- und Produktionsdaten elektronisch gespeichert, sondern auch zunehmend digitale Zugangs- und Zeiterfassungs-systeme installiert. Im öffentlichen Bereich fallen elektronische Daten bei der Finanzverwaltung und den KfZ-Zulassungsstellen ebenso an wie bei den Personenstandsämtern und Krankenkassen. Die Videoüberwachung öffentlicher Plätze liefert zudem große Mengen entsprechenden Bildmaterials.

Schließlich hat sich in den letzten Jahren ein neues Geschäftsmodell von hohem kommerziellen Wert[116] entwickelt, in dem Nutzerdaten nicht nur einfach verarbeitet, also übermittelt oder gespeichert werden,

115 Wikipedia, Suchbegriff *Big Data*; vgl. auch Sieber, *Gutachten zum 69. DJT*, S. 10.
116 Sieber, *Gutachten zum 69. DJT*, S. 10, 28, m.w.N.

sondern mithilfe von Algorithmen beispielsweise Bewegungs-[117], Wähler-[118] oder Kundenprofile[119] erstellt und gewinnbringend vermarktet werden.[120] Die Datengewinnung erfolgt in der Regel dadurch, dass der Nutzer einer Übermittlung und Verarbeitung seiner Daten über Allgemeine Geschäftsbedingungen zustimmt, ohne genau zu wissen, welche Daten davon betroffen sind und was mit den gewonnenen Informationen konkret geschieht.[121]
Daneben führt die zunehmende Vernetzung mit internetfähigen Geräten, die unter der Bezeichnung Internet der Dinge (Internet of Things – IoT) bereits mit einem festen Begriff umschrieben wird, unmittelbar zur Entstehung enormer Datenmengen.[122]

All diese Entwicklungen haben dazu geführt, dass die Zeitspanne, in der sich das Datenvolumen verdoppelt, derzeit bei 18 Monaten liegt; das Datenvolumen, das im Laufe des gesamten Jahres 2000 produziert wurde, wird heute im Laufe eines einzigen Tages erzeugt.[123]

---

117 Zur zunehmenden Bedeutung von Bewegungsprofilen vgl. Spehr, *Jeder Schritt zählt*.

118 Das britische Unternehmen Cambridge Analytica ist in diesem Zusammenhang 2016 gleich zwei Mal in Erscheinung getreten: als Dienstleister für die Brexit-Befürworter und als Wahlkampfhilfe für Donald Trump im US-Präsidentschaftswahlkampf (vgl. Wikipedia.org, Suchbegriff *Cambridge Analytica*; kritisch zur entsprechenden Berichterstattung darüber: Reinbold / Schnack, *Ich ganz allein habe Trump ins Amt gebracht*).

119 Bei Kundenkartenprogrammen wie beispielsweise Payback werden in der Regel aus den angegebenen persönlichen Daten und sämtlichen Details aller Umsätze das Kaufverhalten analysiert und sodann „individuell zugeschnittene Angebote“ unterbreitet (vgl. Payback GmbH, *Einwilligungserklärung zur Datenverarbeitung*). Zur Bedeutung solcher Kundenprofile, durch die bereits heute intelligente Einkaufsassistenten, Inhouse-Navigationssysteme, dynamische Preisschilder, individuelle Rabatte und persönliche Produktvorschläge generiert würden: Spehr, *Datenauswertung*, *Die Macht der Algorithmen*.

120 Zur wirtschaftlichen Bedeutung solcher Profile allgemein vgl. Spehr, *Jeder Schritt zählt*.

121 Sieber, *Gutachten zum 69. DJT*, S. 28 f., 129.

122 Schätzungen zufolge sollen im Jahr 2020 mehr als 20 Milliarden Geräte über das Internet vernetzt sein (s. Jansen, *Der große Kampf um das Internet*). Da sie häufig nicht über besondere Zugriffssicherungen verfügen, kann ihre jeweils geringe Rechnerkapazität relativ einfach in ein schlagkräftiges Botnetz integriert werden (vgl. Europol, *IOCTA 2017*, S. 10).

123 Spehr, *Datenauswertung*, *Die Macht der Algorithmen*.

C. Notwendigkeit und Vorhandensein gesetzlicher Regelungen zum strafprozessualen Umgang mit elektronischen Beweismitteln

In diesem Kapitel wird untersucht, inwieweit die fehlende Körperlichkeit, die elektronische Daten von Gegenständen unterscheidet, rechtliche Relevanz hat (dazu unter I.). Dies ist erheblich, weil nach verfassungsrechtlichen Vorgaben nur rechtlich relevante Gründe eine gesonderte gesetzliche Behandlung bestimmter Regelungsobjekte erlauben.

Es folgt sodann eine Darstellung der derzeit vorhandenen datenspezifischen Regelungen in der StPO (II.), der Fälle ihrer analogen Anwendungen (III.) und schließlich der bestehenden supranationalen Normierungen zum Umgang mit elektronischen Daten im Strafprozess (IV.).

Auf dieser Grundlage werden verbleibende Regelungslücken herausarbeitet (V.) und praktische Lösungsansätze dargestellt (VI.).

Dem auf das deutsche Recht fokussierten Kapitel folgt abschließend ein Exkurs zur vergleichbaren Gesetzeslage in den übrigen Mitgliedstaaten der Europäischen Union.

I. Unkörperlichkeit elektronischer Daten als strafprozessuales Phänomen[124]

Dass elektronische Daten nicht greifbar und damit unkörperlich sind, ist unbestritten. Allerdings wird insbesondere von Woods[125] vertreten, dass sie zum einen als unkörperliche Beweismittel keine Neuartigkeit im Prozessrecht darstellten und sie zum anderen körperliche Merkmale aufwiesen.[126] Damit könne die Strafverfolgungsbehörde für die Erlangung grenzüberschreitend gespeicherter elektronischer Daten auf althergebrachte Rechtsgrundsätze zurückgreifen – wahlweise auf die, die unkörperliche Beweismittel beträfen, oder auf diejenigen, die für körperliche Gegenstände Anwendung fänden.[127]

Woods argumentiert, dass elektronische Daten, jedenfalls wenn sie nicht mit einem territorial-verbundenen Speichermedium verknüpft seien,[128] nicht viel anders als andere Formen unkörperlicher Objekte wären, mit denen das Strafprozessrecht seit vielen Jahren als

---

124 Eine ausführlichere Auseinandersetzung mit Woods` Thesen, auf der die folgenden Ausführungen basieren, findet sich bei Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 4, NZWiSt 2017, 449 (449 f.); vgl. auch Clopton, *Data Institutionalism: A Reply to Andrew Woods*, Stanford Law Review Online, Volume 69, July 2016, S. 9; Svantesson, *Against ‚Against Data Exceptionalism',* 2016 Masaryk University Journal of Law and Technology, S. 200.

125 Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law, der nach eigenen Angaben im April 2016 den ersten Artikel veröffentlicht hat, der sich mit der Anwendung althergebrachter Rechtsprechungsgrundsätze („longstanding jurisdictional principles") auf die Erlangung von elektronischen Beweismitteln in der Cloud befasst (vgl. Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (737)).

126 Zwar legt Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729, den Schwerpunkt seiner Ausführungen ausschließlich auf die Problematik der Erlangung von elektronischen Beweismitteln aus der Cloud, seine Ausführungen zu den Wesensmerkmalen solcher Daten sind jedoch allgemein gehalten und daher auch für die vorliegende Arbeit beachtlich.
Soweit nicht anders kenntlich gemacht, stehen die folgenden Zitate von Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729, immer im Kontext der Problematik der Datenerlangung aus der Cloud.

127 So ausdrücklich Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (763).

128 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (734 f.), spricht von Daten, die sich im „free-floating ether" befänden.

Beweismittel zu tun habe.[129] Als Beispiele solch unkörperlicher Beweismittel nennt er Geld,[130] geistiges Eigentum,[131] Schulden[132] und Unternehmens- / Geschäftsanteile,[133] um sodann darzulegen, dass die Gerichte in der Vergangenheit hinreichend Rechtsgrundsätze zur Erlangung dieser vermeintlichen Beweismittel entwickelt hätten.[134]

Die Argumentation überzeugt nicht: Zum einen verwendet Woods den Begriff „Geld“ sowohl für das jeweils dahinterstehende Recht, also beispielsweise eine Rückzahlungsforderung gegen die Bank, bei der Geld eingezahlt wurde,[135] als auch für die materielle Verkörperung zum Nachweis dieses Rechts, also für die Geldscheine und Münzen als solche.[136] Die letztgenannte Kategorie bezieht sich unzweifelhaft auf körperliche Gegenstände, die in der Vergangenheit strafprozessual mitnichten als unkörperliche Gegenstände behandelt wurden.

Die erstgenannte Kategorie, Geld als Forderung, bezieht sich wie alle übrigen Beispiele auf Rechte und Verpflichtungen. Dies sind rechtliche Konstrukte, damit zutreffend unkörperlich, aber keine Beweismittel. Ob Rückzahlungsansprüche, geistiges Eigentum, Rückzahlungsverpflichtungen oder Anteilsrechte bestehen, ist Ergebnis einer rechtlichen Würdigung.
§ 244 Abs. 2 StPO betont die Zielrichtung jeder Beweisaufnahme, die in der Erforschung der Wahrheit und damit in der Feststellung von Tatsachen liegt. Weder die Entstehung eines Rechts oder einer rechtlichen Verpflichtung, seine Zuordnung zu einer bestimmten Person,

---

129 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (734 f.).
130 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (729, 758 ff.): „money“.
131 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (735, 757): „intellectual property“.
132 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (729, 735, 756 ff., 761): „debts“.
133 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (756 f., 760 f.): „stocks“.
134 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (763 ff.).
135 Zu dieser Begriffsverwendung s. beispielsweise Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (729, 758).
136 Zu dieser Begriffsverwendung s. beispielsweise Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (759).

sein Erlöschen noch das Recht an sich sind „wahr“ oder „tatsächlich“, sie stellen vielmehr rechtliche Würdigungen dar, die aufgrund bestimmter Tatsachen getroffen werden und sodann weitere Rechte oder rechtliche Verpflichtungen begründen können. Elektronische Daten hingegen sind kein rechtliches Konstrukt, sondern ein technisches Etwas, eine Verkörperung einer Information, die ihrerseits auf tatsächliche Vorgänge rückschließen lässt.

Zur Begründung der weitergehenden Behauptung, dass elektronische Daten körperliche Eigenschaften aufwiesen, verweist Woods darauf, dass elektronische Daten in der Cloud auf körperlich vorhandenen Servern gespeichert seien.[137]
Das trifft aber jedenfalls für Daten, die aktuell in der Cloud verarbeitet werden oder sich im Übermittlungsprozess befinden, erkennbar nicht zu; elektronische Beweismittel sind nicht auf gespeicherte Datensätze reduziert. Zudem ist nicht nachvollziehbar, wieso ein elektronischer Datensatz trotz seiner abweichenden, herausragenden Charakteristika mit einem materiellen Speichermedium rechtlich oder tatsächlich gleichzusetzen sein soll.

Im Hinblick auf die bereits ausführlich dargestellten tatsächlichen Besonderheiten elektronischer Beweismittel lässt sich entgegen Woods Folgendes feststellen:

Der überwiegende Teil der Besonderheiten elektronischer Beweismittel, die allesamt auf ihre Unkörperlichkeit zurückzuführen sind, namentlich die unterschiedlichen Übermittlungsarten, das grundsätzliche Verbleiben des Originals beim Dateninhaber, die unterschiedlichen Datenverarbeitungs- und -speicherorte, das Dechiffrierungserfordernis, die Manipulationsanfälligkeit und das Big Data-Phänomen, erfordern jeweils im Einzelnen spezifische strafprozessrechtliche Normierungen.[138] Nur dadurch kann den Prinzipien des Strengbeweisverfahrens,

137 Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (734 f., 763 und explizit auf S. 761): „data resides on physical drives“.

138 Die weiteren genannten Besonderheiten erfordern für einen verbesserten Umgang mit ihnen vor allem mehr personelle und materielle Ressourcen (so der Zeitfaktor und die unterschiedlichen Datenformate) beziehungsweise vorab eine grundsätzliche politische Entscheidung über

dem strafprozessrechtlichen Unmittelbarkeitsgrundsatz für alle Beweismittel, den grenzüberschreitenden Problemen, die regelmäßig mit Daten „in der Cloud“ auftreten, dem besonderen Bedürfnis nach Sicherung der Integrität und Authentizität eines elektronischen Beweismittels und dem bei großen Datenmengen faktisch nicht mehr zu erfüllenden Auftrag umfassender Sachverhaltsaufklärung Genüge getan werden.

Das gilt erst recht, wenn man die Besonderheiten in ihrer Gesamtheit betrachtet.[139]

Entgegen Woods kann für die aufgeworfenen strafprozessuale Probleme bei elektronischen Daten nicht generell auf althergebrachte Rechtsgrundsätze oder Rechtsanwendungsfälle zurückgegriffen werden;[140] die Besonderheiten sind in ihrer Gesamtheit zu speziell und tatsächlich andersartig.

---

ihre Dringlichkeit (so im Hinblick auf die Ortsungebundenheit des Zugriffes, die Anonymität im Netz und die Verschlüsselung).
Für eine ausführliche Herleitung der jeweiligen Handlungserfordernisses aufgrund der genannten jeweiligen Besonderheiten s. Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 4, NZWiSt 2017, 449 (450 ff.).

139 Sieber, *Gutachten zum 69. DJT*, S. 83, sieht im Zusammenhang mit elektronischen Daten „erhebliche[n] Handlungsbedarf, besonders beim Strafprozessrecht“; ebenfalls für einen gesetzgeberischen Handlungsbedarf: Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 9 f. zitiert nach juris); EVIDENCE Project, *Roadmap*, S. 23 (allgemein für die Strafprozessordnungen der EU-Mitgliedstaaten).

140 Bemerkenswerterweise plädiert Woods zwar nachdrücklich für die Anwendung althergebrachter Rechtsgrundsätze auf die Erlangung elektronischer Daten aus der Cloud und zeigt die vermeintliche Möglichkeit für die Gerichte auf, je nach Problemstellung auf die Regelungen für körperliche oder unkörperliche Beweismittel zurückzugreifen (Woods, *Against Data Exceptionalism,* Stanford Law Review, Volume 68, April 2016, S. 729 (763)). Er stellt aber zugleich fest, dass seine Herangehensweise die durch die Charakteristika der elektronischen Daten aufgeworfenen prozessualen Probleme nicht löse (Woods, a.a.O., S. 735, 781), sondern es dafür vielmehr eines Tätigwerdens des Gesetzgebers bedürfe (Woods, a.a.O., S. 781). Ebenfalls für die Unanwendbarkeit der Regeln für körperliche Beweismittel auf elektronische Daten: Sieber, *Gutachten zum 69. DJT*, S. 14.

II. Explizite Regelungen

Verglichen mit der strafprozessualen Relevanz elektronischer Daten als Beweismittel finden sich in der StPO nur wenige spezifische Vorschriften. Sie werden im Folgenden kurz vorgestellt,[141] wobei sich der Fokus der Darstellung insbesondere darauf richtet, ob und gegebenenfalls nach welchen Kriterien eine Norm elektronische Daten klassifiziert.

Die erstmalige Erwähnung erfolgt überraschenderweise in dem 2005 eingefügten und bis 31.12.2017 geltenden § 41a StPO und betrifft die Kommunikation zwischen den Prozessbeteiligten.[142] Sie gibt die technischen Rahmenbedingungen vor, unter denen Dokumente in elektronischer Form an Gerichte und Staatsanwaltschaften übermittelt werden können. Ihr zufolge sind Dokumente, die nach sonstigen Vorschriften der StPO schriftlich abzufassen oder zu unterzeichnen sind, mit einer qualifizierten elektronischen Signatur zu versehen (Abs. 1 S. 1). Gemäß Abs. 1 S. 2 der Norm kann statt der qualifizierten elektronischen Signatur per Rechtsverordnung auch „ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten Dokuments sicherstellt".[143] Die Regelung bezieht sich somit nicht auf elektronische Beweismittel, sondern auf Informationen, die im Rahmen eines Strafverfahrens zwischen den Prozessbeteiligten ausgetauscht werden. Sie ist in ihrem Anwendungsbereich eng auf solche Daten beschränkt, deren Inhalt ein Verfahrensdokument zum Gegenstand haben, und bleibt daher bei der weiteren

141 Eine ausführliche Darstellung zu diesem Thema findet sich bei Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 2, NZWiSt 2017, 329 (333 ff.).

142 Die Norm wurde durch das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22.03.2005, BGBl. I S. 837, in die StPO eingefügt.

143 Die Gesetzesbegründung (BT-Drucks. 15/4067, S. 37) sieht vor, dass es „zur Sicherung der Integrität des Dokuments [...] notwendig [ist], dass die Übermittlung der Dokumente mittels kryptografischer Verfahren erfolgt, die mindestens auf den ‚Standards und Architekturen für eGovernment-Anwendungen (SAGA)' in der jeweils aktuellen Fassung beruhen. Dem Verordnungsgeber wird dadurch zum Beispiel die Möglichkeit eröffnet festzulegen, dass [...] bestimmte Protokolle zu verwenden sind. Ferner ist sicherzustellen, dass das übermittelte Dokument bei dem Eingang beim Gericht so gespeichert wird, dass seine Integrität für die Zeit der Speicherung überprüfbar ist".

Untersuchung außer Betracht.

Während sich § 81h Abs. 1 Nr. 3 StPO auf den automatisierten Abgleich von DNA-Identifizierungsmustern bezieht, regeln die §§ 98a, 98b und 98c StPO den maschinellen Abgleich von sonstigen personenbezogenen Daten im Rahmen der Rasterfahndung beziehungsweise mit weiteren, bereits vorhandenen personenbezogenen Daten. Anders als im Datenschutzrecht, wo der identische Begriff der personenbezogenen Daten gesetzlich definiert wird,[144] differenzieren die genannten Vorschriften indirekt zwischen personenbezogenen und nicht-personenbezogenen Daten, ohne dass das Unterscheidungsmerkmal in der StPO weiter erläutert würde.[145]

Ein mittelbarer Bezug zu elektronischen Daten ergibt sich aus § 97 Abs. 5 S. 1 StPO, der ein Beschlagnahmeverbot unter anderem von Datenträgern, die sich im Gewahrsam von zeugnisverweigerungsberechtigten Personen befinden, normiert.

Daneben erlaubt § 110 Abs. 3 StPO die Durchsicht eines elektronischen Speichermediums bei dem von einer Durchsuchung Betroffenen, die auch auf hiervon räumlich getrennte Speichermedien erstreckt werden darf, soweit auf sie von dem Speichermedium aus zugegriffen werden kann und andernfalls ein Datenverlust zu befürchten wäre; entsprechende Daten dürfen zudem gesichert werden. Die Norm erweitert somit den räumlichen Bereich einer Durchsuchung insbesondere auf Speichermedien in der Cloud, solange sich deren Server in Deutschland befinden.[146] Die Durchsicht dient einer vorläufigen Auswahl der Daten, über deren Sicherstellung oder

144 Vgl. Art. 3 Nr. 1 DS-Richtlinie Strafjustiz, Art. 4 Nr. 1 DS-GVO und § 3 Abs. 1 BDSG.

145 Auch die Gesetzesbegründung zur ursprünglichen Fassung der §§ 98a ff. StPO liefert keine nähere Begriffsbestimmung, sondern referiert nur auf den weiteren Gesetzestext, der von „Daten von Personen, die bestimmte […] Prüfungsmerkmale erfüllen“ spricht (BT-Drucks. 12/989, S. 36 ff.). Laut Menges, in: Löwe-Rosenberg, *StPO*, § 98a, Rn. 3 (zitiert nach juris), sei die Begriffsbestimmung des § 3 Abs. 1 BDSG zugrundezulegen.

146 Da es sich bei § 110 Abs. 3 StPO um eine rein nationale strafprozessuale Befugnisnorm handelt, deren Regelungsbereich sich auf das Hoheitsgebiet des bundesdeutschen Staates beschränkt, wird ein Zugriff auf ausländische Server in Form des virtuellen Grenzübertrittes (VGÜ) nicht erfasst (vgl. Gesetzesbegründung, BT-Drucks. 16/5846, S. 63 f.; LG Hamburg, Beschluss vom 08.01.2008, 619 Qs 1/08).

Beschlagnahme anschließend gesondert zu entscheiden ist.[147] Weder § 97 Abs. 5 S. 1 StPO noch § 110 Abs. 3 StPO differenziert näher hinsichtlich der auf dem Datenträger beziehungsweise Speichermedium gespeicherten Daten.

Die aktuellsten, aus grundrechtlicher Sicht bedeutsamsten Regelungen zu elektronischen Daten finden sich in der jüngsten Fassung der §§ 100a ff. StPO.

Durch die Neufassung des § 100a Abs. 1 S. 2 StPO hat der Gesetzgeber im Sommer 2017 ausdrücklich die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) als Ergänzung zur herkömmlichen Telekommunikationsüberwachung und -aufzeichnung eingeführt.[148] Dafür darf nunmehr auch mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen werden, wenn dies notwendig ist, um die Überwachung in unverschlüsselter Form zu ermöglichen. Gemäß Abs. 4 der Norm sind sämtliche Telekommunikationsanbieter, das heißt geschäftsmäßig handelnde Dienstleister ebenso wie Betreiber eines geschlossenen Systems,[149] zur Mitwirkung bei der Überwachungsmaßnahme verpflichtet. Der Wortlaut des § 100a Abs. 4 StPO verweist hinsichtlich der näheren Ausgestaltung der Mitwirkungspflicht auf das TKG und schließt damit beispielsweise alle Informations- und Kommunikationsdienstleister, die, wie etwa WhatsApp oder Skype, nicht dem TKG sondern dem TMG unterliegen, von der Mitwirkungspflicht aus,[150] obgleich sie aus Sicht des Nutzers teilweise identische Dienste anbieten wie die klassischen Telekommunikationsdienstleister, die dem TKG unterfallen.

Technisch erfolgt eine Quellen-TKÜ durch die Infiltration eines informationstechnischen Systems - also etwa durch Ausnutzung von Sicherheitslücken im Zielsystem oder durch Installation eines

147 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 88.
148 Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017, BGBl. I S. 3202, in Kraft seit 24.08.2017.
149 BGH, Beschluss vom 20.08.2015, StB 7/15, Rn. 10 (zitiert nach juris).
150 Vgl. BT-Drucks. 16/3135, S. 2.

Spähprogrammes - zum Zweck der Telekommunikationsüberwachung.[151] § 100a Abs. 5 StPO gibt einige technische Anforderungen an die Überwachungs- und Aufzeichnungssoftware vor, um das Risiko einer versehentlichen oder bewussten, erkennbaren oder nicht erkennbaren Datenveränderung auf dem Zielgerät zu verringern.[152]

§ 100a Abs. 1 S. 2 StPO benennt als Überwachungsobjekt sowohl den Inhalt als auch die Umstände einer laufenden Kommunikation und stellt damit beide Datenkategorien einheitlich auf eine Stufe. Allerdings ist der Kommunikationsbegriff als solcher unklar. Es ist umstritten, ob damit nur die soziale Kommunikation, mithin das kommunikative Sozialverhalten durch mindestens zwei interagierende Personen unter Verwendung eines Telekommunikationsmediums angesprochen wird oder darüberhinausgehend auch sogenannte Mensch-zu-Maschine Kommunikation[153] beziehungsweise Maschine-zu-Maschine Kommunika-

151 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/7 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 5; Gesetzesbegründung, BT-Ausschussdrucks. 18(6)334, S. 18; Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (409 f.).

152 Demnach muss die verwendete Spähsoftware sicherstellen, dass in zeitlicher Hinsicht lediglich solche Kommunikation überwacht wird, die ab dem Zeitpunkt der Anordnung stattfindet (§ 100a Abs. 5 S. 1 Nr. 1b StPO), dass an dem infiltrierten informationstechnischen System nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (Nr. 2), und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden (Nr. 3). Zudem sind gemäß § 100a Abs. 5 S. 2 StPO die eingesetzte Software nach dem Stand der Technik gegen unbefugte Nutzung zu schützen und – ganz pauschal – kopierte Daten gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

153 Mensch-zu-Maschine Kommunikation liegt beispielsweise bei der bloßen Internetrecherche eines Nutzers, dem menschengesteuerten Aufruf einer bestimmten Internetseite oder dem Abruf von in der Cloud gespeicherten Daten durch den Nutzer vor. Entsprechende Informationen können im Einzelfall durchaus für die weiteren strafprozessualen Ermittlungen relevant sein, sodass aus Sicht der Strafverfolgungsbehörden durchaus ein Interesse daran besteht, Zugriff auf solche Daten zu haben. Daneben weisen Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 8, zitiert nach juris), auf die Möglichkeit hin, dass mehrere zugangsberechtigte Personen ein einziges in der Cloud abgelegtes Textdokument dergestalt bearbeiten, dass sie jeweils nur darauf zugreifen, ohne mit den anderen Personen direkt in Kontakt zu treten, aber durch ihre Tätigkeit mittelbar eben doch einen Informationsaustausch untereinander durchführen.

tion,[154] also allgemein der technische Datenaustausch zwischen zwei Telekommunikationsanlagen[155] erfasst wird.[156]

Mit der Einführung des neugefassten § 100b StPO hat der Gesetzgeber ebenfalls im Sommer 2017 gänzlich Neuland betreten, indem er erstmals die online-Durchsuchung als Ermittlungsmaßnahme anerkennt.[157] Der Begriff bezieht sich auf einen verdeckten staatlichen Zugriff auf ein fremdes informationstechnisches System mit dem Ziel, über ein externes Computersystem dessen Nutzung zu überwachen und potentiell sämtliche gespeicherten Inhalte aufzuzeichnen.[158] Regelungsinhalt ist damit die Gewinnung von ausschließlich elektronischen Daten – jeder Art - zu Beweiszwecken, die, ähnlich der Quellen-TKÜ, technisch durch die Implementierung einer Spähsoftware umgesetzt wird. Entsprechend verweist § 100b Abs. 4 StPO hinsichtlich der technischen Anforderungen an die angewandte Software auf § 100a Abs. 5 StPO. Aus Gründen der Verhältnismäßigkeit ist die online-Durchsuchung auf „auch im Einzelfall besonders schwer“ wiegender Taten beschränkt[159] und unter weiteren engen Bedingungen nur subsidiär anwendbar.[160]

§ 100d StPO bestimmt für alle Maßnahmen gemäß §§ 100a ff. StPO einen absoluten Schutz solcher Daten, „die den Kernbereich privater Lebensgestaltung betreffen“. Damit wird ein Begriff aus der

154 Maschine-zu-Maschine Kommunikation, wie sie bereits näher dargestellt wurde, hat heute noch keine besondere strafprozessuale Relevanz. Mit der stetig wachsenden Verbreitung des Internets der Dinge und den dadurch zur Verfügung stehenden Daten wird ihre Bedeutung für die Strafverfolgungsbehörden allerdings signifikant steigen; vgl. nur Heller, *Alexa, war es Mord?*.

155 Zu dieser Umschreibung vgl. Hiéramente / Fenina, *Telekommunikations-überwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 4, zitiert nach juris), m.w.N.

156 Der Meinungsstreit ist höchstrichterlich bislang nicht abschließend geklärt; ausführlich zu den jeweils vertretenen Positionen: Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 4 ff., zitiert nach juris); insbesondere zum Cloud Computing: Sieber, *Gutachten zum 69. DJT*, S. 107.

157 Die online-Durchsuchung wurde ebenfalls eingeführt durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Straf-verfahrens vom 17.08.2017, BGBl. I S. 3202, in Kraft seit 24.08.2017.

158 BT-Ausschussdrucks. 18(6)334, S. 23.

159 § 100b Abs. 1 Nr. 2 StPO.

160 Vgl. BT-Ausschussdrucks. 18(6)334, S. 25.

Rechtsprechung des Bundesverfassungsgerichts aufgegriffen, ohne dass dieser näher konkretisiert wird.[161]

Die Quellen-TKÜ und die online-Durchsuchung erweitern den kleinen Kreis derjenigen Ermittlungsinstrumente, die auf die Gewinnung ausschließlich elektronischer Daten gerichtet sind, und der außerdem noch die §§ 100g, 100i und 100j StPO umfasst.[162]

§ 100g StPO führt den Begriff der Verkehrsdaten in das Strafverfahrensrecht ein und regelt die Voraussetzungen ihrer Erhebung durch die Strafermittlungsbehörden.[163] Aus dem gesetzlichen Verweis auf die abschließende Auflistung des § 96 Abs. 1 TKG ergibt sich, dass es sich bei den Verkehrsdaten um eine Fallgruppe der Telekommunikationsdaten handelt,[164] wobei sich § 100g StPO

161 Die Gesetzesbegründung (BT-Ausschussdrucks. 18(6)334, S. 27) verweist ausweichend darauf, dass „die Frage, ob aufgrund tatsächlicher Anhaltspunkte der Kernbereich privater Lebensgestaltung betroffen sein könnte, […] jeweils konkret vom Gericht unter Berücksichtigung aller Umstände des Einzelfalles zu würdigen“ sei; die frühere Regelung des § 100c Abs. 4 S. 2 StPO a.F., wonach Gespräche in Betriebs- oder Geschäftsräumen in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen waren, sei bewusst nicht übernommen worden.

162 Die §§ 81h Abs. 1 Nr. 3, 98a ff. StPO gehören nicht zu diesem Kreis, weil sie die bereits bestehende Verfügungsgewalt über die abzugleichenden Daten, deren ursprüngliches Format grundsätzlich unerheblich ist, voraussetzen (vgl. Wortlaut des § 81h Abs. 1 Nr. 3 StPO mit Bezugnahme auf „festgestellte DNA-Identifizierungsmuster“ und Gesetzesbegründung zu §§ 98a ff. StPO, BT-Drucks. 12/989, S. 36 ff.). Die zu vergleichenden Daten können dabei ursprünglich in jedem beliebigen Format (beispielsweise in Papierform oder analog gespeichert) vorliegen; es genügt, dass sie für den maschinellen Abgleich digitalisiert werden können.

163 Über den Wortlaut der Norm hinaus soll dadurch auch das IP-Tracking - eine technische Maßnahme, bei der etwa mithilfe von Spähsoftware das infizierte Gerät veranlasst wird, vom Nutzer unbemerkt die aktuell genutzte IP-Adresse an den Überwachenden mitzuteilen - gestattet sein, weil es sich dabei um eine Vorstufe der ausdrücklich erlaubten Erhebung der IP-Adresse handele; vgl. mit weiteren Details: BGH, Beschluss vom 23.09.2014, 1 BGs 210/14, Rn. 4 (zitiert nach juris).

164 § 96 Abs. 1 TKG erfasst abschließend
„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

ausschließlich auf solche Daten bezieht, die in unmittelbarem Zusammenhang mit einem konkreten Kommunikationsvorgang stehen.[165] Abs. 3 der Norm gestattet ausdrücklich die sogenannte Funkzellenabfrage, also die Erhebung aller in einem bestimmten Zeitraum in einer Funkzelle angefallenen Verkehrsdaten. Diese Ergänzung ist erforderlich, weil bei der Funkzellenabfrage regelmäßig auch Daten unbeteiligter Dritter erfasst werden und dafür eine explizite Ermächtigungsgrundlage erforderlich ist.[166] § 101a StPO steht in unmittelbarem Zusammenhang mit § 100g StPO und regelt die formellen Voraussetzungen einer Anordnung zur Erhebung von Verkehrsdaten sowie den Umgang mit dadurch gewonnenen personenbezogenen Daten.

Nach dem Wortlaut des § 100g StPO und dem expliziten Verweis auf die Legaldefinition von Verkehrsdaten im TKG kommt eine Anwendung auf solche Dienstleister, die dem TMG unterliegen, nicht in Betracht,[167] obgleich diese Nutzungsdaten[168] speichern dürfen, die vom Inhalt her eine deutliche Nähe mit den Verkehrsdaten des TKG aufweisen.[169] Da andererseits die §§ 15 Abs. 5 S. 4, 14 Abs. 2 TMG die Übermittlung vorhandener Nutzungsdaten an die Strafverfolgungsbehörden gestatten, läuft dies in der Praxis auf eine freiwillige Datenübermittlung hinaus, die die Telemediendienstleister durchführen dürfen, die aber mangels gesetzlicher Ermächtigungsgrundlage in der StPO seitens der

---

abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten“.

165 Hauck, in: Löwe-Rosenberg, *StPO,* § 100a, Rn. 65 (zitiert nach juris), m.w.N. Daher werden Standortdaten, die beispielsweise ein Mobilfunkgerät im Stand-by Modus regelmäßig und automatisch aussendet, um im Falle eines Anrufes möglichst schnell erreichbar zu sein, nicht erfasst, sodass ihre Erhebung gesondert in § 100g Abs. 1 S. 3 StPO (für künftig anfallenden Standortdaten) und § 100i Abs. 1 Nr. 2 StPO (für bereits in der Vergangenheit entstandene Standortdaten) geregelt ist.

166 Hauck, in: Löwe-Rosenberg, *StPO*, § 100g, Rn. 43 (zitiert nach juris).

167 Karg, *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung*, DuD 2015, 85 (87 f.), m.w.N.

168 Unter Nutzungsdaten versteht man gemäß § 15 Abs. 1 TMG alle personenbezogenen Daten eines Nutzers, deren Erhebung und Verwendung erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen.

169 Karg, *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung*, DuD 2015, 85 (86).

Strafverfolgungsbehörden[170] nicht förmlich angeordnet werden darf.[171]

§ 100i StPO betrifft den Einsatz technischer Mittel, um die Gerätenummer eines Mobilfunkendgerätes,[172] die Kartennummern der darin enthaltenen Karten[173] sowie den Standort des Gerätes zu ermitteln. Die Vorschrift ist eng an § 100a f. StPO angelehnt und bezieht sich ausschließlich auf Mobilfunkendgeräte. Ihr Regelungskern betrifft den Einsatz sogenannter IMSI-Catcher[174] insbesondere zur Erstellung eines Bewegungsprofils oder zur Vorbereitung einer nachfolgenden Kommunikationsüberwachung oder Verkehrsdatenerhebung,[175] wenn die Rufnummer des betroffenen Gerätes nicht bekannt ist.

§ 100j StPO schließlich betrifft die Bestandsdatenauskunft, zu der geschäftsmäßige Telekommunikationsanbieter im Sinne des TKG verpflichtet sind. Wie bei den Verkehrsdaten wird auch hinsichtlich der Bestandsdaten für die Begriffsbestimmung auf das TKG, konkret auf die §§ 95, 111 TKG verwiesen.[176] Dadurch ist eine behördliche Anfrage an

170 Anders als für die Strafverfolgungsbehörden bestehen entsprechende Ermächtigungsgrundlagen in vielen Polizei- und Ordnungsgesetzen zur Prävention von Straftaten und in den Aufgabengesetzen der Geheimdienste (vgl. Karg, *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung*, DuD 2015, 85 (87), m.w.N.).

171 Karg, *Zugriff von Ermittlungsbehörden auf Nutzungsdaten bei der Strafverfolgung*, DuD 2015, 85 (85 f.); vgl. auch BT-Drucks. 16/3135, S. 2.

172 Gemeint ist die 15-stelligen Seriennummer IMEI (International Mobile Equipment Identity), mit der jedes GSM-, UMTS- und LTE-Endgerät weltweit eindeutig identifiziert werden kann (vgl. Wikipedia, Suchbegriff *IMEI)*.

173 Von Bedeutung ist hierbei insbesondere die SIM-Karte (Subscriber Identity Module, s. Wikipedia, Suchbegriff *SIM Karte*), auf der die weltweit jeweils einmalig vergebene IMSI-Nummer (International Mobile Subscriber Identity) gespeichert wird, die, unabhängig von der Telefonnummer, der Identifizierung des Netzteilnehmers dient (Wikipedia, Suchbegriff *IMSI).*

174 Dabei handelt es sich um ein Gerät, mit dem die IMSI-Nummer auf einer SIM-Karte ohne direkten körperlichen Zugriff auf die Karte in Erfahrung gebracht und Mobilfunktelefonate mitgehört werden können, da sich der IMSI-Catcher gegenüber dem Endgerät als Funkzelle und gegenüber dem Netzwerk als Mobiltelefon ausgibt (vgl. Wikipedia, Suchbegriff *IMSI Catcher*).

175 Sieber, *Gutachten zum 69. DJT*, S. 64.

176 § 95 TKG beschreibt den Begriff der Bestandsdaten nicht näher, sondern verweist auf § 3 TKG, unter dessen Nr. 3 Bestandsdaten allgemein definiert werden als „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“, während § 111 Abs. 1 TKG konkretisierend folgende Informationen abschließend erfasst:
„1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,

Telemediendienstleister, die gemäß § 14 TMG ebenfalls Bestandsdaten erheben dürfen, unzulässig.
§ 100j Abs. 2 StPO stellt klar, dass Bestandsdaten „auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden können“. Dies betrifft die in der Praxis überaus häufige Fallgestaltung, dass insbesondere zu Anfang der Ermittlungstätigkeit lediglich eine IP-Adresse bekannt ist,[177] die mit der Begehung einer Straftat in Verbindung steht, während die Zuordnung eines konkreten Anschlusses oder gar eines konkreten Namens mit Adresse ohne weitere Informationen unmöglich ist.

Die verbleibenden Regelungen zu elektronischen Daten findet sich in §§ 483 ff. StPO und betreffen die allgemeine Befugnis der Strafverfolgungsbehörden zur Verarbeitung personenbezogener Daten, deren explizite Gestattung aus Datenschutzgründen gemäß § 4 Abs. 1 BDSG erforderlich ist. Soweit es um die Datenübermittlung zwischen im Einzelnen genannten Behörden geht, gestattet § 488 Abs. 1 StPO ausdrücklich den Einsatz eines automatisierten Verfahrens, in dem gemäß S. 2 die beteiligten Stellen zu gewährleisten haben, „dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten“. Gleiches gilt gemäß § 493 Abs. 1 S. 2 StPO für die automatisierte Datenübermittlung im Rahmen des länder-übergreifenden staatsanwaltschaftlichen Verfahrensregisters, wobei durch § 493 Abs. 1 S. 2 2. HS StPO ausdrücklich der zuständigen Stelle die „Verantwortung für die Richtigkeit und die Aktualität der Daten“ auferlegt wird.

3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns“.

177 Europol, *Pressmitteilung vom 17.10.2017.*

III. Analoge Anwendungen[178]

Aufgrund der bisherigen Darstellung dürfte deutlich geworden sein, dass sich elektronische Daten ihrer Art nach wesentlich von den herkömmlichen Beweismitteln der StPO unterscheiden, gesetzliche Regelungen zum strafprozessualen Umgang mit ihnen jedoch nur bruchstückhaft vorhanden sind. Daher wird unter verschiedenen Aspekten und mit unterschiedlichen Schwerpunkten die Anwendbarkeit einzelner Normierungen, die sich auf körperliche Gegenstände beziehen, auf elektronische Daten diskutiert und faktisch praktiziert.[179] Ein herausragendes Beispiel für die Bemühung um eine Analogie ist die sich widersprechende Rechtsprechung des Bundesgerichtshofs und des Bundesverfassungsgerichts aus dem Jahr 2009 zur gesetzlichen Grundlage für eine Sicherstellung und Beschlagnahme von E-Mails auf dem – mangels abweichender Hinweise jeweils unterstellten inländischen - Mailserver des Providers beziehungsweise zur Verfassungskonformität der §§ 94 ff. StPO als Grundlage für eine solche Maßnahme.[180]

Während der 1. Strafsenat des Bundesgerichtshofs im Beschluss vom 31.03.2009[181] feststellt, dass die Sicherstellung und Beschlagnahme von E-Mails auf dem Server des Dienstleisters nicht allein auf §§ 94 ff. StPO gestützt werden könne, sondern aufgrund der Vergleichbarkeit von E-Mails mit herkömmlichen Postsendungen und der damit erhöhten Schutzwürdigkeit auf §§ 99 f. StPO, den Regelungen zur Postbeschlagnahme, zurückgegriffen werden müsse, hält der 2. Senat des Bundesverfassungsgerichts im Beschluss vom 16.06.2009[182] die im konkreten

178 Die unter diesem und den folgenden Punkten folgende Darstellung basiert im Wesentlichen auf der Veröffentlichung Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 3, NZWiSt 2017, 417.

179 Sieber, *Gutachten zum 69. DJT*, S. 64 f.

180 Betroffen sind die Entscheidungen BGH, Beschluss vom 31.03.2009, 1 StR 76/09, und BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43.
Zur ausführlichen Besprechung beider Entscheidungen: Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402.

181 BGH, Beschluss vom 31.03.2009, 1 StR 76/09.

182 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43.

Fall angewandten §§ 94 ff. StPO als Ermächtigungsgrundlage für eine solche Maßnahme jedenfalls dann für ausreichend, wenn die Ermittlungsmaßnahme nicht heimlich, nur punktuell, außerhalb eines laufenden Kommunikationsvorganges und bei bestehender Einwirkungsmöglichkeit des Betroffenen auf den Datenbestand erfolgt.[183]

Es scheint, dass der 3. Strafsenat des Bundesgerichtshofs nunmehr der Auffassung des Bundesverfassungsgerichts folgt, da er im Beschluss vom 04.08.2015 ohne nähere Begründung auf die §§ 94 ff. StPO als Grundlage einer Beschlagnahme von auf dem Mailserver eines Providers gespeicherten Daten verweist und feststellt, dass § 101 Abs. 1 StPO nicht einschlägig sei, obwohl sich diese Norm ausdrücklich auch auf die Postbeschlagnahme gemäß § 99 StPO bezieht.[184]

Beide Entscheidungen, die nicht näher auf eine mögliche Differenzierung der betroffenen Daten eingehen, sind in ihrer Begründung wie auch in ihrer praktischen Umsetzung problematisch und spiegeln das dringende Bedürfnis der Strafverfolgungsbehörden nach entsprechender Rechtssicherheit wider. Dennoch werden die Entscheidungen in einer Vielzahl von Fällen keine Relevanz haben, weil sich elektronische Daten zunehmend auf ausländischen Servern befinden und damit dem Herrschaftsbereich der StPO entzogen sind.[185] Das gilt auch unter dem Aspekt, dass die in Deutschland tätigen großen Internet-Dienstleister ihren Hauptsitz überwiegend in den USA haben.[186]

---

183 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 75; noch weitergehend für die Anwendung der §§ 94 ff. StPO als „allgemeine Vorschriften“ im Sinne des § 100g Abs. 5 StPO: Gesetzesbegründung, BT-Drucks. 16/5846, S. 55; Hauck, in: Löwe-Rosenberg, *StPO*, § 100g, Rn. 45.

184 BGH, Beschluss vom 04.08.2015, 3 StR 162/15.

185 Vgl. bereits LG Hamburg, Beschluss vom 08.01.2008, 619 Qs 1/08. Selbst wenn man annähme, dass dem zugangsberechtigten Dienstleister in solchen Fällen aus §§ 94 f. StPO eine Beschaffungspflicht obläge, wäre dieser gleichzeitig an die Datenschutzgesetze des Speicherortes gebunden, was in vielen Fällen einer Datenübermittlung an ausländische Strafverfolgungsbehörden entgegenstünde. Tatsächlich ist es selbst innerhalb der EU-Mitgliedstaaten den Telekommunikationsdienstleistern in den meisten Staaten untersagt, Daten direkt, also ohne Einschaltung des betroffenen Staates, an ausländische Behörden zu übermitteln (s. Europäische Kommission, *Report on the 28 February 2017 expert meeting*, S. 1). Für die US-amerikanischen Service Provider gilt dies gemäß § 2702 des Electronic Communications Privacy Act of 1986 (ECPA) jedenfalls für Kommunikationsinhaltsdaten.

186 Sieber, *Gutachten zum 69. DJT*, S. 114, m.w.N. spricht davon, dass „die

In der Rechtsprechung hat sich in Anlehnung an die gängige Unterscheidung in der Ermittlungspraxis mittlerweile auch die Einbeziehung von Inhaltsdaten neben Bestands- und Verkehrsdaten zur Komplettierung der Kommunikationsdaten durchgesetzt,[187] ohne dass der Begriff in der StPO aufgegriffen wird.[188]

Durchsuchung und die Beschlagnahme von Computersystemen […] aus tatsächlichen und rechtlichen Gründen häufig schwierig“ seien.

187 Vgl. etwa BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, zugleich BVerfGE 130, 151, oder BVerfG, Urteil vom 20.04.2016, 1 BvR 966/09 und 1 BvR 1140/09, zugleich BVerfGE 141, 220.

188 Die Verwendung der Begriffe ist nicht durchgängig stringent: Beispielsweise stellt das BVerfG im Beschluss vom 15.08.2014, 2 BvR 969/14, Rn. 47 (zitiert nach juris), ohne nähere Begründung explizit fest, „dass es sich bei E-Mails und Verkehrsdaten um unterschiedliche Kategorien von Daten“ handele, obgleich „E-Mails“ nicht nur Kommunikationsinhaltsdaten sondern immer auch Verbindungsinformationen beinhalten, die hinsichtlich Absenderadresse, Empfängeradresse und Sendezeitpunkt für den Endnutzer unmittelbar aus dem Nachrichtenkopf erkennbar sind.

IV. Einschlägige supranationale Regelungen

Der grenzüberschreitende Bezug spielt bei elektronischen Beweismitteln eine herausragende Rolle.[189] Das liegt zum einen daran, dass sich gespeicherte Daten, wie bereits dargestellt, häufig auf ausländischen Servern befinden.[190] Zum anderen haben viele Diensteanbieter, die auch den deutschen Markt bedienen, ihren Hauptsitz[191] und / oder ihre tatsächliche Datenverarbeitungsstelle[192] im Ausland, sodass die eigentliche Auskunfts- oder Mitwirkungshandlung dort zu vollziehen ist. Schließlich kann die mobile Nutzungsmöglichkeit vieler Geräte unmittelbar durch einen Ortswechsel des Nutzers zur grenzüberschreitenden Lage führen.[193]

Strafprozessuale Ermittlungstätigkeit ist in allen Fällen grenzüberschreitender Beweismittelerlangung grundsätzlich nur im Rahmen der internationalen Rechtshilfe in Strafsachen zulässig,[194] was eigenständige, nicht-einvernehmliche Zugriffe im betroffenen Drittstaat ausschließt.[195] Während die allgemeinen Regelungen des Völkerstrafrechts gegebenenfalls noch einen Zugriff auf öffentlich zugängliche Daten zu rechtfertigen vermögen, entfällt diese Möglichkeit jedenfalls

189 Vgl. Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (243).

190 Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (410), spricht gar davon, dass die Speicherung von Daten im Ausland „angesichts der internationalen Natur des Internets eher der Regelfall“ sei.

191 Hier sind mit den derzeitigen „Großen Sechs“ (Apple, Facebook, Google, Microsoft, Twitter und Yahoo!) vor allem die USA betroffen.

192 So betreibt beispielsweise die Microsoft Corporation die Datenverarbeitung ihrer europäischen Privatkunden ausschließlich von Cork, Irland, aus.

193 In technischer Sicht übernimmt dann das ausländische Netz die Ausführung der Dienstleistung, was als „Daten-Roaming“ bezeichnet wird.

194 Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (411); Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 4, zitiert nach juris), m.w.N.

195 Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (410).

für alle Daten, die nicht unmittelbar öffentlich zugänglich sind.[196] Die dafür erforderlichen Spezialregelungen fehlen weitestgehend und sind nur wie folgt vorhanden:

1. Recht der Europäischen Union

Wie bereits erwähnt, enthält Art. 2 der AAIS-Richtlinie Legaldefinitionen der Begriffe Informationssystem und Computerdaten.

Der Rahmenbeschluss des Rates vom 22.07.2003 zur Europäischen Sicherstellungsanordnung[197] erleichtert die Beweissicherung allgemein und ermöglicht beispielsweise die vorläufige Sicherung gespeicherter E-Mails.[198] Das Verfahren bezieht sich auf sämtliche Beweismittel und ausschließlich auf deren Sicherstellung, sodass die Übergabe des sichergestellten Beweismittels mit einem gesonderten Ersuchen im Rahmen des üblichen Rechtshilfeverfahrens zu erfolgen hat und keine besondere Dateneinteilung vorgenommen wird.[199]

Ergänzend erging am 18.12.2008 der Rahmenbeschluss des Rates zur Europäischen Beweisanordnung,[200] durch den die Erlangung eines in einem anderen EU-Mitgliedstaat bereits erhobenen Beweismittels vereinfacht werden sollte.[201] Er trifft ebenfalls keine Unterscheidung hinsichtlich möglicher Datenkategorien.

Durch die EEA-Richtlinie vom 03.04.2014, die gemäß ihres Art. 36 Abs. 1 bis zum 22.05.2017 von den Mitgliedstaaten in nationales Recht

196 Zur ausführlichen Diskussion vgl. Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 2 ff., zitiert nach juris), m.w.N.
197 Rahmenbeschluss 2003/577/JI des Rates vom 22.07.2003 über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union, ABl. EU L 196 vom 02.08.2003, S. 45.
198 Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (410).
199 EEA-Richtlinie, Begründung Ziff. 3.
200 Rahmenbeschluss 2008/978/JI des Rates vom 18.12.2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen, ABl. EU L 350 vom 29.12.2008, S. 72.
201 EEA-Richtlinie, Begründung Ziff. 4.

umzusetzen war, wird nunmehr ein holistischer Ansatz verfolgt, der das Rechtshilfeübereinkommen von 2000 ersetzt[202] und die bisherigen Instrumente der Europäischen Sicherstellungsanordnung und der Europäischen Beweisanordnung zusammenfassend unter dem Begriff der Europäischen Ermittlungsanordnung regelt.[203] Dabei wird für weite Bereiche der Grundsatz der gegenseitigen Anerkennung ausgedehnt, ohne jedoch vollständig vom Prinzip der Rechtshilfe abzurücken, da auch die EEA-Richtlinie weiterhin keine unmittelbare Beweiserhebung eines Staates im Hoheitsgebiet eines anderen Staates sondern lediglich eine erleichterte Zusammenarbeit vorsieht.[204] Er betrifft sämtliche Beweismittel, ohne auf unterschiedliche Datenkategorien einzugehen.

2. Die Cybercrime-Konvention von 2001

Die Cybercrime-Konvention aus dem Jahr 2001, die vom Europarat als Übereinkommen über Computerkriminalität initiiert wurde, steht grundsätzlich allen Staaten offen. Bislang wurde sie von 56 Staaten ratifiziert,[205] darunter neben Deutschland[206] die meisten EU-Mitgliedstaaten,[207] Israel, Japan, Kanada, Südafrika und die USA.

Dort, wo sie Anwendung findet, ist gemäß Art. 32 lit. a) jeder Vertragspartei ein direkter Zugriff auf „öffentlich zugängliche gespeicherte Computerdaten (offene Quellen)“[208] gestattet. Für nicht

202 Vgl. Europäische Kommission, *Progress Report,* 07.12.2016, S. 10.

203 EEA-Richtlinie, Begründung Ziff. 5, 7.
Gemäß EEA-Richtlinie, Begründung Ziff. 8, bleiben die bisherigen Instrumente allerdings erhalten, weil „die Bildung einer gemeinsamen Ermittlungsgruppe und die Beweiserhebung im Rahmen einer solchen Gruppe spezifische Vorschriften [erfordern], die besser getrennt geregelt werden“.

204 Vgl. Brodowski, *Der „Grundsatz der Verfügbarkeit“ von Daten zwischen Staat und Unternehmen,* ZIS 2012, 474 (478).

205 Europarat, *Chart of signatures and ratifications of Treaty 185* (Stand: 04.01.2018).

206 Nach Sieber, *Gutachten zum 69. DJT*, S. 66 f., fehlt es trotz der Ratifizierung in Deutschland weiterhin an einer vollständigen Umsetzung der Konvention im Strafprozessrecht.

207 Bemerkenswerterweise ist ein Beitritt Irlands bislang nicht erfolgt, obgleich hier viele international tätige Internet-Dienstleister Datenspeicherzentren betreiben, beispielsweise die Microsoft Corporation, Google und Yahoo!.

208 Der Begriff Computerdaten wird in Art. 1 lit b) der Cybercrime-Konvention inhaltlich wie in der AAIS-Richtlinie legaldefiniert. Die in Art. 1 lit a) der Konvention dargestellte Legaldefinition des Begriffes Computersystem ist hingegen enger als der in der AAIS-Richtlinie bestimmte Begriff des

öffentlich zugängliche gespeicherte Informationen hingegen fehlt es – bis auf den in Art. 32 lit. b) geregelten Ausnahmefall der Zustimmung des unmittelbar Betroffenen - an einer entsprechenden Regelung, da sich die Vertragsstaaten bislang nicht auf eine solche einigen konnten.[209] Allerdings sehen die Art. 16 ff., 29 ff. der Konvention vorläufige Maßnahmen zur Sicherung elektronischer Beweismittel - sogenannte Quick-Freeze Verfahren - vor,[210] deren endgültige Sicherstellung sodann nach Erlangung einer entsprechenden gerichtlichen Entscheidung beziehungsweise bei Auslandsbezug im Rahmen der Rechtshilfe zu erfolgen hat.[211]

Die Cybercrime-Konvention unterscheidet zudem bezüglich Kommunikationsdaten zwischen Verkehrsdaten, die in Art. 1 lit. d) legaldefiniert werden,[212] und Bestandsdaten, deren Definition sich in Art. 18 Abs. 3 findet.[213] Die Inhalte der Begriffe sind denen des TKG ähnlich, aber

---

Informationssystems, der auch Computerdaten als solche dem Informationssystems zuweist. Der Grund für die abweichenden Regelungen, deren Wortlaut im Jahr 2001 beziehungsweise 2013 bestimmt wurde, liegt vermutlich in der späteren Berücksichtigung des Cloud Computings, das 2001 noch nicht existierte und 2013 nunmehr miterfasst werden sollte.

209 Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 2, zitiert nach juris), m.w.N.; Sieber, *Gutachten zum 69. DJT*, S. 145 f.

210 Brodowski, S*trafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (411); Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 4, zitiert nach juris), m.w.N.

211 Vgl. Sieber, *Gutachten zum 69. DJT*, S. 123; Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 2, zitiert nach juris), m.w.N.

212 Danach umfasst der Begriff Verkehrsdaten „alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht“.

213 Bestandsdaten sind danach „alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:
a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dauer des Dienstes;
b) die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung

nicht identisch; insbesondere stellt Art. 18 Abs. 3 der Cybercrime-Konvention explizit fest, dass Bestandsdaten nicht notwendig elektronische Daten sein müssen. Daneben erwähnt Art. 18 Abs. 3 Inhaltsdaten („content data“) in negativer Abgrenzung zu Verkehrs- und Bestandsdaten, ohne dass die Cybercrime-Konvention selbst eine Definition des Begriffes vorsieht.[214]

3. Die Europäische Menschenrechtskonvention

Die EMRK enthält keine ausdrücklichen Regelungen zum Umgang mit elektronischen Daten im Strafprozess. Allerdings hat sich der Europäische Gerichtshof für Menschenrechte in einer Vielzahl von Entscheidungen mit der Erlangung und Verwertung elektronischer Daten befasst und dabei wiederholt herausgestellt, dass die jeweiligen staatlichen Maßnahmen an Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) und Art. 10 EMRK (Freiheit der Meinungsäußerung) zu messen seien.[215]

Soweit ersichtlich hat sich der Europäische Gerichtshof für Menschenrechte bislang nur ein einziges Mal in einem Nebensatz zur unterschiedlichen Schutzwürdigkeit verschiedener Datenklassen geäußert, als er in der Bărbulescu-Entscheidung[216] darauf hinwies, dass zwischen der Beobachtung des Kommunikationsflusses und der des Kommunikationsinhaltes zu unterscheiden sei, wobei die Beobachtung des Kommunikationsinhaltes eine klar eingriffsintensivere Methode sei, die einer gewichtigeren Rechtfertigung bedürfe.[217] Eine Begründung für

---

und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;
c) andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen“.

214 In Europarat, *Erläuternder Bericht zur Cybercrime-Konvention*, Abschnitt 209, wird dargelegt, dass sich der Begriff Inhaltsdaten auf den Kommunikationsinhalt beziehe.

215 Zuletzt ausdrücklich für Art. 8 EMRK im Zusammenhang mit Bestandsdaten und dynamischer IP-Adresse: EGMR, Urteil vom 24.04.2018 („Benedik v. Slovenia“), appl. no. 62357/14, Rn. 110; für eine Übersicht der wichtigsten Entscheidungen vgl. EGMR, *Factsheet New technologies*; EGMR, *Factsheet Personal data protection*; EGMR, *Guide on Article 8 of the European Convention on Human Rights*, S. 66 f., 79.

216 EGMR, Urteil vom 05.09.2017 („Bărbulesu v. Romania“), appl. no. 61496/08.

217 EGMR, Urteil vom 05.09.2017 („Bărbulesu v. Romania“), appl. no.

diese Auffassung fehlt; sie entspricht dem Inhalt nach der verbreiteten Unterscheidung von Kommunikationsverkehrs- und -inhaltsdaten.

Ob der EGMR in naher Zukunft detaillierter auf unterschiedliche Datenkategorien und ihre jeweilige Schutzwürdigkeit eingehen wird, ist derzeit offen.[218]

61496/08, Rn. 121: „a distinction should be made between monitoring of the flow of the communications and of their content. […] Since monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification“.

218 Anhängige Verfahren, in denen dies der Sache nach möglich wäre, sind unter anderem: Big Brother Watch et al. v. United Kingdom (appl. no. 62322/14) und Breyer v. Deutschland (appl. no. 50001/12). Der jeweilige Verkündungstermin für eine Endentscheidung ist derzeit nicht absehbar (Stand: 30.04.2018).

V. Verbleibende Regelungslücken

Aus der bisherigen Darstellung lässt sich ableiten, dass hinsichtlich elektronischer Beweismittel im Strafprozess quantitativ und qualitativ erhebliche Normierungsdefizite bestehen. Insgesamt fehlt es konzeptionell an einer umfassenden, systematischen Gesetzgebung, die den Strafermittlungsbehörden geeignete Ermittlungsinstrumentarien, die dem aktuellen Stand der Technik entsprechen, zur Verfügung stellt, die den Schutz der Verdächtigen- und Bürgerrechte umfassend gewährleistet und Rechtssicherheit auf dem komplexen Feld der elektronischen Beweismittel für den Strafprozess schafft.[219] Bereits im Ansatz fehlt es an einer klaren Begriffsverwendung für unterschiedliche Arten der elektronischen Beweismittel. Dort, wo Normierungen bestehen, sind sie teilweise verfassungsrechtlich bedenklich,[220] teilweise unklar in ihrer Auslegung[221] und teilweise für

219 Sieber, *Kurzgutachten,* S. 8; vgl. auch Hiéramente / Pfister, *Datenerhebung beim Hersteller von Mobiltelefonen, Zum Erfordernis des Strukturwandels bei der strafprozessualen Datenerhebung*, StV 2017, 477, m.w.N.

220 Verfassungsrechtlich bedenklich sind aufgrund des Gebots der Normenbestimmtheit und der Normenklarheit vor allem die Anwendung der §§ 94 f. StPO auf elektronische Daten, sowohl für offene als auch insbesondere für verdeckte Maßnahmen, sowie die Zulässigkeit der Quellen-TKÜ generell. Hinsichtlich der §§ 100g und 100j StPO stellt sich die Frage nach der Rechtfertigung der Ungleichbehandlung von Telekommunikations- und sonstigen Kommunikationsdienstleistern für die strafprozessrechtliche Erhebung von Verkehrs- und Bestandsdaten. Aufgrund des Verhältnismäßigkeitsgebots bestehen zwischen-zeitlich wegen der technischen Fortentwicklung und der damit verbundenen gleichzeitigen Mehrfachvergabe identischer IP-Adressen an eine Vielzahl von Nutzern erhebliche Zweifel an der Verfassungsmäßigkeit des § 100j Abs. 2 StPO, dessen Anwendungsbereich sich im konkreten Einzelfall nunmehr regelmäßig auf eine große Zahl unbeteiligter Dritter erstreckt (vgl. Europol, *Pressemitteilung vom 17.10.2017*).
Zur Bedeutung der Normenbestimmtheit, der Normenklarheit, der Verhältnismäßigkeit und Ausgewogenheit sowie der Angemessenheit als verfassungsrechtliche Schlüsselprinzipien für die Gesetzgebung vgl. Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 201.

221 Unklarheiten bestehen insbesondere im Rahmen des § 100a StPO, soweit es um den Begriff der Telekommunikation geht (Mensch-zu-Mensch, Mensch-zu-Maschine, Maschine-zu-Maschine).

die Praxis schlichtweg ungeeignet[222].[223]

Der derzeit wichtigste Regelungsbedarf betrifft den Bereich der Ermächtigungsgrundlagen für datenspezifische Ermittlungsmaßnahmen, für den überwiegend die - unpassenden - für körperliche Gegenstände entwickelten Rechtsvorschriften angewandt werden.[224] Zwar wurden mit der Einführung der Quellen-TKÜ und der online-Durchsuchung inhaltlich weitreichende Maßnahmen geschaffen, die allerdings nur einen Teil des Ermittlungsspektrums abdecken. Es fehlt weiterhin an umfassenden Normierungen zur Sicherstellung von elektronischen Daten, zum Umgang mit großen Datenmengen und in diesem Zusammenhang auch zu Durchsichtsbefugnissen vor einer endgültigen Sicherstellung.

Eine Besonderheit elektronischer Daten gegenüber den herkömmlichen Beweismitteln liegt darin, dass das Ausmaß der Relevanz, die Sensibilität der Daten, verlässlich erst nach ihrer Sichtung erfolgen kann.[225] Das trifft zwar generell auch auf Schriftstücke zu. Ein Schriftstück dient aber in der Regel der Kommunikation mit anderen Personen, sodass häufig schon die äußerliche Form des Schriftstückes und die Angaben zum Absender und Empfänger jedenfalls in gewissem Rahmen Rückschlüsse auf die Sensibilität erlauben. Diese Möglichkeit ist bei der elektronischen Kommunikation deutlich eingeschränkt, weil es zum einen an der Formenvielfalt fehlt – eine E-Mail oder eine WhatsApp-Nachricht weisen immer die selbe Form auf, egal, an wen sie gerichtet sind, für einen Brief in Papierform gilt dies nicht zwingend –, zudem richtet sich die Identifikation der an der Kommunikation Beteiligten in der realen Welt in der Regel mindestens nach dem

222 So dürfte die Beschlagnahme elektronischer Daten gemäß §§ 94 ff. StPO faktisch zunehmend leer laufen, weil immer mehr Daten auf ausländischen Servern beziehungsweise bei international tätigen Dienstleistern mit Sitz im Ausland gespeichert werden und damit aus rechtlichen und tatsächlichen Gründen dem direkten Zugriff der hiesigen Strafermittlungsbehörden entzogen sind; zur selben Problematik auf internationaler Ebene: Internet & Jurisdiction Policy Network, *Cross Border Access to User Data*, S. 4.

223 Ausführlich dazu: Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 4, NZWiSt 2017, 449 (450 ff.).

224 Sieber, *Gutachten zum 69. DJT*, S. 153.

225 Vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 283.

Namen und häufig auch der Anschrift, während in der virtuellen Welt (irgend-) eine Zeichenfolge genügt, solange sie vom Provider eindeutig zugeordnet werden kann. Auch bei kleinen Datenmengen ist dem jeweils erlangten Datensatz nicht anzusehen, inwieweit er wegen des Persönlichkeitsschutzes aufgrund seines Inhalts einem möglichen Beweisverwertungsverbot unterliegt. Bislang gibt es keine Vorschriften dazu, welche Stelle die erforderliche und äußerst praxisrelevante Datendurchsicht zur Entscheidung der Beweismittelverwertbarkeit vornehmen muss.[226]

Selbst wenn die Auffassungen des Bundesverfassungsgerichts und des Bundesgerichtshofs darin übereinstimmen, dass die Erlangung von beim Dienstleister gespeicherten E-Mails aus rechtlicher Sicht zulässig ist, bleibt für die ausführenden Ermittlungspersonen unklar, nach welchen formalen Voraussetzungen sie vorzugehen haben. Hier besteht aus praktischer Sicht dringender Klärungsbedarf.[227]

Es ist desweiteren völlig offen, ob und gegebenenfalls wie der Informationsaustausch von Mensch-zu-Maschine und Maschine-zu-Maschine, dessen Umfang und Bedeutung für das Strafverfahren künftig deutlich ansteigen wird, in das bestehende System einzuordnen ist,[228] weil auch der Inhalt eines Datensatzes, der sich nicht auf eine bewusste Kommunikation bezieht,[229] den Betroffenen in seinen unterschiedlichen Lebensbereichen unterschiedlich stark berühren kann. Die Bandbreite mit fließendem Übergang reicht von annähernd irrelevant bis hochsensibel.

Im Hinblick auf die Erlangung elektronischer Beweismittel und ihrer Einführung in die Hauptverhandlung fehlt es zudem unabhängig von

226 Vgl. Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (305).

227 Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (412).

228 Vgl. Sieber, *Gutachten zum 69. DJT*, S. 106 ff.

229 Inhalte von Datensätzen, die sich nicht auf Kommunikationsinhalte beziehen, sind beispielsweise die bereits erwähnten Standortdaten oder die Auflistung in der Vergangenheit besuchter Webseiten oder erfolgter Downloads.

der Art der betroffenen Datensätze und unabhängig von der jeweils zulässigen Ermittlungsmaßnahme durchgehend an Normierungen, die die Authentizität und Integrität eines letztlich potentiell zur Verurteilung führenden elektronischen Beweismittels verfahrensrechtlich bestmöglich absichern. Die herausragende Bedeutung einer solchen Absicherung hat der Bundesgesetzgeber für ganz spezielle Datengruppen jenseits der strafprozessualen Beweismittelerlangung zum Beispiel durch die Regelungen der §§ 41a a.F., 483 ff. StPO zum Ausdruck gebracht.[230]

Die Bedeutung der angesprochenen Sicherungsregelungen geht über die formaler Verfahrensregeln hinaus, weil sie sich unmittelbar auf die Bestimmung des Beweiswertes eines elektronischen Datensatzes und damit auf die Beweiswürdigung durch den Richter auswirken.[231] Lediglich § 100a Abs. 5 S. 3 StPO bestimmt in allgemeiner Form, dass „kopierte Daten […] nach dem Stand der Technik gegen Veränderungen, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen“ sind.

Aufgrund des technischen Fortschritts erfolgen Kommunikationsprozesse bereits heute vermehrt über Dienstleister, die nicht dem TKG, sondern dem TMG unterfallen. Ihre strafprozessualen Mitwirkungs- und Auskunftspflichten sind ungeregelt und durch bestehende Datenschutzregelungen grundsätzlich untersagt, obgleich sie aus Sicht des Verbrauchers häufig die gleichen Dienste wie Telekommunikationsdienstleister anbieten[232] und mit Bestandsdaten und Nutzungsdaten im Sinne des TMG über vergleichbare Datensätze wie die

230 Wie bereits dargelegt, betreffen die genannten Vorschriften nicht die kritische Phase der Beweismittelerlangung und -aufbereitung.

231 Sieber, *Gutachten zum 69. DJT*, S. 68.
In den USA wurden Ende 2016 in einem Verfahren des FBI elektronische Beweismittel nicht zugelassen, weil die Behörde trotz entsprechender gerichtlicher Anordnung keine näheren Angaben zu ihrer Erlangung machte (s. Osborne, *FBI refuses to release Tor exploit details, evidence thrown out of court*, Zero Day online, 16.05.2016).
Vgl. auch Mason, *Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now – But they Don`t Know it,* Computer and Telecommunications Law Review, 2017, Volume 23, Issue 8, S. 213 (222 f.), m.w.N.

232 Augenscheinlich ist dies für Telefondienste, die „klassisch“ oder beispielsweise als WhatsApp- oder Skype-Anruf mit Voice-over-IP über das Internet durchgeführt werden können, ohne dass es für den Nutzer einen erkennbaren Bedienungsunterschied gibt.

Telekommunikationsanbieter im Sinne des TKG verfügen. Dies gilt zunehmend auch für die Hersteller der Kommunikations-Hardware, die sich häufig nicht mehr trennscharf von den klassischen Telekommunikationsdienstleistern unterscheiden lassen.[233]

Neben diesen innerstaatlichen Aspekten besteht gesetzlicher Regelungsbedarf auch in grenzüberschreitender Hinsicht:[234]

An erster Stelle gilt dies mit Blick auf die Jurisdiktion, die Ermittlungszuständigkeit deutscher Strafverfolgungsbehörden. Mit Cloud Computing und der heutiger Technik für elektronische Telekommunikation ist es einem Dienstleister möglich, in Deutschland tätig zu sein, ohne dass er mit materieller Infrastruktur, Personal oder einem (tatsächlichen oder rechtlichen) Firmensitz im Land vertreten ist. Selbst die Prozesssteuerung der angebotenen Dienstleistungen muss nicht notwendig vom Inland aus erfolgen. Es besteht daher erheblicher Klärungsbedarf, nach welchen Kriterien und unter welchen Voraussetzungen ein in Deutschland tätiger, aber physisch nicht vorhandener Dienstleister, der Zugang zu potentiellen strafprozess-rechtlich relevanten elektronischen Beweismitteln hat, dem deutschen Strafprozessrecht unterliegt.[235] Die Frage ist erheblich, weil ein gesellschaftliches Interesse an einer funktionierenden Strafverfolgung jedenfalls dann besteht, wenn sich eine Tat unmittelbar im Inland auswirkt – ungeachtet der Frage, wo der Täter handelte und wo die für das Strafverfahren erforderlichen Beweismittel zu finden sind.[236]

Außerdem stellt sich die Frage, inwieweit eine Rangordnung für verschiedene Zuständigkeiten gilt, wenn – etwa beim Einsatz von

233 Hiéramente / Pfister, *Datenerhebung beim Hersteller von Mobiltelefonen, Zum Erfordernis des Strukturwandels bei der strafprozessualen Datenerhebung*, StV 2017, 477.

234 Einen skizzenhaften Überblick über einige mögliche grenzüberschreitende Fallkonstellationen gibt Internet & Jurisdiction Policy Network, *Cross Border Access to User Data*, S. 10.

235 Vergleichbare Probleme stellen sich nicht nur in strafprozessrechtlicher, sondern auch in datenschutzrechtlicher Hinsicht – vgl. OVG Schleswig-Holstein, Beschlüsse vom 22.04.2013, 4 MB 10/13 und 4 MB 11/13, DuD 2013, 475.

236 Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (680).

Botnetzen oder bei Angriffen auf die Cloud – einer einzigen Tat mehrere Tatorte zugeordnet werden können, die sich in unterschiedlichen Jurisdiktionen befinden.[237] Die vorhandenen Regelungen hierzu sind für die praktischen Fragen unzureichend.[238]

Ein weiteres Problem betrifft die Ermittlungsbefugnisse deutscher Behörden im „cyber space“, wenn im Rahmen eines virtuellen Grenzübertritts (VGÜ, englische Umschreibung: „loss of location“) auf elektronische Daten zugegriffen wird, die zwar auf ausländischen Servern gespeichert, aber vom Inland aus zugänglich sind.[239] Die Frage erstreckt sich auf Situationen, in denen der Speicherort möglicherweise, also zum Zeitpunkt der Ermittlungsmaßnahme nicht sicher feststehend, im Ausland ist (potentielle VGÜ, englische Umschreibung: „loss of knowledge of location“).[240] Ihr kommt eine besondere Bedeutung für die Fälle zu, in denen der Speicherort selbst im Nachhinein nicht mehr eindeutig geklärt werden kann[241] – ein Szenario, das im Rahmen des zunehmenden Cloud Computings nicht selten auftritt.[242]

Komplexer als bei rein nationalen Ermittlungsmaßnahmen stellt sich die

237 Sieber, *Gutachten zum 69. DJT*, S. 75.
238 Ausführlich zu den vorhandenen Regelungen (wie etwa der Cybercrime-Konvention) und ihrer Unzulänglichkeit: Sieber, *Gutachten zum 69. DJT*, S. 74 f., m.w.N.
239 Laut Gercke, *Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten*, StraFo 2009, 271 (S. 1, zitiert nach juris), war bereits im Jahr 2009 in 80% der Fälle, in denen das Internet als Medium bei der Begehung oder Durchführung von Straftaten genutzt wurde, für die Ermittlungsbehörden ein Zugriff auf im Ausland gespeicherte Daten erforderlich. Zur rechtlichen Problematik und möglichen Lösungsansätzen insbesondere im Zusammenhang mit der Staatssouveränität und dem Territorialitätsprinzip: Sieber / Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, Max Planck Yearbook of United Nations Law, Volume 20 (2016), S. 241 (251 ff.).
240 Sieber, *Gutachten zum 69. DJT*, S. 77.
241 Europäische Kommission, *Progress Report,* 07.12.2016, S. 14.
242 Während die Europäische Kommission Services, *Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*, S. 10, alternative Lösungsansätze aufzeigt und dabei ausdrücklich feststellt, dass nach Expertenmeinung ein Festhalten am bisherigen Territorialitätsbegriff im Zusammenhang mit dem Speicherort elektronischer Daten nicht sinnvoll sei, hat der Europarat, T-CY, *Final Report*, 16.09.2016, S. 47, konkrete Vorschläge für Ermittlungsbefugnisse zur Erlangung von Bestandsdaten, für Datensicherungsanordnungen und für Notfallsituationen erarbeitet.

Problematik der vorläufigen Datensicherung im Ausland. Wegen des Flüchtigkeitscharakters elektronischer Daten und bestehender Datenschutzvorschriften in vielen Ländern ist sie durchaus zeitkritisch. Sie wird durch „Einfrieren“ der Daten in Quick-Freeze Verfahren durchgeführt.[243] Innerhalb der Europäischen Gemeinschaft findet die vorläufige Sicherung über die Instrumente der Europäischen Ermittlungsanordnung und der Europäischen Sicherstellungsanordnung statt.[244] Entsprechende Regelungen mit sonstigen Drittstaaten fehlen.[245]

Daneben fehlen unter dem Stichwort „Gesetzeskollision“ verlässliche Regelungen dazu, wie sich Dienstleister zu verhalten haben, wenn sie in das grenzüberschreitende Spannungsfeld von strafprozessualer Mitwirkungspflicht und datenschutzrechtlichem Handlungsverbot geraten. Die Problematik ist reziprok, da sie sowohl die Fälle erfasst, in denen die Mitwirkungspflicht im Inland und das Handlungsverbot im Ausland bestehen, als auch diejenigen, in denen in Deutschland gespeicherte Daten von hiesigen Unternehmen ohne Beschreitung des Rechtshilfeweges direkt an ausländische Strafverfolgungsbehörden übermittelt werden sollen, was ihnen derzeit untersagt ist.[246]

Schließlich haben Dienstleister, die nicht vom TKG und den dortigen Entschädigungsregelungen erfasst werden, derzeit ebenso wenig wie sonstige Dritte, die Zugang zu beweiserheblichen elektronischen Daten haben und darüber, ohne Zeuge zu sein, Auskunft erteilen, einen gesetzlichen Vergütungs- oder Entschädigungsanspruch. Dies betrifft nicht nur die in der Praxis vorwiegend betroffenen US-amerikanischen Provider, sondern auch die inländischen, die dem TMG unterfallen, und Privatpersonen.

Zusammenfassend ist festzustellen, dass der Gesetzgeber dringend

243 Sieber, *Gutachten zum 69. DJT*, S. 123.
244 Art. 32 EEA-Richtlinie und Art. 1 Europäische Sicherstellungsanordnung.
245 Sieber, *Kurzgutachten,* S. 7.
246 In Deutschland ergibt sich das Verbot der direkten Kooperation mit ausländischen Strafermittlungsbehörden für inländische Dienstleister im Umkehrschluss aus der enumerativen Auflistung der ausschließlich nationalen Behörden, an die eine Datenübermittlung erfolgen darf, in §§ 112 Abs. 2, 113 Abs. 3 TKG und § 14 Abs. 2 TMG.

aufgerufen ist, die erforderlichen Regelungen zu erlassen, wobei offensichtlich davon abgesehen werden sollte, dies durch Einzelnormierungen und Querverweise zu versuchen.[247] Aufgrund der Vielzahl der klärungsbedürftigen Regelungslücken würde ein solcher Flickenteppich kaum zu einer befriedigenden Lösung führen, zumal das System der StPO erkennbar nicht auf unkörperliche Beweisgegenstände ausgerichtet ist. Vielmehr ist ein schlüssiges Gesamtkonzept zu entwickeln,[248] das elektronische Beweismittel nicht nur als neuartige Kategorie in den Kanon der Strengbeweismittel einführt, sondern auch explizite Regelungen zu ihrer Erlangung und Verwertung im Strafprozess enthält, die den wichtigsten Besonderheiten Rechnung tragen.

247 Sieber, *Gutachten zum 69. DJT*, S. 16, fordert eine „grundlegende Anpassung“ im Gegensatz zu den bisher erfolgten „partielle[n] gesetzliche[n] Reformen“; im Ergebnis ebenso und allgemein für die EU-Mitgliedstaaten: EVIDENCE Project, *Roadmap*, S. 19.

248 So auch Sieber, *Gutachten zum 69. DJT*, S. 13.

VI. Umgang mit den Regelungslücken in der Praxis

Neben dem Rückgriff auf Normierungen, die auf körperliche Beweismittel zugeschnitten sind, behilft sich die Praxis mit unterschiedlichen Vorgehensweisen, die im Folgenden – nicht abschließend – in aller Kürze dargestellt werden sollen:

Um der Bedeutung der Sicherung der Authentizität und Integrität elektronischer Beweismittel verfahrenstechnisch gerecht zu werden, haben sowohl das Bundeskriminalamt als auch alle 16 Landeskriminalämter spezielle Fachabteilungen für die digitale Forensik eingerichtet,[249] in denen auf höchstem fachlichen Niveau eine Kompetenzbündelung stattfindet.[250] Auf Ebene der Europäischen Union wurde Europol mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Centre, EC3) eine entsprechende Fachbehörde angegliedert, die zwar selbst keine Ermittlungsverfahren durchführt, aber die jeweiligen nationalen Ermittlungsbehörden strategisch und operativ unterstützt.[251]

Um möglichst schnell relevante Daten zu erhalten, ist es den Strafverfolgungsbehörden in den meisten EU-Mitgliedstaaten gestattet, Informationen zu verwerten, die sie auf freiwilliger Basis von einem Dienstleister erlangen.[252] Während es den europäischen Dienstleistern aus Datenschutzgründen überwiegend gesetzlich verboten ist, elektronische Daten unmittelbar an eine ausländische Ermittlungsbehörde zu übermitteln,[253] ist dies den US-amerikanischen Providern,

249 BKA, *Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft*.

250 Vgl. allgemein zum Hauptaufgabenfeld der forensischen Informatik: Sieber, *Gutachten zum 69. DJT*, S. 68 f.; LKA Baden-Württemberg, *Cybercrime und Digitale Spuren, Jahresbericht 2016*, S. 23 ff.

251 Unter der Schirmherrschaft des EC3 haben sich beispielsweise im Mai 2017 führende Unternehmen aus dem Bereich der digitalen Forensik dafür ausgesprochen, künftig ein einheitliches Format bei der Datenanalyse zu verwenden, um eine erleichterte Weiterverarbeitung seitens auf Seiten der Strafverfolgungsbehörden zu ermöglichen (s. Europol, *Pressemitteilung vom 12.05.2017*).

252 Eine Ausnahme bildet in dieser Hinsicht unter anderem die Slowakei, wo eine freiwillige direkte Zusammenarbeit ausländischer Dienstleister mit den nationalen Strafverfolgungsbehörden mit dem Argument untersagt ist, dass mit einer solchen Zusammenarbeit bestehende Rechtshilfeabkommen umgangen würden.

253 Europäische Kommission, *Progress Report,* 07.12.2016, S. 4.

die einen Großteil der relevanten elektronischen Daten innehaben,[254] jedenfalls für sogenannte subscriber data[255] und traffic data[256] insofern erlaubt, als sie aus Sicht des US-Bundesgesetzgebers eigenständig über eine Datenübermittlung entscheiden können.[257] Obgleich es keine nähere Ausgestaltung dieser freiwilligen[258] Mitwirkung gibt,[259] ist ihre praktische Bedeutsamkeit enorm: Alleine aus Deutschland erreichten im zweiten Halbjahr 2016 knapp 31.300 Anfragen (ohne Notfallanfragen) die sechs großen US-amerikanischen Provider Apple Inc., Facebook, Google, Microsoft Corporation, Twitter und Yahoo!, von denen mit knapp 17.200 ca. 55 Prozent beantwortet wurden.[260]

Diese Praxis wirft eine Vielzahl rechtlicher und tatsächlicher Probleme auf. Hingewiesen sei an dieser Stelle lediglich auf die erhebliche Rechtsunsicherheit, die maßgeblich auf dem unterschiedlichen Verständnis der verbreiteten Begriffsverwendung von Bestands-,

254 Europäische Kommission, *Progress Report,* 07.12.2016, S. 6.

255 Subscriber data meint im Wesentlichen Bestandsdaten; allerdings wird der Begriff weder von den Providern noch von den auskunftsersuchenden Staaten einheitlich verwendet.

256 Wie bei den subscriber data gibt es auch für die traffic data, die Verkehrsdaten, keine eindeutige Begriffsverwendung.

257 Die Erlaubnis folgt aus § 2702 des Electronic Communications Privacy Act of 1986 (ECPA); vgl. auch Sieber, *Gutachten zum 69. DJT*, S. 78.

258 Ob der Begriff der Freiwilligkeit angemessen ist, soll hier nicht weiter verfolgt werden. Fraglich ist dies allerdings, da die Initiative zur Zusammenarbeit in den allermeisten Fällen von den Strafverfolgungsbehörden ausgeht und die Anfrage überwiegend nach den formellen nationalen Verfahrensregeln, also förmlich, erfolgt. Nicht selten beinhaltet dies eine gerichtliche Verfügung, die sich nach dem Selbstverständnis der europäischen Gerichte aber kaum auf eine geprüfte Option zum Tätigwerden, sondern vielmehr auf eine bejahte Pflicht zur Beauskunftung (jedenfalls nach nationalen Maßstäben) bezieht; teilweise wird die gerichtliche Verfügung von den Providern sogar als Voraussetzung einer Beauskunftung verlangt.

259 Vgl. Internet & Jurisdiction Policy Network, *Cross Border Access to User Data*, S. 4; zum Teil existieren bilaterale Abkommen einzelner Länder oder gar einzelner Strafverfolgungsbehörden mit einem Provider (Europäische Kommission, *Progress Report,* 07.12.2016, S. 4). Ihr näherer Inhalt ist nicht öffentlich zugänglich.

260 Die Zahlen ergeben sich aus den von den Unternehmen veröffentlichten Transparenzberichten für das 2. Halbjahr 2016:
Apple Inc., *Report on Government and Private Party Requests for Customer Information, July 1 – December 31, 2016;*
Facebook, *Bericht über Regierungsanfragen, Deutschland, Juli 2016 – Dezember 2016;*
Google, *Transparency Report, Requests for user information, Germany;*
Microsoft Corporation, *Law Enforcement Requests Report, 2016 (Jul – Dec),* Landesauswahl Deutschland;
Twitter Inc., *Information requests, July to December, 2016;*
Yahoo!, *Government Data Requests, July 1, 2016 – December 31, 2016.*

Verkehrs- und Inhaltsdaten beruht.[261] Weitere Probleme ergeben sich aus fehlenden Standards zur Frage, nach welchen Kriterien ein Provider als inländisch oder ausländisch zu betrachten ist, aus den uneinheitlichen und unbeständigen Formvorgaben der Dienstleister, die bei der Auskunftsanfrage von den Strafverfolgungsbehörden zu beachten sind, und aus der aus Sicht der Strafverfolgungsbehörden fehlenden Verlässlichkeit der Provider-Reaktion auf eine Anfrage.[262] Daneben ist zu beachten, dass durch die direkte Kooperation nicht nur bestehende Rechtshilfeabkommen unterlaufen, sondern zudem gegebenenfalls auch Souveränitätsrechte von Drittstaaten verletzt werden.[263]

Zur Frage, wie mit dem speziellen Problem der Mehrfachvergabe identischer dynamischer IP-Adresse umzugehen ist, wurde Ende Januar 2017 unter Europols Federführung ein fachspezifisches Netzwerk (European Network of Law Enforcement Specialists on CGN) gegründet, das die Anzahl der Fälle, die wegen der entsprechenden Providerpraxis nicht weiter ermittelt werden, systematisch dokumentieren, den internen Informationsaustausch fördern und den Dialog mit den Providern zur technischen Lösung des Problems fördern soll.[264] Allgemeinere Netzwerke auf der Ebene der Europäischen Union sind beispielsweise das Europäische Justizielle Netzwerk (European Judicial Network, EJN) und das Europäische Netz für die Fortbildung von Richtern und Staatsanwälten (European Judicial Training Network, EJTN), die sich ebenfalls mit einzelnen Problemen im Zusammenhang mit elektronischen Beweismitteln auseinandersetzen.

261 Europäische Kommission, *Progress Report,* 07.12.2016, S. 4.
262 Europäische Kommission, *Progress Report,* 07.12.2016, S. 4 und 6 f.
263 Ausführlich dazu: Kleinhans, *Die Cloud im rechtsfreien Raum, Wie regeln wir den Datenzugriff durch Sicherheitsbehörden im 21. Jahrhundert?*, S.2.
264 Europol, *Pressemitteilung vom 02.02.2017.* Zu weiteren Maßnahmen für diesen Problembereich auf EU-Ebene vgl. Europol, *Pressemitteilung vom 17.10.2017.*

Exkurs: Derzeitige Lage in den übrigen EU-Mitgliedstaaten und Lösungsansätze auf EU-Ebene[265]

I. Derzeitige Lage in den übrigen EU-Mitgliedstaaten

Vorab ist festzustellen, dass generell auch in den übrigen Mitgliedstaaten der Europäischen Union vergleichbare Probleme wie in Deutschland bestehen, wenn es um strafprozessuale elektronische Beweismittel geht. Dies ergibt sich aus der Auswertung einer von der Europäischen Kommission zwischen Juni und Oktober 2016 durchgeführte Umfrage unter den EU-Mitgliedstaaten mit dem englischen Titel „Improving criminal justice in cyberspace“.[266]

Hinsichtlich der Einteilung elektronischen Beweismittel geben mindestens 5 Mitgliedstaaten[267] gesetzlich keine bestimmten Kategorien vor, während im Übrigen eine Einteilung ähnlich wie in Deutschland in Bestandsdaten, Verkehrsdaten und Inhaltsdaten vorherrscht,[268] wobei der Inhalt der jeweiligen Begriffsbestimmungen jedoch stark variiert.[269]

---

265 Die folgende Darstellung basiert im Wesentlichen auf der Veröffentlichung Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 3, NZWiSt 2017, 417 (423 f.) während Abschnitt II bei Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 4, NZWiSt 2017, 449 (453 ff.) vertieft dargestellt wird.

266 Vgl. Europäische Kommission, *Progress Report,* 07.12.2016 und Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*.
Die Umfrage war Teil eines von der Kommission durchgeführten Expertenprozesses, in dessen Rahmen zudem mehrere Treffen mit Sachverständigen aus allen Mitgliedstaaten stattfanden, unter anderem am 17./18.01.2017 und am 28.02.2017. Die jeweiligen Berichte der Expertentreffen sind online auf der Seite der zuständigen Generaldirektion Migration und Inneres in englischer Sprache abrufbar (https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en; Stand: 31.01.2018).

267 Gemäß Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 3, sind dies jedenfalls Estland, Italien, Kroatien, Luxemburg und Ungarn.

268 Gemäß Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 3, existieren Legaldefinitionen für Bestandsdaten („subscriber data“) in mindestens 14 Mitgliedstaaten, für Verkehrsdaten („traffic data“) in mindestens 17 Mitgliedstaaten und Inhaltsdaten („content data“) in mindestens 9 Mitgliedstaaten.

269 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 3.

Obgleich mindestens 20 EU-Mitgliedstaaten hinsichtlich der Beweismittelerlangung keine Unterscheidung der Provider je nach angebotener Dienstleistung vorsehen,[270] scheinen sich in der Praxis die auch in Deutschland diskutierten Probleme des Umganges mit Telekommunikationsdienstleistern („electronic communication services“), Telemediendienstleistern („information society services“) und sonstigen online-Dienstleistern („services in other sectors“) zu stellen.[271]

Desweiteren gibt es innerhalb der EU-Mitgliedstaaten unterschiedliche Ansätze, wonach sich die Bewertung eines Dienstleisters als inländisch oder ausländisch richtet.[272]

Während es in den meisten Fällen keine gesetzlichen Normierungen hinsichtlich direkter Anfragen der Strafverfolgungsbehörden an ausländische Dienstleister gibt,[273] fehlt es auch umgekehrt in der Mehrzahl der Mitgliedstaaten an einer aus datenschutzrechtlicher Sicht erforderlichen gesetzlichen Ermächtigung der inländischen Dienstleister, auf direkte Anfragen ausländischer Strafverfolgungsbehörden unmittelbar zu antworten.[274]

Nicht nur in Deutschland tritt das VGÜ-Problem auf, wenn bei Durchführung einer Ermittlungsmaßnahme unklar ist, in welchem Land die begehrten elektronischen Daten gespeichert sind, und somit Ungewissheit darüber herrscht, welcher Staat betroffen sein könnte und an welche Stelle ein Übermittlungsgesuch gerichtet werden

270 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 2; eine solche Unterscheidung erfolge jedoch mindestens in Deutschland, Kroatien, Malta, Rumänien, Tschechien und Zypern.

271 Europäische Kommission, *Report on the 17 / 18 January 2017 expert meeting*, S. 1.

272 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 2, nennt Kriterien wie den Hauptsitz des Unternehmens, der Bewerbung einer Dienstleistung im jeweiligen Land und / oder den Ort der Datenspeicherung. Daneben könnte die Verwendung der Landessprache auf einer Firmenwebsite oder das Vorhandensein einer bestimmten Menge an Nutzern aus dem jeweiligen Land als Zuordnungskriterium angedacht werden.

273 Europäische Kommission, *Report on the 28 February 2017 expert meeting*, S. 1.

274 Europäische Kommission, *Report on the 28 February 2017 expert meeting*, S. 1.

müsste.[275] Während manche EU-Mitgliedstaaten in solchen Fällen eine inländische Datenspeicherung unterstellen und den direkten Zugriff auf die Daten wie unter eindeutig inländischen Umständen handhaben, richten sich andere bei potentiellem oder feststehendem Auslandsbezug nach weiteren Zugriffsvoraussetzungen („safeguards“).[276]
Soweit elektronische Beweismittel im regulären Rechtshilfeverfahren erlangt werden sollen, stellt sich dieses Verfahren zunehmend als problematisch dar:[277] kritisiert wird länderübergreifend nicht nur, dass die Bearbeitung von Tätigkeitsersuchen zu lange dauere, sondern auch, dass es keine fixen Bearbeitungsfristen gebe und die Verfahren komplex und zudem von Land zu Land unterschiedlich seien.[278] Schließlich werden selbst in diesen offiziellen Verfahren nur in den wenigsten Fällen sichere Kommunikationswege zum Datenaustausch genutzt,[279] was sowohl in datenschutzrechtlicher Hinsicht als auch im Hinblick auf die Authentizität- und Integritätssicherstellung bedenklich ist.

Insgesamt lässt sich feststellen, dass die Diversität der jeweiligen Regelungen beziehungsweise ihr Fehlen Rechtsunsicherheit für alle Beteiligten verursacht und gleichzeitig ein Hindernis für alle gemeinsamen und grenzüberschreitenden Ermittlungen darstellt.[280] Da die Mehrzahl der elektronischen Beweismittel zunehmend einen grenzüberschreitenden Bezug aufweist – sei es über die Mobilität der Täter, sei es über den Sitz des Dienstleisters beziehungsweise seines Datenkontrollzentrums, sei es über den Speicherort der Daten - handelt es sich um eine Problematik, die nicht rein national gelöst werden kann.[281]

---

275 Europäische Kommission, *Report on the 17 / 18 January 2017 expert meeting*, S. 2.
276 Europäische Kommission, *Report on the 17 / 18 January 2017 expert meeting*, S. 2.
277 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 5.
278 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 5.
279 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 6.
280 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 1; Europol, *IOCTA 2017,* S. 63.
281 Ebenso im Ergebnis und jedenfalls für bestimmte Problemfelder: Rat der Europäischen Union, *Schlussfolgerungen vom 09.06.2016,* S. 2 ff.; Europol, *IOCTA 2017,* S. 63 f.

II. Lösungsansätze auf EU-Ebene

1. Die Schlussfolgerungen des Rates der Europäischen Union vom 09.06.2016[282]

Der Rat der Europäischen Union hat unter Anerkennung der herausragenden Bedeutung elektronischer Beweismittel für den Strafprozess, der Häufigkeit des grenzüberschreitenden Bezuges und der damit verbundenen Probleme, wie sie bereits dargestellt wurden, mit den Schlussfolgerungen vom 09.06.2016 der Europäischen Kommission aufgetragen, Lösungen für folgende Bereiche auszuarbeiten: Verbesserung der direkten Zusammenarbeit der Dienstleister mit den Strafverfolgungsbehörden, Beschleunigung und Vereinfachung des Rechtshilfeverfahrens im Zusammenhang mit elektronischen Beweismitteln und Überprüfung der Anknüpfungspunkte für die Zuständigkeit für Ermittlungsmaßnahmen im „Cyberspace“.[283]

2. Der Zwischenbericht der Europäischen Kommission vom 07.12.2016

Der Zwischenbericht präsentiert ausführlich die einzelnen aktuellen Problemfelder der Praxis, wie sie bereits angeschnitten wurden. Dabei nimmt die direkte Zusammenarbeit vor allem mit den US-amerikanischen Dienstleistern den größten Raum ein.[284] Sodann werden die derzeitigen Schwierigkeiten der Rechtshilfe- und Anerkennungsverfahren analysiert[285] und derzeitig praktizierte Anknüpfungspunkte für Ermittlungszuständigkeiten im Internet untersucht[286]. Im letzten Teil des Berichts werden in allgemeiner Form mögliche praktische und gesetzgeberische Verbesserungsmaßnahmen vorgestellt. Konkret erwähnt die Kommission die Entwicklung eines sicheren online-Portals zum behördlichen Informationsaustausch, die Einrichtung einer zentralen Kontaktstelle („single point of contact“,

282 Ein ausführlicher Überblick über den Kerngehalt der Schlussfolgerungen findet sich bei Brodowski, *Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick,* ZIS 2017, 11 (20).
283 Rat der Europäischen Union, *Schlussfolgerungen vom 09.06.2016*, S. 5 f.
284 Europäische Kommission, *Progress Report,* 07.12.2016, S. 6 ff.
285 Europäische Kommission, *Progress Report,* 07.12.2016, S. 10 ff.
286 Europäische Kommission, *Progress Report,* 07.12.2016, S. 12 ff.

SPOC) sowohl auf Behörden- als auch auf Providerseite, Fortbildungsmaßnahmen, Standardisierungen und die Verringerung der Anzahl der verwendeten behördlichen Formulare, die Angleichung der formellen Vorgaben der Provider, die Errichtung einer online-Plattform zu Informationszwecken für die Strafverfolgungsbehörden über die providerabhängigen unterschiedlichen Anfragevoraussetzungen, die Überarbeitung bestehender Rechtshilfe- und Rechtsanerkennungsabkommen insbesondere mit den USA, die konkrete Ausgestaltung der Mitwirkungspflichten der ausländischen Dienstleister und denkbare Ansätze für den direkten Zugriff der Strafverfolgungsbehörden auf - möglicherweise oder sicher - im Ausland befindliche Daten.[287] Ein Schwerpunkt liegt zudem auf einer Harmonisierung der Datenklassifikation auf EU-Ebene.[288]

3. Der Abschlussbericht der Europäischen Kommission Services vom 22.05.2017

Der am 22.05.2017 von den Europäische Kommission Services veröffentlichte Abschlussbericht zum durchgeführten Expertenprozess besteht aus einem technischen Dokument und einem dazugehörigen komprimierten Kurzbericht als Zusammenfassung.

Das ausführliche technische Dokument nimmt auf 31 Seiten eine im Vergleich zum Zwischenbericht vom Dezember 2016 erweiterte Problemdarstellung vor. Genannt werden ergänzend die unterschiedliche Anwendung von Kriterien, mit denen im Hinblick auf die Erlangung elektronischer Daten bestimmt werde, ob überhaupt ein grenzüberschreitender Bezug vorliege, daneben das stetig wachsende Anfragevolumen, die bestehende Rechtsunsicherheit, die Frage, nach welchen Maßstäben und von wem der Nutzer von einer Datenbeauskunftung zu unterrichten sei, sowie die besondere Problematik im Zusammenhang mit „Corporate Customers“.[289]

Sodann wird im Detail auf folgende konkrete praktische

287 Europäische Kommission, *Progress Report,* 07.12.2016, S. 16 ff.
288 Europäische Kommission, *Progress Report,* 07.12.2016, S. 18 f.
289 Europäische Kommission Services, *Technical Document*, S. 5 ff.

Verbesserungsmöglichkeiten eingegangen: die Einrichtung einer zentralen Kontaktstelle jeweils auf Behörden- und Providerseite, die Angleichung der formellen Vorgaben der Provider, Standardisierungen und die Verringerung der Anzahl der verwendeten behördlichen Formulare, Fortbildungsmaßnahmen für die Strafverfolgungsbehörden und die Errichtung einer online-Plattform zu Informationszwecken für die Strafverfolgungsbehörden über die providerabhängigen unterschiedlichen Anfragevoraussetzungen, die Fortentwicklung eines einheitlichen elektronischen Formulars für die Europäische Beweisanordnung und die Entwicklung eines sicheren online-Portals zum verbesserten Informationsaustausch der EU-Behörden, das ab dem Sommer 2019 einsatzbereit sein soll, sowie der Austausch von „best practices“ und Fortbildungsmaßnahmen.[290]

Als mögliche gesetzgeberische Lösungen werden folgende Ansätze genannt: die Schaffung einer Ermächtigungsgrundlage für behördliche Auskunftsverlangen, die Klarstellung der Auskunftsbefugnis inländischer Dienstleister gegenüber ausländischen Strafverfolgungsbehörden, die Verpflichtung von Dienstleistern, die keinen Sitz in der EU haben, hier einen rechtlichen Vertreter zu benennen, die Festlegung von im Einzelnen näher beschriebenen Mindeststandards für den direkten Zugriff der Strafverfolgungsbehörden auf im Ausland gespeicherte Daten und schließlich der Abschluss multilateraler oder bilateraler Vereinbarungen mit Nicht-EU-Staaten.[291]

Der nun folgende Schlussteil beschäftigt sich mit Aspekten, die für jegliche gesetzgeberische Lösungen bedacht werden müssten.[292]

Bei der ergänzenden Problembeschreibung wird erneut die unterschiedliche Begriffsverwendung bei der Datenkategorisierung aufgegriffen und beispielhaft auf die IP-Adresse verwiesen, die wahlweise als Bestandsdatensatz oder als Verkehrsdatensatz subsumiert werde; zudem umfasse die herkömmliche Kategorisierung nicht alle potentiell relevanten Daten.[293] Weil die einschlägige

290 Europäische Kommission Services, *Technical Document*, S. 11 ff.
291 Europäische Kommission Services, *Technical Document*, S. 20 ff.
292 Europäische Kommission Services, *Technical Document*, S. 30 f.
293 Europäische Kommission Services, *Technical Document*, S. 6.

Datenkategorie maßgeblich für die jeweiligen prozessualen Schutzbestimmungen sei, führe die uneinheitliche Begriffsverwendung zu ungleichen Sicherungsstandards, zu Gesetzeskonflikten und in praktischer Hinsicht zu Missverständnissen zwischen der anfragenden Strafverfolgungsbehörde und dem Adressaten im Ausland.[294]

Daran anknüpfend wird unter den legislativen Verbesserungsvorschlägen an erster Stelle die Vereinheitlichung der Definition unterschiedlicher Datenklassen auf EU-Ebene genannt.[295] Die Sachverständigen hätten eine Harmonisierung der üblicherweise verwendeten Begriffe, die Einbeziehung derzeitiger Definitionen (etwa in der Cybercrime-Konvention, in der DS-Richtlinie oder im aktuellen Vorschlag der Europäischen Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation[296]) und Überlegungen, wie Daten außerhalb des klassischen Kommunikationsbegriffes einzuordnen seien, angeregt.[297] Bei der Begriffsbestimmung sei eventuell zu berücksichtigen, von wem die Datenherausgabe verlangt werde (bei Dienstleistern etwa in Abhängigkeit von der Art der Dienstleistung) und ob die Datenerlangung über einen Dritten oder direkt erfolge.[298] Da von mehreren Beteiligten betont worden sei, dass jegliche Datenkategorisierung technikneutral sein müsse, um beständig sein zu können, sei parallel an die Einrichtung eines „Wörterbuches“[299] auf technischer Ebene zu denken.

Im Hinblick auf die Schutzwürdigkeit elektronischer Daten, so der Abschlussbericht, sei davon auszugehen, dass der Zugriff auf Bestandsdaten generell von geringerer Eingriffsintensität sei, während der Zugriff auf Inhaltsdaten grundsätzlich am schwerwiegendsten sei.[300] Allerdings sei es unklar, wo in diesem Zwischenbereich der Zugriff auf Metadaten anzusiedeln sei; die „Tele2 / Watson“ -

294 Europäische Kommission Services, *Technical Document*, S. 6.; ähnlich auch Europarat, T-CY, *Final Report*, 16.09.2016, S. 7 f.
295 Europäische Kommission Services, *Technical Document*, S. 18 f.
296 Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation* vom 10.01.2017.
297 Europäische Kommission Services, *Technical Document*, S. 19.
298 Europäische Kommission Services, *Technical Document*, S. 19.
299 Der Originaltext spricht von „technical library“ (s. Europäische Kommission Services, *Technical Document*, S. 19).
300 Europäische Kommission Services, *Technical Document*, S. 31.

Entscheidung es Europäischen Gerichtshofes vom Dezember 2016[301] deute darauf hin, dass es sich hierbei ebenfalls um eine eher sensible Datenkategorie handele.[302]

4. Der Gesetzesvorschlag der Europäischen Kommission vom 17.04.2018

Unmittelbar nach der Veröffentlichung des Abschlussberichts vom 22.05.2017 haben die EU-Mitgliedstaaten beim Ratstreffen „Justiz und Inneres“ am 08.06.2017 die Europäische Kommission aufgefordert, die vorgeschlagenen praktischen Maßnahmen umzusetzen und baldmöglichst die angedachten Gesetzesvorschläge zu konkretisieren.

Während die Umsetzungsphase für die praktischen Maßnahmen noch andauert,[303] hat die Europäische Kommission am 17.04.2018 einen Gesetzesentwurf für einen erleichterten Zugang der Strafverfolgungsbehörden zu grenzüberschreitenden elektronischen Beweismitteln vorgestellt.[304] Der Entwurf umfasst einen Verordnungs- und einen Richtlinienvorschlag.

a) Verordnungsvorschlag

Der Verordnungsvorschlag[305] sieht die Einführung einer Europäischen Vorlageanordnung („European Production Order“) vor, die es den Strafverfolgungsbehörden der Mitgliedstaaten ermöglichen soll, elektronische Daten, die als Beweismittel in Betracht kommen,[306] direkt von einem ausländischen Dienstleister anzufordern – unabhängig davon, wo dieser seinen Sitz, etwaige Niederlassungen, etwaige

301 EuGH, Urteil vom 21.12.2016 („Tele2 / Watson“), C-203/15 und C-698/15.
302 Europäische Kommission Services, *Technical Document*, S. 31.
303 Stand: 30.04.2018; s. Seite der Generaldirektion Migration und Inneres (https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en).
304 Europäische Kommission, *Pressemitteilung vom 17.04.2018*.
305 COM(2018) 225 final; die amtliche deutsche Übersetzung liegt derzeit noch nicht vor (Stand: 30.04.2018).
306 Für Bestands- und Zugangsdaten („subcriber data“ und „access data“) soll die Europäische Vorlageanordnung gemäß Art. 5 Abs. 3 des Vorschlags für alle Straftaten in Betracht kommen, während sie bei Verkehrs- und Inhaltsdaten („transactional data“ und „content data“) gemäß Art. 5 Abs. 4 des Vorschlags nur bei besonders schweren Straftaten, die konkret benannt werden, zur Anwendung kommen soll.

Datenkontrollzentren oder sein Datenspeicherzentrum unterhält. Voraussetzung ist lediglich, dass der Dienstleister in der EU tätig ist.[307] Nach Erhalt der Europäischen Vorlageanordnung soll der Dienstleister zur Auskunftserteilung binnen 10 Tagen, im Notfall sogar binnen 6 Stunden verpflichtet sein.[308]
Zur vorläufigen Datensicherung soll zudem das Instrument der Europäischen Datenspeicherungsanordnung („European Preservation Order“) eingeführt werden. Die vorgeschlagene Datenspeicherungspflicht, die ohne Verlängerungsanordnung nach 60 Tagen erlöschen soll, bezieht sich ausschließlich auf die Datensätze, die bei Erhalt der Anordnung bereits in gespeicherter Form beim Dienstleister vorlagen, nicht also auf danach erst entstehende Datensätze.[309]

Ein wirkliches Novum des Verordnungsvorschlags liegt zum einen in der Einführung einer weiteren Datenkategorie, den Zugangsdaten („access data“). Sie stellen eine Unterart der Verkehrsdaten dar und sollen wegen ihrer herausragenden Bedeutung für die Strafermittlung und der geringeren Eingriffsintensität den geringeren Anforderungen, die für Bestandsdaten gelten, unterliegen.[310]

Zum anderen sind die vorgeschlagenen Anordnungsinstrumente so konzipiert, dass sie für den im EU-Ausland adressierten Dienstleister unmittelbar rechtlich verbindlich sein sollen, ohne dass es – wie sonst im zwischenstaatlichen Rechtsverkehr üblich – irgendeiner Mitwirkung oder Benachrichtigung des betroffenen Zielstaates bedarf.[311] Der Zielstaat soll lediglich im Rahmen der Vollstreckung der Anordnung tätig werden müssen.[312]

b) Richtlinienvorschlag

Um zu gewährleisten, dass das Anknüpfungskriterium des Tätigseins in

307 Der englische Text spricht von „offering services“; s. Art. 3 Abs. 1 des Verordnungsvorschlags.
308 Art. 9 Abs. 1, 2 des Verordnungsvorschlags.
309 Art. 2 Nr. 6 i.V.m. 10 Abs. 1 des Verordnungsvorschlags.
310 Vgl. Art. 2 Nr. 8, 9 des Verordnungsvorschlags sowie amtliche Begründung S. 13 f.
311 Art. 2 Nr. 1, 2 des Verordnungsvorschlags.
312 Vgl. Art. 14 des Verordnungsvorschlags.

der EU auf alle Dienstleister einheitlich angewandt wird, sieht der ergänzende Richtlinienentwurf[313] die Verpflichtung für alle hier tätigen Dienstleister vor, einen gesetzlichen Vertreter („legal representative“) in der Europäischen Union zu benennen, der im Zusammenhang mit der Erhebung von Beweismitteln in Strafverfahren für die Einhaltung und Vollstreckung von Beschlüssen und Anordnungen der zuständigen Behörden der Mitgliedstaaten verantwortlich ist.[314]

313 COM(2018) 226 final; die offizielle deutsche Übersetzung liegt derzeit noch nicht vor (Stand: 30.04.2018).
314 Europäische Kommission, *Pressemitteilung vom 17.04.2018*.

D. Klassifizierung elektronischer Daten für strafprozessuale Zwecke

Das deutsche Strafverfahrensrecht erkennt elektronische Daten als potentielle Beweismittel an, ohne sie in allgemeiner Form zu definieren, zu umschreiben oder zu bestimmen. Es wurde ausführlich dargelegt, dass im Rahmen von Strafermittlungsverfahren zunehmend auf sie zurückgegriffen wird. Für ihre Erlangung und Verwertung stehen verschiedene Ermittlungsmaßnahmen zur Verfügung.
Weil es in der Praxis weder möglich noch sinnvoll ist, die Eingriffsvoraussetzungen für jeden Datensatz individuell festzulegen, werden elektronische Daten ganz im Sinne der modernen Gesetzgebungslehre, wie sie bereits angesprochen wurde,[315] kategorisiert, um generelle, pauschale Aussagen über ihre Sensibilität, also über ihre Schutzwürdigkeit, und damit mittelbar über notwendige Eingriffsvoraussetzungen zu erlauben.

Im Folgenden werden die derzeit in der StPO verwendeten Datenkategorien dargestellt und sodann untersucht, ob sich die derzeitige Differenzierung an rechtlich bedeutsamen und / oder sonstigen Kriterien orientiert (dazu unter I. und II.).
Die Analyse wird in einem ersten Zwischenergebnis ergeben, dass sich die derzeitige Kategorisierung nicht vorrangig nach rechtlich relevanten Merkmalen richtet, daher Zweifel an der Verfassungsmäßigkeit ihrer Zugrundelegung in der StPO bestehen und, weil die derzeitige Einteilung einen Großteil potentiell relevanter Daten unberücksichtigt lässt, eine Neuklassifizierung sinnvoll ist.

Um sie vornehmen zu können, folgt im Rahmen von Vorüberlegungen (III.) zur angestrebten Neuklassifizierung eine rechtstheoretische Erörterung ihrer Erforderlichkeit, die im zweiten Zwischenergebnis festgehalten wird. Sodann werden die für eine Neuklassifizierung unumgänglichen Prämissen sowie die aktuell diskutierten alternativen Abgrenzungskriterien untersucht. Dies führt zu dem dritten Zwischenergebnis, dass sie sämtlich keine befriedigende Lösung

315 Kapitel A II Ziff. 1.

bieten.

Nach den einschlägigen verfassungsrechtlichen Vorgaben, die ausführlich dargestellt werden, ergibt sich als neues, maßgebliches Differenzierungsmerkmal die berechtigte Erwartungshaltung des Datenberechtigten in Bezug auf die Wahrung der Vertraulichkeit bezüglich eines bestimmten Datensatzes (IV.).

Mit diesem Kriterium kann nachfolgend eine Datenkategorisierung in fünf Klassen erfolgen, die der verfassungsmäßigen Werteordnung entspricht und daher als Grundlage einer Neukonzeptionierung der StPO herangezogen werden kann.

Die Gegenüberstellung der herkömmlichen und der neuen Klassifizierung (V.) bilden mit der Darstellung ausgewählter Zuordnungsbeispiele (VI.) den Abschluss dieses Kapitels.

I. Derzeitige Kategorisierungen

Die wenigen expliziten Bezugnahmen auf elektronische Beweismittel im deutschen Strafverfahrensrecht differenzieren nur in Ausnahmefällen zwischen verschiedenen Datenkategorien. Von diesen werden folgende genannt:

1. Personenbezogene Daten

Personenbezogene Daten (§§ 98a ff., 101a, 483 ff. StPO), speziell solche, die den Kernbereich privater Lebensgestaltung betreffen (§ 100d StPO) und DNA-Identifizierungsmuster (§ 81h Abs. 1 Nr. 3 StPO), gespeicherte und öffentlich zugängliche gespeicherte Daten (§§ 100b, 110 Abs. 3 StPO, Art. 32 lit. a) der Cybercrime-Konvention), Daten aus einer laufenden Kommunikation (§ 100a StPO) sowie innerhalb der Kommunikationsdaten bei leicht abweichender Begriffsverwendung Verkehrsdaten (§§ 100g StPO i.V.m. 96 Abs. 1 TKG, Art. 1 lit. d) der Cybercrime-Konvention), Bestandsdaten (§§ 100j StPO i.V.m. 95, 111 Abs. 1 TKG, Art. 18 Abs. 3 der Cybercrime-Konvention) und Inhaltsdaten (gefestigte höchstrichterliche Rechtsprechung und Art. 18 Abs. 3 der Cybercrime-Konvention).

2. DNA-Identifizierungsmuster

Während bei den personenbezogenen Daten einschließlich derer, die den Kernbereich privater Lebensgestaltung betreffen, die inhaltliche Ausgestaltung dem Datenschutzrecht beziehungsweise der Rechtsprechung überlassen bleibt, bezieht sich die Kategorie der DNA-Identifizierungsmuster auf einen ganz spezifischen biologisch-technischen Inhalt.
In allen Fällen gibt es kein konkretes Gegenstück, keine Negativabgrenzung, sondern nur allgemein nicht-personenbezogene Daten, Daten, die nicht den Kernbereich privater Lebensgestaltung betreffen, und Daten, deren Inhalt nicht aus DNA-Identifizierungs-mustern besteht.

3. Gespeicherte Daten

Die Fallgruppe gespeicherter Daten (mit der Untergruppe öffentlich zugänglicher gespeicherter Daten) ist auf den Datenzustand zum Zeitpunkt des Zugriffes der Strafverfolgungsbehörde zurückzuführen. Ihr stehen Daten aus laufender Kommunikation gegenüber. Damit werden solche Daten, die, ohne Kommunikationsdaten zu sein, zum Zeitpunkt des staatlichen Zugriffs gerade lokal entstehen oder ohne Speicherung verarbeitet, also insbesondere zeitgleich aus dem Internet oder der Cloud heruntergeladen werden, von keiner der beiden Alternativen erfasst.

4. Kommunikationsdaten

Eine konkrete, detaillierte Untergliederung elektronischer Beweismittel ist lediglich für den Bereich der Kommunikationsdaten festzustellen. Diese werden durch Bestands-, Verkehrs- und Inhaltsdaten vollständig beschrieben. Aufgrund der enormen Praxisrelevanz dieser Art elektronischer Daten hat sich ihre Unterscheidung, wie bereits ausführlich dargestellt, in vielen Ländern durchgesetzt; sie werden im folgenden Kapitel gesondert betrachtet.

5. Stellungnahme

Insgesamt lässt sich feststellen, dass im deutschen Strafprozessrecht verschiedene Differenzierungskriterien zur punktuellen Unterscheidung unterschiedlicher Arten von elektronischen Beweismitteln angesetzt werden, die jedoch bis auf den Bereich der Kommunikationsdaten keine umfassende Klassifizierung erlauben. Die Anwendung verschiedener Differenzierungskriterien führt zu Überschneidungen dergestalt, dass beispielsweise ein Großteil der erfassten Datenklassen personenbezogene Daten beinhaltet, sich Daten aus einer laufenden Kommunikation ebenso wie gespeicherte Daten sowohl auf Bestands-, Verkehrs- und Inhaltsdaten beziehen können und Kernbereichsdaten potentiell jedenfalls einen Teil der Kommunikationsinhaltsdaten aber gegebenenfalls auch nicht kommunizierte Inhalte abdecken.

Querverweise auf Rechtsgebiete außerhalb der StPO wie das Telekommunikations- oder das Datenschutzrecht indizieren ebenso wie die teilweise Überlappung einzelner Kategorien, dass die strafprozessrechtlichen Regelungen keiner konzeptionellen Struktur bei der Erfassung elektronischer Beweismittel folgen.

II. Spezialfall Kommunikationsdaten

In den folgenden Abschnitten wird die derzeitige Einteilung der Kommunikationsdaten vorgestellt (dazu unter 1.), bevor die Entstehung dieser Kategorisierung dargelegt (2.) und ihre rechtliche Problematik erläutert werden (3.).

1. Bestands-, Verkehrs- und Inhaltsdaten

Die derzeit im Strafverfahrensrecht angewandte Kategorisierung der Kommunikationsdaten unterscheidet explizit zwischen Bestandsdaten, Verkehrsdaten und Inhaltsdaten. Der allgemeinen Auffassung folgend ist bei dieser Reihenfolge von zunehmender Sensibilität der jeweiligen Datensätze auszugehen. Das bedeutet, dass Bestandsdaten generell als weniger schutzwürdig als Verkehrsdaten gelten, die ihrerseits einen geringen Schutz vor staatlicher Kenntnisnahme als Inhaltsdaten erfahren.[316] Diese Annahme liegt – ohne nähere Begründung - auch der vergleichbaren Begriffsverwendung im internationalen Kontext zugrunde.[317]

316 So ausdrücklich Europarat, T-CY, *Final Report*, 16.09.2016, S. 38; zum Verhältnis von Kommunikationsinhaltsdaten zu sonstigen Kommunikationsdaten: BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 70; Europäische Kommission Services, *Technical Document*, S. 31; zum Verhältnis von Bestandsdaten („Teilnehmerdaten“) zu sonstigen Daten: Rat der Europäischen Union, *Schlussfolgerungen vom 09.06.2016*, S. 5.

317 Vgl. Europarat, *Erläuternder Bericht zur Cybercrime-Konvention*, Abschnitt 230; Europarat, T-CY, *Final Report*, 16.09.2016, S. 12 f., 38; Europäische Kommission Services, *Technical Document*, S. 6, 19, mit dem ergänzenden Hinweis, dass statt Verkehrsdaten auch von Metadaten oder Transaktionsdaten („transactional data“) gesprochen wird. Gemäß Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*, S. 3, fehlt es allerdings jedenfalls in Estland, Italien, Kroatien, Luxemburg und Ungarn überhaupt an einer gesetzlichen strafprozessualen Datenkategorisierung. Auch der EGMR geht davon aus, dass die Überwachung des Kommunikationsflusses („flow of the communications“) weniger eingriffsintensiv als die des Kommunikations-inhaltes („content of communication“) sei (EGMR, Urteil vom 05.09.2017 („Bărbulesu v. Romania“), appl. no. 61496/08, Rn. 121).
In den USA wird über Titel 18 § 2702 des US Federal Criminal Codes, der über den Electronic Communications Privacy Act of 1986 (ECPA) eingeführt wurde, bei gespeicherten Daten unterschieden zwischen Inhaltsdaten und Nicht-Inhaltsdaten ("non-content data"), wobei letztere nach Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (672), in Bestandsdaten ("basic subscriber information")

2. Begriffsentstehung

Bevor das Internet 1990 kommerziell nutzbar und damit frei zugänglich,[318] 1991 das World Wide Web für die Öffentlichkeit eingeführt[319] und Anfang der 1990-er Jahre die ersten digitalen Mobilfunknetze in Betrieb genommen wurden,[320] war die Bedeutung elektronischer Daten als Beweismittel im Strafprozess verschwindend gering. Dies lag zum einen an der geringen Menge vorhandener elektronischer Daten und zum anderen daran, dass ein Großteil der vorhandenen Daten das Resultat der Digitalisierung solcher Informationen war, die in anderer beweistauglicher Form existierten: Im Zweifel wurde auf das papierne Dokument und das entwickelte Foto und nicht auf ihre eingescannte elektronische Form zurückgegriffen.

Mit der technischen Weiterentwicklung der Telekommunikation von analoger zu originär digitaler Informationsübermittlung änderte sich der Fokus zunächst allein in diesem Bereich, der aufgrund der Bedürfnisse der Telekommunikationsanbieter zwischen Kunden-, Abrechnungs- und sonstigen Daten unterschied.
Die Verfügbarkeit der Kundendaten war erforderlich, um die monatlichen Rechnungen dem Kunden in Papierform zukommen zu lassen - Prepaid-Verträge und online-Rechnungsstellung waren faktisch nicht existent - und Auskünfte über bestehende Anschlüsse zu erteilen.[321] Zum Nachweis der Richtigkeit der Abrechnung mussten detaillierte Angaben zu den abgerechneten Verbindungen vorgelegt werden können, also insbesondere die angewählte Rufnummer mit konkreten Zeitangaben. Der Inhalt der Kommunikation war für die

und Verkehrsdaten ("transactional data") untergliedert werden. Svantesson, *Data categorisation and law enforcement access to cloud data*, beschreibt als gebräuchliche Klassifizierung ein 2-Klassen-Modell („metadata and data“) oder das beschriebene 3-Klassen-Modell.

318 Wikipedia, Suchbegriff *Internet.*

319 Wikipedia, Suchbegriff *World Wide Web.*

320 Laut Wikipedia, Suchbegriff *Mobilfunk*, wurde in Deutschland das erste digitale Mobilfunknetz im Jahr 1992 eingeführt.

321 Eine Auskunft konnte von jedem beliebigen Dritten über Sondernummern fernmündlich oder mithilfe des Telefonbuches eingeholt werden, wobei der dortige Eintrag „lange Zeit für jeden Anschlussinhaber verpflichtend“ war (Wikipedia, Suchbegriff *Telefonbuch*) und außer dem Namen und Vornamen des Anschlussinhabers häufig auch die Adresse beauskunftet wurde.

Telekommunikationsdienstleister hingegen bedeutungslos.

Die dadurch vorgegebene Einteilung in Kunden-, Verbindungs- und Inhaltsdaten basierte auf dem Leitbild einer ortsgebundenen, individuellen Kommunikation zwischen zwei Personen. Ihre Adaption im Strafprozessrecht als unmittelbare Konsequenz der zunehmenden Digitalisierung des Fernmeldeverkehrs[322] fügte sich nahtlos in die Unterscheidung ein, die hinsichtlich der Eingriffsintensität in das Brief-, Post- und Fernmeldegeheimnis aus Art. 10 GG für die klassische Kommunikation in Schriftform bis heute angewandt wird: die Informationen, die einem verschlossenen Brief mittelbar und unmittelbar zu entnehmen sind,[323] unterliegen geringeren Zugangsvoraussetzungen als der Inhalt eines solchen Briefes, der gemäß § 100 Abs. 3, 4 StPO nur nach gesonderter richterlicher Entscheidung über die Brieföffnung erfasst werden darf.

Die von den Telekommunikationsdienstleistern vorgegebene Daten-einteilung, die in Deutschland bereits 1996 im Datenschutzrecht kodifiziert wurde,[324] wurde sukzessive zwischen 2001 und 2015 in die StPO übernommen.[325] Auch nach der tatsächlichen Erweiterung des für die Strafermittlungsbehörden relevanten Datenspektrums insbesondere nach Verbreitung des Smartphones ab ca. 2007,[326] durch das beispielsweise die Massenkommunikation in Sozialen Netzwerken auf

322 Vgl. Hauck, in: Löwe-Rosenberg, *StPO*, § 100g, Entstehungsgeschichte (zitiert nach juris).

323 Zu denken ist hierbei in erster Linie an die Information darüber, mit wem eine Person von wo nach wo in welcher Häufigkeit und in welchem Umfang kommuniziert.

324 Der Vorläufer des TKG, die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (TDSV), definierte in seiner Fassung vom 12.07.1996 in § 4 Abs. 1 den Begriff der Bestandsdaten und in § 5 Abs. 1 den der Verbindungsdaten. Nach der Gesetzesbegründung zur ursprünglichen Fassung der §§ 93 f. TKG vom 22.06.2004, die ausdrücklich Bestandsdaten und Verkehrsdaten zum Gegenstand haben, beziehen sich beide Begriffe auf die §§ 4 f. TDSV (BT-Drucks. 15/2316, S. 88 f.).

325 Während § 100g Abs. 3 StPO in der Fassung vom 20.12.2001 erstmals den Begriff „Telekommunikationsverbindungsdaten“ verwendet und diese einzeln auflistet, verweist § 100g Abs. 3 StPO in der Fassung vom 21.12.2007 erstmals ausdrücklich auf „Verkehrsdaten“ im Sinne des TKG. Der erste Verweis auf Bestandsdaten im Sinne des TKG findet sich – ohne ausdrückliche Verwendung des Begriffes – in § 100j Abs. 1 StPO in der Fassung vom 20.06.2013; die Bezeichnung selbst taucht erstmals in der Überschrift des § 100j StPO in der Fassung vom 17.07.2015 auf.

326 Wikipedia, Suchbegriff *Smartphone.*

Sprach-, Text- und Bildebene erst ermöglicht wurde und nunmehr originär digitale Kalender- und Adressbucheinträge eher die Regel als die Ausnahme sind, und der neuesten Zunahme von Maschine-zu-Maschine Kommunikation wird die bisherige Datenklassifizierung bis heute angewandt und auf die zugrundeliegende Annahme der unterschiedlichen Eingriffsintensitäten zurückgegriffen.

3. Problematik der aktuellen Begriffsverwendung

Die aktuelle Begriffsverwendung ist in verschiedener Hinsicht problematisch: Zum einen bezieht sie sich ausschließlich auf Kommunikationsdaten (dazu unter a)), wobei die Unterscheidung nicht stringent für alle Beweismittel eingehalten wird (b)). Zudem haben sich seit ihrer Entstehung nicht nur das Kommunikationsverhalten der Nutzer (c)) sondern auch die Datenbedürfnisse der Kommunikations-anbieter geändert (d)). Schließlich sind die Strafverfolgungsbehörden im Bereich der elektronischen Beweismittel zunehmend auf die internationale Zusammenarbeit angewiesen, die erschwert wird, wenn mit den einheitlich verwendeten Begriffen unterschiedliche Bedeutungen assoziiert werden (e)).

a) Beschränkung auf Kommunikationsdaten

Die derzeitige Einteilung bezieht sich ausschließlich auf Kommunikationsdaten, sie ist daher von vorneherein lückenhaft. Sie ist zudem in ihrer praktischen Anwendung nicht stringent.

Unabhängig davon, wie der Begriff der Kommunikation im strafprozessualen Sinn genau zu verstehen ist,[327] verbleibt es selbst bei weitestmöglicher Auslegung bei Datensätzen, die nicht erfasst werden und gleichzeitig durchaus für die Strafermittlungsbehörden relevant sein können. Dies gilt etwa für alle Daten, die lediglich auf einem Speichermedium des Datenerzeugers - etwa dem Computer des

327 Zu möglichen Auslegungen und dem herrschenden Verständnis des strafprozessualen Kommunikationsbegriffes: Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 4 ff., zitiert nach juris).

Verdächtigen - abgelegt und nie auf ein anderes Gerät übertragen worden sind. Zudem ist an den Informationsaustausch im Rahmen des Internets der Dinge zu denken. Es beschreibt die Vernetzung verschiedener Geräte, die über das Internet einen Informationsaustausch durchführen, ohne dass daran eine Person unmittelbar beteiligt wäre. Dadurch entstehen elektronische Daten, die nicht mehr als Kommunikation im Sinne von sozialer Interaktion zwischen zwei oder mehreren Personen subsumiert werden können, die aber dennoch einem Informationsaustausch dienen.

Auch wenn Kommunikationsdaten derzeit einen erheblichen Anteil an der Gesamtheit der strafprozessual relevanten elektronischen Beweismittel haben, so rücken aufgrund der Digitalisierung des Alltags und der wachsenden Verbreitung des Internets der Dinge die sonstigen Daten zunehmend in den Blickpunkt der Strafverfolgungsbehörden.[328] Auch sie weisen hinsichtlich ihrer Sensibilität eine erhebliche Bandbreite auf, weil die Kreation eines jeglichen elektronischen Datensatzes letztlich auf eine menschliche Entscheidung beziehungsweise auf ein menschliches Verhalten zurückzuführen ist[329] – beispielsweise sorgt der smarte Kühlschrank für die automatisierte Nachbestellung der Milchvorräte nur, weil er entsprechend programmiert und in Betrieb genommen wurde, und sendet die elektronische Fußfessel bestimmte Geokoordinaten nur, weil der sich der Träger an einem bestimmten Ort aufhält. Es dürfte weitgehend Einigkeit darüber bestehen, dass die jeweils betroffenen elektronischen Daten unterschiedlich schutzwürdig sind.
Das gilt, um ein weiteres Beispiel zu nennen, ersichtlich auch für die Aufnahmedaten einer Kamera, die an einen Bewegungsmelder gekoppelt ist und das Bildmaterial automatisch an einen bestimmten Empfänger versendet: das identische Gerät kann als „Fotofalle“ zur Tierbeobachtung ebenso und unter identischer Programmierung eingesetzt werden wie zur Überwachung des Personenverkehrs an bestimmten Orten.

---

328 Vgl. nur Heller, *Alexa, war es Mord?*.
329 Vgl. Mason, *Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now – But they Don`t Know it,* Computer and Telecommunications Law Review, 2017, Volume 23, Issue 8, S. 213 (214), m.w.N.

In der derzeitigen Praxis werden für den strafprozessualen Zugang und die forensische Verwertung sämtliche Nicht-Kommunikationsdaten einheitlich behandelt; insbesondere kommen nach der Rechtsprechung des Bundesverfassungsgerichts die §§ 94 f. StPO für die Sicherung und Beschlagnahme aller elektronischen Daten zur Anwendung, wenn die Maßnahme offen und nicht heimlich erfolgt, die Daten nur punktuell und auf den Ermittlungszweck begrenzt erhoben werden, es sich um Daten außerhalb eines laufenden Kommunikationsvorganges handelt und derjenige, dem die Daten zuzurechnen sind, eine Einwirkungsmöglichkeit auf den Datenbestand hat; dies soll unabhängig davon gelten, bei wem die Daten gespeichert sind und um welche Art von Daten es sich handelt.[330]

Eine Gleichbehandlung ist jedenfalls solange rechtlich fragwürdig, wie nicht für alle Daten der größtmögliche Schutz gewährleistet wird. Dies gilt insbesondere bei der Anwendung der §§ 94 f. StPO, die nur ein vergleichsweise niedriges Schutzniveau gewähren. Hier drängt sich der Schluss auf, dass entgegen verfassungsrechtlichen Vorgaben wesentlich Ungleiches gleich behandelt wird.

Umgekehrt gelten für die Datenerhebungen im Rahmen einer online-Durchsuchung gemäß § 100b StPO für alle auf dem Gerät vorhandenen Daten dieselben Maßstäbe, die der Gesetzgeber unter Verweis auf die einschlägige Rechtsprechung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung als besonders hoch beurteilt.[331]
Wenn unterstellt wird, dass diese hohen Maßstäbe den verfassungsrechtlichen Anforderungen für den Zugriff selbst auf sensibelste Daten gerecht werden, so ist es aus verfassungsrechtlicher Sicht unschädlich, dass unter diesen Voraussetzungen auch auf weniger sensible Daten zugegriffen werden kann.

330 Vgl. BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, und BVerfG, Urteil vom 02.03.2006, 2 BvR 2099/04, zugleich BVerfGE 115, 166.
331 Vgl. Gesetzesbegründung zu §§ 100a ff. StPO, BT-Ausschussdrucks. 18(6)334, S. 10.

b) Differenzierung je nach angewandtem Beweismittel

Ein Bruch der derzeitigen Datenklassifikation besteht außerdem darin, dass die Differenzierung in Abhängigkeit vom angewandten Beweismittel vorgenommen wird. Mit anderen Worten fehlt es an einer stringenten Anwendung der derzeitigen Klassifizierung: Nach der aktuellen Rechtslage wird bei Informationen über eine Kommunikation für die Zugriffsmöglichkeit der Strafverfolgungsbehörde nach Bestands-, Verkehrs- und Inhaltsdaten unterschieden, wenn ihr Nachweis mithilfe des Beweismittels elektronische Daten erfolgen soll, während der Nachweis etwa mithilfe des Zeugen- oder Urkundsbeweises eine solche Differenzierung nicht kennt. Der Zeuge kann unterschiedslos zu den äußeren Umständen einer Kommunikation (ob, wann, wo, mit wem, wie lange etc.) als auch zu deren Inhalt befragt werden. Entsprechendes gilt für den jeweiligen Inhalt einer Urkunde, die verlesen wird. Es ist aber nicht nachvollziehbar, weshalb die Anwendung der Klassifizierung, die unmittelbaren Bezug zur angenommenen Sensibilität eines Datensatzes hat, vom zur Verfügung stehenden Beweismittel abhängig sein sollte.

Das gilt umso mehr für die derzeit gängige Praxis, bei der mangels eindeutiger Verfahrensregelungen elektronische Daten de facto nicht als eigenständige Beweismittel sondern über die herkömmlichen Beweismittel in die Hauptverhandlung eingeführt werden. Hierdurch werden ohne erkennbare Handlungsvorgabe Beweismittelkategorien vermischt und rechtliche Wertungswidersprüche provoziert.

c) Geändertes Kommunikationsverhalten

Individuelle Kommunikation erfolgt zwar weiterhin per Festnetztelefonie und Briefpost, wird aber spätestens seit der Einführung des Smartphones zunehmend von Mobilfunktelefonie und elektronischer Kommunikation im weiteren Sinne verdrängt.[332] Gemäß dem Sprachgebrauch der Europäischen Kommission sind mit elektronischer Kommunikation sogenannte „Over-the-top“- oder „OTT“-Kommunika-

332 Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation*, 10.01.2017, S. 2.

tionsdienste, also Internetdienste gemeint, die eine interpersonelle Kommunikation ermöglichen[333] und dafür technisch auf der herkömmlichen Übertragungsinfrastruktur aufbauen.[334] Ganz konkret handelt es sich beispielsweise um die Voice-over-IP Telefonie, die im Übrigen als alternative Übermittlungstechnik zunehmend auch von der klassischen Festnetztelefonie eingesetzt wird,[335] die Sofortnachrichten-übermittlung („Instant-Messaging“) und web-gestützte E-Mail-Dienste. Sofern diese Dienste nicht unmittelbar vom Netzanschlussbetreiber zur Verfügung gestellt werden, führt dies dazu, dass das Produkt mindestens eines weiteren Dritten in die Dienstleistungskette eingefügt wird, durch die dem Nutzer die Kommunikation mit anderen ermöglicht wird. Die strafprozessuale Annahme, es handele sich bei klassischer Telekommunikation und moderner Internettelefonie unabhängig von der Beteiligung weiterer Dritter grundsätzlich um wesentlich ungleiche Dienstleistungen, die unterschiedlich zu behandeln seien,[336] ist jedenfalls aus Sicht des Nutzers, der „telefoniert“, und aus Sicht der Telekommunikationsdienstleister, die klassische Telefondienste zunehmend mit Voice-over-IP als Internetdienste durchführen, nicht einleuchtend.

Desweiteren hat sich – technikbedingt – die äußere Form der Nachrichten geändert: Der verschlossene Umschlag des klassischen Briefes, dessen Zweck vor allem darin liegt, die unbefugte Kenntnisnahme des Briefinhaltes durch Dritte zu verhindern, hat zwar in der Vornahme einer Verschlüsselung sein Pendant bei der elektronischen Post, kommt dort aber bei weitem nicht in allen Fällen zur Anwendung. Ohne eine solche Verschlüsselung sind sämtliche Inhaltsdaten von E-Mails, von Voice-over-IP Telefonaten oder von mithilfe von Browsern über das Internet versandte Informationen für

333 Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation*, 10.01.2017, S. 2.
334 Über OTT-Dienste hinaus erfasst das deutsche Telemediengesetz außer den Kommunikationsdiensten auch elektronische Informationsdienste (§ 1 Abs. 1 TMG).
335 Wikipedia, Suchbegriff *IP-Telefonie*.
336 Zur unterschiedlichen rechtlichen Behandlung vgl. nur die ausführlich dargelegten Auskunfts- und Mitwirkungspflichten der dem TKG unterfallenden Telekommunikationsdienstleister und der dem TMG unterfallenden Telemedien-Dienstleister.

jeden am Datentransport beteiligten Dienstleister offen einsehbar.[337] Um in der Diktion des Bundesverfassungsgerichts zu bleiben: Es leuchtet ein, dass unter den genannten Umständen der Inhalt eines verschlossenen Briefes etwas wesentlich Ungleiches im Verhältnis zum unverschlüsselten Inhalt elektronischer Kommunikation ist. Dennoch genießt beides de lege lata als „Kommunikationsinhalt“ einen erhöhten rechtlichen Schutz.[338]

Daneben ist zu beobachten, dass die modernen Kommunikationsdienste zu einer erheblichen Verbreitung von Massenkommunikation geführt haben. Ohne nennenswerten Aufwand ist es heute möglich, über E-Mail-Verteiler, Chatgruppen und diverse Foren zeit- und inhaltsgleich eine Vielzahl von Adressaten anzusprechen.[339]

Schließlich hat die einfache, extrem kostengünstige Art der Kommunikation, die als Text-, Sprach-, Video- oder Bildmitteilung stattfindet, zu einer generellen Trivialisierung der Kommunikationsinhalte geführt, weil der Preis der Fern-Kommunikation, anders als vor Einführung des Internets, in der Regel keine nennenswerte Rolle mehr spielt.

d) Geänderte Datenbedürfnisse der Kommunikationsdienstleister

Nach Einführung der Mobilfunktelefonie, die, anders als die Festnetztelefonie, ortsungebunden ist, und der Möglichkeit, Rechnungen ausschließlich in elektronischer Form zu versenden

337 Bundesamt für Sicherheit in der Informationstechnik, *Verschlüsselung, Verschlüsselt kommunizieren.*

338 Dies gilt jedenfalls gemäß der derzeitigen Kategorisierung elektronischer Daten, unverständlicherweise jedoch nicht für E-Mails, deren Beschlagnahme beim Provider sich einheitlich nach §§ 94 f. StPO ohne Rücksicht darauf richten soll, dass „E-Mails“ sowohl Verkehrs- als auch Inhaltsdaten sowie häufig außerdem Bestandsdaten umfassen.

339 Laut online-Auskunft von http://friendorfollow.com/twitter/most-followers/ vom 28.01.2018, 15:40 Uhr, hat der ehemalige US-Präsident Barack Obama 99.507.862 „Followers“, also Personen, die automatisch jede seiner per Twitter (als einem der größten OTT-Dienstleister) verschickten Nachrichten erhalten; die US-amerikanische Sängerin Katy Perry erreicht mit jeder Twitter-Nachricht unmittelbar sogar 108.474.965 Personen. Die technische Möglichkeit, mit vernachlässigbarem Aufwand eine Vielzahl von Datenübertragungen durchzuführen, wird im kriminellen Bereich etwa bei DDoS-Angriffen genutzt (vgl. Europol, *IOCTA*, S. 27)

beziehungsweise von vorneherein Prepaid-Verträge ohne nachträgliche Rechnungslegung abzuschließen, besteht aus Sicht der klassischen Telekommunikationsdienstleister jedenfalls für diesen Bereich keine Notwendigkeit mehr, Bestandsdaten zu erheben. Gleiches gilt für die meisten Dienstleister, die dem Telemediengesetz unterfallen, insbesondere, wenn sie ihre Dienste unentgeltlich anbieten. Mit unentgeltlich ist in diesem Zusammenhang „ohne unmittelbare Bezahlung“ gemeint; die gewinnbringende Verwertung der erlangten Nutzerdaten ist wirtschaftlich äußerst relevant, erfordert aber nicht notwendig die Erfassung derjenigen Daten, die gemäß § 111 Abs. 1 TKG als Bestandsdaten erhoben werden können.[340]

Die Erhebung sämtlicher bisher benötigter Verkehrsdaten zum Zwecke der Abrechnung mit dem einzelnen Nutzer ist aus Sicht der Dienstleister zwischenzeitlich jedenfalls dort entbehrlich, wo die Internetnutzung über öffentlich zugängliche Hot Spots oder im Rahmen von Flatrates erfolgt. Zudem sind die klassischen Verkehrsdaten für die meisten Telemedien-Dienstleister im Hinblick auf die Erbringung ihrer Dienste irrelevant.

Hingegen ist die Erhebung und Verwendung von Kommunikations-inhaltsdaten durch alle Arten von Internetdienstleistern deutlich in den Vordergrund gerückt – so sehr, dass die politische Ebene zum Schutz der Nutzer bereits reagiert hat.[341]

e) Steigende Relevanz der internationalen Zusammenarbeit und unterschiedliche inhaltliche Bedeutung der verwendeten Begriffe

Aufgrund der Mobilität der Nutzer und ihrer Kommunikationsgeräte, der globalen Infrastruktur des Internets, die unabhängig von Landesgrenzen aufgebaut und zugänglich ist, sowie der grenz-überschreitenden Tätigkeit der großen Kommunikations- und

340 Allgemein zur wirtschaftlichen Bedeutung elektronischer Daten: Dettweiler, *Smart Home, Tausche Daten gegen* Rabatt; Spehr, *Datenauswertung, Die Macht der Algorithmen*.

341 Vgl. beispielsweise Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation*, 10.01.2017.

Informationsdienstleister insbesondere im Bereich der Cloud-Dienste sind die Strafverfolgungsbehörden für die Erlangung elektronischer Daten zunehmend auf Unterstützung aus dem Ausland angewiesen.[342] Unabhängig davon, ob diese Unterstützung von Behörden im Rahmen förmlicher Rechtshilfeverfahren oder direkt von ausländischen Dienstleistern erbracht wird, muss sich jegliche Anfrage auf eine möglichst genaue Beschreibung der gewünschten Datensätze stützen. Gleichzeitig werden die in vielen Ländern genutzten Begriffe der Bestands-, Verkehrs- und Inhaltsdaten oft mit unterschiedlichen Bedeutungsinhalten verknüpft.[343] Dies führt in der Praxis häufig zu ermittlungshemmenden Missverständnissen.

4. Zwischenergebnis

Die strafprozessuale Klassifizierung elektronischer Daten ist außerhalb des Bereiches der Kommunikationsdaten einerseits äußerst allgemein, soweit sie sich beispielsweise auf personenbezogene Daten oder gespeicherte Daten bezieht, andererseits sehr spezifisch und punktuell, soweit sie beispielsweise DNA-Identifizierungsmuster hervorhebt. Eine umfassende Differenzierung, die im erforderlichen Maße unterscheidet und zugleich nicht über das, was ausreichend ist, hinausgeht, fehlt.

Die Aufteilung der Kommunikationsdaten in Bestands-, Verkehrs- und Inhaltsdaten wurde nicht originär nach strafprozessualen Gesichtspunkten entwickelt, sondern entspricht den früheren Bedürfnissen der Telekommunikationsdienstleister. Diese haben sich mit der technischen Fortentwicklung partiell verändert; auf OTT-

342 Ausführlich dazu: Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 3, NZWiSt 2017, 417 (419), m.w.N.; Svantesson, *Data categorisation and law enforcement access to cloud data*.

343 Laut Europäische Kommission Services, *Technical Document*, S. 6, wird beispielsweise die IP-Adresse teilweise als Bestandsdatensatz (so selbst für die dynamische IP-Adresse: § 100j Abs. 2 StPO) und teilweise als Verkehrsdatensatz eingeordnet; anders als §§ 100j StPO i.V.m. 95, 111 Abs. 1 TKG erfasst Art. 18 Abs. 3 b der Cybercrime-Konvention auch „Angaben über Rechnungsstellung und Zahlung“ als Bestandsdaten. Zugangssicherungscodes wie Gerätepasswörter, PIN (Persönliche Identifikationsnummer) und PUK (Personal Unblocking Key) werden zwar nicht im Katalog der §§ 95, 111 Abs. 1 TKG genannt, aber gemäß § 100j Abs. 1 S. 2 StPO den Bestandsdaten gleichgesetzt (Hauck, in: Löwe-Rosenberg, *StPO*, § 100j, Rn. 10 (zitiert nach juris)).

Dienstleister, die mittlerweile ebenfalls Kommunikationsdienstleistungen erbringen, oder heutige Abrechnungsmodelle sind sie nicht zugeschnitten. Auch wenn derzeit noch der Zugriff auf Telekommunikationsdaten für die Ermittlungen im Internet von zentraler Bedeutung ist,[344] so rücken elektronische Daten, die keine Kommunikationsdaten im engeren Sinne sind, zunehmend in der Blickpunkt der Strafverfolgungsbehörden.

Die etablierte gesetzliche Datenklassifizierung führt daher zu Regelungslücken und rechtlichen Unklarheiten hinsichtlich aller Nicht-Kommunikationsdaten, zu Ungleichbehandlungen hinsichtlich der auskunftsverpflichteten und nicht auskunftsverpflichteten Dienstleister und außerdem zu Hindernissen in der Strafverfolgung, da die Begriffe zwar international verwendet aber mit unterschiedlichen Bedeutungsinhalten verstanden werden.[345]

Während die rein praxisorientierte Kategorisierung zunächst noch mit der Grundrechtsrelevanz des Brief-, Post- und Fernmeldegeheimnisses in Einklang stand, die vom Regelfall der ortsgebundenen, individuellen Kommunikation zwischen zwei Personen unter Zuhilfenahme eines Informationsübermittlers und grundsätzlich geschütztem Kommunikationsinhalt ausgehen durfte, gelten diese Grundannahmen heute in vielen Fällen nicht mehr. Nachrichten werden zunehmend mithilfe mobiler Geräte, deren Funktionsumfang weit über die klassische Sprachtelefonie hinausgeht, an eine Mehrzahl von Empfängern gleichzeitig gerichtet, die Übermittlung erfolgt mehr und mehr unter Einbeziehung nicht nur eines, sondern mehrerer Dienstleister auf unterschiedlichen Ebenen[346] und gestattet ohne Anwendung einer Verschlüsselung grundsätzlich jedem Beteiligten eine uneingeschränkte Kenntnisnahme des Kommunikationsinhaltes.

---

344 Sieber, *Gutachten zum 69. DJT*, S. 116.

345 Svantesson, *Data categorisation and law enforcement access to cloud data*, spricht in diesem Zusammenhang von der Gefahr einer „überholten Konzeptualisierung“, aus der schlechte Rechtsstrukturen („poor legal frameworks“) resultierten.

346 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 23; Hiéramente / Fenina, Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?, StraFo 2015, 365 (S. 2, zitiert nach juris), m.w.N.

Damit verschiebt sich die Grundrechtsrelevanz entsprechender behördlicher Eingriffe. Neben dem in Art. 10 GG normierten Brief-, Post- und Fernmeldegeheimnis treten zunehmend das Recht auf informationelle Selbstbestimmung und insbesondere das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme in den Vordergrund, auf die die bisherige Einteilung nicht mehr ohne Weiteres übertragbar ist.[347] Es ist heute nicht mehr nachvollziehbar, warum massenhaft verbreitete, inhaltlich triviale Kommunikationsinhaltsdaten grundsätzlich einen höheren Schutz vor staatlicher Kenntnisnahme genießen sollten, als potentiell sensible Verkehrsdaten oder sonstige Datensätze, die nicht unmittelbar als Kommunikationsdaten subsumierbar sind.[348]

Mit der herkömmlichen Kategorisierung elektronischer Kommunikationsdaten werden vergleichbar sensible Daten als wesentlich Gleiches ungleich und unterschiedlich sensible Daten innerhalb einer Gruppe als wesentlich Ungleiches gleich behandelt. Die Feststellung typischer tatsächlicher Grundmerkmale einer Gruppe von Regelungsobjekten orientiert sich entgegen der modernen Gesetzgebungslehre nicht (mehr) an Kriterien, denen aus Erwägungen der Gerechtigkeit und Zweckmäßigkeit auch für das Recht unterschiedliche Bedeutung zukommt,[349] sondern folgt nur noch den veralteten praktischen Bedürfnissen der Telekommunikationsanbieter. Eine Neuklassifizierung elektronischer Beweismittel für strafprozessuale Zwecke ist daher sinnvoll.

---

347 Laut BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 198, schützt das Grundrecht auf informationelle Selbstbestimmung nicht nur „Informationen, die bereits ihrer Art nach sensibel sind“, sondern auch solche, „die für sich genommen nur geringen Informationsgehalt haben“.

348 Während der EuGH die grundrechtliche Bedeutung der Bestands- und Verkehrsdaten und ihre hohe Sensibilität im Einzelfall hervorhebt, ohne sie durch eine Bezugnahme auf Inhaltsdaten zu relativieren (vgl. nur EuGH, Urteil vom 08.04.2014 („Digital Rights Ireland“), C-293/12 und C-594/12, Rn. 26 f., und EuGH, Urteil vom 21.12.2016 („Tele2 / Watson“), C-203/15 und C-698/15, Rn. 98 ff.), betont das Bundesverfassungsgericht ohne nähere Begründung die erhöhte Schutzwürdigkeit von Kommunikationsinhaltsdaten im Vergleich zu sonstigen Kommunikationsdaten (vgl. BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 70).

349 Formulierung dieser Anforderung nach Schneider, *Gesetzgebung*, S. 26.

III. Vorüberlegungen zur Herleitung einer Neuklassifizierung elektronischer Beweismittel für strafprozessuale Zwecke

1. Erforderlichkeit einer Neuklassifizierung

Die Feststellung, dass eine Neuklassifizierung sinnvoll ist, führt zur Frage, ob sie aus verfassungsrechtlichen Gründen nicht sogar erforderlich, also zwingend geboten ist (dazu unter a)). Unabhängig vom Ergebnis kommen als theoretische Handlungsalternativen zu einer umfassenden Neuordnung die einheitliche Regelung sämtlicher elektronischer Daten auf höchstem Abstraktionsniveau (b)) und die Ausweitung der derzeitigen Kategorisierungsmaßstäbe für Kommunikationsdaten auf sämtliche Nicht-Kommunikationsdaten (c)) in Betracht.

a) Verfassungsrechtliche Vorgaben

Gemäß Art. 19 Abs. 1 GG obliegt es dem Gesetzgeber, förmliche Gesetze zu erlassen, die einen Eingriff in die Grundrechte des Einzelnen erlauben; ohne eine solche Rechtsgrundlage ist ein Eingriff rechtswidrig.[350] Da jede strafrechtliche Ermittlungshandlung jedenfalls die in Art. 2 Abs. 1 GG garantierte allgemeine Handlungsfreiheit des Einzelnen berührt, bedarf es mithin in diesem Bereich entsprechender förmlicher Gesetzgebung.

Es wurde bereits beschrieben, dass im Sinne der modernen Gesetzgebungslehre ein förmliches Gesetz aus verfassungsrechtlichen Gründen prinzipiell einen generellen, allgemeinen Charakter aufweisen muss,[351] der es vom grundsätzlich unzulässigen Einzelfallgesetz ebenso unterscheidet wie von Gerichtsentscheidungen und Verwaltungsakten.[352] Die Allgemeinheit des Regelungsinhaltes kommt darin zum

350 Hesselberger, in: Leibholz / Rinck, Art. 19, Rn. 2 (zitiert nach juris); Schneider, Gesetzgebung, S. 16.

351 Das Erfordernis des allgemeinen Charakters wird unmittelbar aus Art. 19 Abs. 1 GG abgeleitet, der nach herrschender Meinung eine Konkretisierung des allgemeinen Gleichheitssatzes enthält (Hesselberger, in: Leibholz / Rinck, *GG*, Art. 19, Rn. 11 (zitiert nach juris)).

352 Vgl. Hesselberger, in: Leibholz / Rinck, *GG*, Art. 19, Rn. 12, 31 (zitiert nach juris); Schneider, Gesetzgebung, S. 20 f.

Ausdruck, dass Rechtsfolgen für eine unbestimmte Vielzahl an Fällen vorgegeben werden und diese Fälle sich nach abstrakten, typischen Grundmerkmalen tatsächlicher Gegebenheiten richten.[353] Die Bildung von Fallgruppen anhand typischer, regelungsrelevanter Kennzeichen ist daher notwendige Voraussetzung eines förmlichen Gesetzes.

Damit stellt sich die Frage, auf welchem Abstraktionsgrad und nach welchen Kriterien die fallgruppenspezifischen Merkmale zu bestimmen sind. Eine konkrete Regelung dazu gibt es nicht.[354] Der Gesetzgeber hat vielmehr eine Gestaltungsfreiheit im Hinblick auf die Bestimmung der Unterscheidungsmerkmale.[355]
Die Bestimmung muss jedoch sachgerecht getroffen werden und hat in dem Rahmen zu erfolgen, den die Grundrechte und die Grundprinzipien der verfassungsmäßigen Ordnung beschreiben,[356] oder, mit den Worten des Bundesverfassungsgerichts, anhand solcher Kriterien, denen „aus Erwägungen der Gerechtigkeit und Zweckmäßigkeit auch für das Recht unterschiedliche Bedeutung zukommt“.[357] Aus beiden Formulierungen ergibt sich, dass die Klassifizierung der Regelungsobjekte jedenfalls nach rechtlich relevanten Kriterien erfolgen muss. Soweit damit die Grundrechte betroffen sind, genügt es nicht, auf einheitliche Grundsätze zurückzugreifen, vielmehr bedarf es der Herausarbeitung der spezifischen Grundrechtsschutzbereiche, die im konkreten Regelungsfall betroffen sind.[358]

Bezogen auf elektronische Daten wurde dargelegt, dass die Gleichbehandlung aller Nicht-Kommunikationsdaten ihrer rechtlich relevanten unterschiedlichen Sensibilität in keiner Weise Rechnung trägt und die Typisierung der Kommunikationsdaten aufgrund der

353 Schneider, Gesetzgebung, S. 22; Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 13.
354 Burghart, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 27 (zitiert nach juris), m.w.N.; Schneider, Gesetzgebung, S. 38.
355 Schneider, Gesetzgebung, S. 39; Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 41.
356 Hesselberger, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 34 (zitiert nach juris), m.w.N.; Schneider, Gesetzgebung, S. 38 f.
357 BVerfG, Urteil vom 18.12.1953, 1 BvL 106/53, zugleich BVerfGE 3, 225, Rn. 37 (zitiert nach juris); vgl. auch Burghart, in: Leibholz / Rinck, *GG*, Art. 3, Rn. 26 (zitiert nach juris), m.w.N.
358 Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (54).

technischen und gesellschaftlichen Entwicklung im Kommunikationsbereich nicht mehr mit den verfassungsrechtlichen Wertevorgaben in Einklang zu bringen ist.

Es kann dahinstehen, ob diese Entwicklung bei Erlass der einschlägigen Normen bereits stattfand oder absehbar war, weil die derzeitige Typisierung jedenfalls heute aus tatsächlichen Gründen überholt ist. Allein dieser Umstand begründet eine Handlungspflicht des Gesetzgebers,[359] sodass eine Neuklassifikation elektronischer Daten nicht nur sinnvoll, sondern aus verfassungsrechtlichen Gründen erforderlich ist, um die Erhebung und Verwertung elektronischer Daten im Strafprozess einerseits aus Sicht des Datenberechtigten grundrechtskonform und andererseits aus Sicht der Strafverfolgungsbehörden praktikabel auszugestalten.

b) 1. Alternative: Einheitliche Regelung für sämtliche elektronische Daten

Eine unterschiedslose rechtliche Gleichsetzung aller elektronischen Daten ohne weitere Differenzierung wäre – vergleichbar mit der grundsätzlich unterschiedslosen Zugänglichkeit zu allen Informationen, die zum Beispiel über die herkömmlichen Beweismittel erlangt werden können - als alternative Ausgestaltung einer Neuklassifizierung denkbar.[360] Eine solche Typisierung auf höchstem Abstraktionsniveau

359 Vgl. Schneider, Gesetzgebung, S. 40, 56, m.w.N.; Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (22); zur Diskussion um die vom BVerfG postulierte Nachbesserungspflicht des Gesetzgebers: Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 20, m.w.N.

360 Die in § 244 Abs. 2 StPO normierte gerichtliche Pflicht zur Wahrheitserforschung, die sich „auf alle Tatsachen und Beweismittel“ erstreckt, „die für die Entscheidung von Bedeutung sind“, impliziert, dass jedes zur Verfügung stehende Beweismittel grundsätzlich voll auszuschöpfen ist und die von ihm erhältlichen entscheidungsrelevanten Informationen umfänglich in Erfahrung zu bringen sind. Von diesen Grundsätzen gibt es einige wenige Ausnahmen für die Frage, ob ein tatsächlich vorhandenes Beweismittel überhaupt zur Anwendung kommt (vgl. beispielsweise § 245 Abs. 1 S. 2 StPO für das Absehen einer einzelnen Beweiserhebung bei Einverständnis aller Prozessbeteiligten oder die diversen Regelungen zum Zeugnisverweigerungsrecht einzelner Personen). Ist die Beweiserhebung hingegen mithilfe eines bestimmten Beweismittels durchzuführen, sieht das Strafprozessrecht lediglich in § 55 StPO, der zum Schutz vor eigener Strafverfolgung oder einer Verfolgung naher Angehöriger ein Auskunftsverweigerungsrecht des Zeugen

hätte zur Konsequenz, dass der Zugang zu und die Verwertung aller elektronischen Beweismittel einheitlich geregelt werden könnten. Der Maßstab für sämtliche Ermittlungsbefugnisse entspräche dem, der auf den sensibelsten Datensatz anzuwenden ist.

Ausgehend vom derzeitigen gesetzlichen Wertungsschema wäre konsequenterweise umfassend das Niveau für Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, anzuwenden, was wegen des diesbezüglich bestehenden absoluten Beweiserhebungs- und -verwertungsverbotes de facto zu einer Unzugänglichkeit sämtlicher personenbezogener elektronischer Daten im Strafermittlungsverfahren führen würde.

Es ist offensichtlich, dass diese Handhabung aufgrund der enormen strafprozessualen Bedeutung solcher Daten für die Wahrheitsfindung nicht umsetzbar wäre.

Dies gilt entsprechend, wenn Kernbereichsdaten außer Betracht blieben – auch wenn dadurch gerade durch einen Bruch des strukturellen Ansatzes eine Datenklassifizierung vorgenommen würde – und diejenigen strengen Maßstäbe angelegt würden, die auf gerade noch verwertbare sensibelste Daten zutreffen.

Die praktische Umsetzbarkeit einer entsprechenden Regelung würde bereits personell daran scheitern, dass sämtliche datenbezogenen Ermittlungsmaßnahmen nur auf Antrag der Staatsanwaltschaft und mit richterlicher Bestätigung durchgeführt werden dürften. Zudem würden elektronische Beweismittel nur noch bei schwersten Straftaten verwertbar sein, was ihrer praktischen Relevanz für sämtliche Straftaten nicht gerecht würde. Schließlich wäre aufgrund der Bandbreite der unterschiedlichen, rechtlich begründeten Sensibilität elektronischer Daten ihre einheitliche gesetzliche Behandlung

---

begründet, eine potentielle, punktuelle inhaltliche Beschränkung des gerichtlichen Informationsgewinnes vor. Im Übrigen gilt, dass alle entscheidungsrelevanten Informationen, die das Beweismittel innehat, unabhängig von ihrem Inhalt grundsätzlich zugänglich und verwertbar sind, solange sie sich nicht auf den Kernbereich der privaten Lebensgestaltung beziehen.

ungeachtet der praktischen Unbrauchbarkeit als gleiche Behandlung wesentlich ungleicher Sachverhalte ohne sachlichen Grund und damit als verfassungswidrig zu qualifizieren, sodass auch rechtsdogmatische Gründe gegen den genannten Ansatz sprechen.

Es bedarf daher einer differenzierten Regelung; die einheitliche Behandlung sämtlicher elektronischer Daten im Strafermittlungsverfahren wäre weder praktikabel noch verfassungsgemäß.

c) 2. Alternative: Ausweitung der derzeitigen Kategorisierungsmaßstäbe für Kommunikationsdaten auf sämtliche elektronische Daten

Es wäre denkbar, jedenfalls die Kategorien Verkehrs- und Inhaltsdaten auf sämtliche Datensätze, namentlich auf die Nicht-Kommunikationsdaten auszuweiten. Auch sie weisen einen eigentlichen Informationsinhalt auf und sind, wenn sie übermittelt oder lokal verarbeitet werden, bestimmten Verkehrs- oder Metadaten zuzuordnen.

Eine solche Ausweitung würde zwar eine Regelungslücke schließen, wäre aber wegen der dargelegten Problematiken, die insbesondere die Abhängigkeit der Typisierung vom verwendeten Beweismittel und die Zweifel an der Verfassungsmäßigkeit insbesondere hinsichtlich der Sensibilitätsbestimmung betreffen, nicht weiter zielführend. Der Großteil der aktuellen Unzulänglichkeit bliebe bestehen. Zudem wäre eine völlige Neukonzeption erforderlich, um die Auskunftsverpflichteten zu bestimmen, die, soweit es Nicht-Kommunikationsdaten beträfe, keinesfalls als Telekommunikationsdienstleister subsumiert werden könnten.

Auf der herkömmlichen Unterscheidung sollte daher nicht aufgebaut werden, zumal ihre Kriterien für die Gruppenzuordnung nicht mit Blick auf rechtliche Anforderungen entwickelt wurden, sondern den praktischen Bedürfnissen der Telekommunikationsdienstleister entsprachen.

d) Zwischenergebnis

Zusammenfassend lässt sich festhalten, dass eine Neuklassifikation elektronischer Beweismittel für strafprozessuale Zwecke nicht nur sinnvoll, sondern aus verfassungsrechtlichen Gründen erforderlich ist. Aufgrund der Vielfältigkeit und Komplexität elektronischer Daten genügt die derzeitige Klassifikation den rechtlichen Anforderungen nicht, weil sie im Hinblick auf Nicht-Kommunikationsdaten wesentlich Ungleiches ohne erkennbaren sachlichen Grund gleich und im Hinblick auf Kommunikationsdaten wesentlich Gleiches ohne erkennbaren sachlichen Grund ungleich behandelt.

Eine vollkommen einheitliche Behandlung sämtlicher personenbezogener elektronischer Daten würde weder ihrer unterschiedlichen, rechtlich begründeten Sensibilität noch der praktischen Bedeutung dieses Beweismittels gerecht.
Sie ist daher ebenso abzulehnen wie die Übertragung der für Kommunikationsdaten entwickelten Typisierung auf sämtliche Daten, die den verfassungsrechtlichen Anforderungen an eine sachgerechte, rechtlich nachvollziehbare Differenzierung nicht (mehr) genügt.

Vielmehr bedarf es eines gänzlich neuen Ansatzes, bei dem die Typisierung allein den verfassungsrechtlichen Vorgaben folgt.

2. Prämissen einer konzeptionellen Neuklassifizierung

Aus der Erörterung der herkömmlichen Datenklassifizierung wurden Schwachstellen ersichtlich, die es bei der Neuklassifikation zu vermeiden gilt. Insbesondere ist darauf zu achten, dass sie sämtliche elektronische Daten erfasst (dazu unter a)), technikneutral ausgestaltet ist (b)) und zudem allgemeine Begriffe statt einzelner Katalogauflistungen verwendet (c)).

a) Erfassung sämtlicher elektronischer Daten

Es wurde bereits ausführlich dargelegt, dass ein wesentliches Manko

der derzeitigen Dateneinteilungen darin liegt, dass sie entweder zu allgemein gehalten sind oder sich ausschließlich auf Kommunikationsdaten beziehen. Letzteres führt neben der Schwierigkeit, beim heutigen Stand der Technik den Kommunikationsbegriff sinnvoll eindeutig zu definieren, zu erheblichen und zunehmenden Lücken in Bezug auf alle Nicht-Kommunikationsdaten, die gleichfalls von großer Bedeutung für die Strafverfolgungsbehörden sind. Diesen Bedenken soll die Neuklassifizierung dadurch Rechnung tragen, dass sie sämtliche elektronische Daten erfasst.[361]

b) Technikneutrale Ausgestaltung

Aufgrund des technischen Fortschrittes, der sich insbesondere im IT-Bereich mit einer enormen Geschwindigkeit vollzieht, muss jegliche Datenklassifikation, wenn sie verlässlich und stabil sein soll, technikneutral sein.[362] Sie darf also nicht von technischen Kriterien abhängen, weil sie ansonsten mit jeder technischen Neuerung veraltet und damit nicht mehr umfassend anwendbar ist. Das Problem zeigt sich bereits heute beispielsweise für Daten aus dem Bereich der Telefonie, wo der strafprozessual detailliert geregelte Bereich der klassischen Festnetztelefonie zunehmend durch den bislang nur rudimentär geregelten Bereich der Internettelefonie verdrängt wird. Daneben ist es, um ein weiteres Beispiel zu nennen, durchaus denkbar, dass mithilfe Künstlicher Intelligenz eine Datenübermittlung künftig ohne zentrale Server und damit ohne entsprechende Dienstleister auskommen wird, was keinen Einfluss auf den Grundrechtsschutz des Nutzers haben sollte.

361 Zur Notwendigkeit einer ganzheitlichen Datenerfassung im Rahmen einer Datenklassifizierung vgl. auch Europäische Kommission Services, *Technical Document*, S. 18 f., 31.

362 In diesem Sinne auch: Europäische Kommission, *Report on the 17 / 18 January 2017 expert meeting*, S. 1; zur empfohlenen Technikneutralität speziell für den Bereich der Bestimmung des Schutzbereiches des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme: Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (302); Europäische Kommission Services, *Technical Document*, S. 19, schlagen vermittelnd die Ergänzung allgemeingültiger Definitionen durch ein „Wörterbuch“ („library“) auf technischer Ebene vor. Allgemein zum Erfordernis der Stabilität eines Gesetzes: Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 201.

Das Risiko der Veralterung besteht selbst dann, wenn keine technische Neuerung zur Anwendung kommt, sondern, was grundsätzlich jederzeit möglich ist, ein technischer Standard durch einen anderen, nicht unbedingt neu entwickelten, ersetzt wird. So existieren beispielsweise neben dem weitverbreiteten Internet-Protokoll (IP) bereits heute mehrere andere Netzwerkprotokolle, die sich nur nicht als Standard durchgesetzt haben. Dabei ist es nicht ausgeschlossen, dass das Internet-Protokoll irgendwann durch ein anderes Netzwerkprotokoll ersetzt wird.

Beide denkbaren Entwicklungen – technische Neuerungen und Standardänderungen - würden bei technikabhängiger Daten-qualifizierung mittelbar den Grundrechtsschutz des Nutzers beeinträchtigen, weil spezifische, noch nicht oder nicht mehr erfasste Datensätze strafprozessrechtlich gleichsam „in der Luft“ hingen.[363] Ein besonders deutliches Beispiel ist in diesem Zusammenhang die erst Mitte 2013 eingeführte Regelung des § 100j Abs. 2 StPO,[364] die eine Bestandsdatenauskunft explizit und sehr technikspezifisch „anhand einer […] Internetprotokoll-Adresse“ gestattet. Mit der seitdem stattfindenden Verbreitung der CGN-Technik, bei der identische dynamische IP-Adressen zeitgleich bis zu mehreren Tausend Nutzern zugeordnet werden, hat alleine die technische Entwicklung dazu geführt, dass heute im Vergleich zu 2013 eine deutlich größere Anzahl von unbeteiligten Dritten von einer Ermittlungsmaßnahme gemäß § 100j Abs. 2 StPO betroffen ist. Dies wiederum weckt im Rahmen der Verhältnismäßigkeitsprüfung erhebliche Zweifel an der derzeitigen Verfassungsmäßigkeit der Norm – allein aufgrund der zwischen-zeitlichen technischen Entwicklung.

Zudem bestehen dogmatische Bedenken gegen eine Anwendung technischer Kriterien zur Bestimmung der rechtlichen Schutzwürdigkeit elektronischer Datensätze.
Diese existieren zwar faktisch nur in einem technischen Umfeld,

363 Vgl. für den technologieneutralen Schutz der Rechte natürlicher Personen im Bereich des Datenschutzes: DS-Richtlinie Strafjustiz, Begründung Ziff. 18.
364 Eingeführt durch das Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20.06.2013, BGBl. I S. 1602.

namentlich in einem informationstechnischen System. Aus den technischen Gegebenheiten lassen sich aber originär keine Rechtsfolgen und damit keine rechtliche Schutzwürdigkeit der einzelnen Datensätze ableiten; sie haben als solche keinen Einfluss auf den gesetzgeberischen Handlungsrahmen, den alleine die Grundrechte und die Grundprinzipien der verfassungsmäßigen Ordnung beschreiben.

c) Keine Katalogauflistung einzelner Datensätze

Im Zusammenhang mit der zu vermeidenden Technikabhängigkeit der Kategorisierung steht die Auflistung von Katalogdaten, wie sie etwa für Verkehrsdaten in § 96 Abs. 1 TKG oder für Bestandsdaten in § 111 Abs. 1 TKG vorgenommen wird. Eine solche Liste ist auf den ersten Blick nützlich, weil relativ einfach festgestellt werden kann, ob ein bestimmter Datensatz der jeweiligen Kategorie zuzuordnen ist oder nicht. Dadurch werden Unklarheiten und Auslegungsprobleme vermieden.

Umgekehrt führt eine umfassende Auflistung von Einzelobjekten häufig zur Unübersichtlichkeit einer Norm. Gegen die Katalogauflistung spricht außerdem, dass sie selbst bei sorgfältigster Erstellung aufgrund technischer, rechtlicher und / oder gesellschaftlicher Fortentwicklung relativ schnell unvollständig oder unzutreffend werden kann und dann insbesondere unter Berücksichtigung der Geschwindigkeit des technischen Fortschritts einerseits und der Dauer eines Gesetzgebungsverfahrens andererseits grundsätzlich den tatsächlichen Gegebenheiten hinterherhinkt.

Schließlich begegnen Katalogauflistungen grundsätzlichen Bedenken, weil sie durch die konkrete Darstellung eine im Sinne der modernen Gesetzgebungslehre erwünschte Abstraktion vermeiden. Das ist insbesondere im strafprozessualen Bereich bedenklich, wo die Einteilung zur Vermeidung unzulässiger Einzelfallgesetze nach abstrakten Rechtsgrundsätzen und -prinzipien zu erfolgen hat. Folgt die Einteilung diesen Rechtsgrundsätzen (die gegebenenfalls gegen-

einander abzuwägen sind), so ist eine abstrakte Klassifizierung grundsätzlich möglich und sollte sich dann auch in der Regelung niederschlagen; folgt die Einteilung den Rechtsgrundsätzen nicht oder nicht durchgängig, so läuft sie Gefahr, verfassungswidrig zu sein.

3. Mögliche Kriterien zur Unterscheidung elektronischer Daten

Im Folgenden wird untersucht, welche konkreten Unterscheidungsmerkmale unter Berücksichtigung der abstrakten Vorgaben einer Neuklassifikation zugrundegelegt werden können. Es wurde bereits herausgestellt, dass eine Unterscheidung unter Berücksichtigung der „abstrakten, typischen Grundmerkmale tatsächlicher Gegebenheiten“ beziehungsweise „anhand solcher Kriterien, denen aus Erwägungen der Gerechtigkeit und Zweckmäßigkeit auch für das Recht unterschiedliche Bedeutung zukommt“ zu erfolgen hat.

Soweit ersichtlich, gibt es bislang keine höchstrichterliche oder vertiefte, umfassende wissenschaftliche Auseinandersetzung zu konkreten Unterscheidungskriterien für elektronische Daten. Im Einzelnen werden folgende Kriterien, die in der Literatur in unterschiedlichem Umfang angesprochen werden, auf ihre Geeignetheit als Unterscheidungsmerkmal untersucht: die Intensität der Grundrechtsschutzbetroffenheit (dazu unter a)), der abstrakte Inhalt eines Datensatzes (b)), sein Volumen (c)), sein Entstehungsumfeld in technischer Sicht (d)), sein aktueller Verarbeitungszustand (e)), die Unterscheidungskriterien des Datenschutzrechts (f)), die Relevanz eines Datensatzes für das Strafverfahren und die Schwere des zugrundeliegenden Deliktes (g)) sowie die anwendbaren Ermittlungsmaßnahmen (h)).

a) Intensität der Grundrechtsschutzbetroffenheit

Vom Sinn und Zweck der vorzunehmenden Datenkategorisierung, also der Ausgestaltung der widerstreitenden Positionen Grundrechtsschutz des Betroffenen, des Opfers und öffentliches Strafverfolgungsinteresse,

ergibt sich als erstes, naheliegendes Kriterium die Intensität der Grundrechtsbetroffenheit, die dem jeweiligen Datensatz immanent ist.[365] Damit werden in erster Linie die datenspezifischen Grundrechte angesprochen, namentlich das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG, das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung und das ebenfalls auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG fußende Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[366]

Daneben kann die Erhebung elektronischer Daten beim Betroffenen je nach Umständen des Einzelfalles die Grundrechte aus Art. 12 GG (Berufsausübungsfreiheit etwa des herausgabeverpflichteten Providers), Art. 13 GG (Unverletzlichkeit der Wohnung, beispielsweise bei dortiger Datenerlangung) und Art. 14 GG (Recht auf Eigentum, etwa bei Beschlagnahme eines Datenträgers) tangieren.

Zwar kann auf dieser Abstraktionsebene festgestellt werden, dass elektronische Datensätze als umso schutzwürdiger einzuordnen sind, je größer die Eingriffsintensität einer bestimmten Maßnahme in die datenspezifischen Grundrechte ist, sodass im Hinblick auf die Daten durchaus unterschiedliche Fallgruppen gebildet werden können. Diese Feststellung spiegelt auch die in mehreren Entscheidungen geäußerte Auffassung des Bundesverfassungsgerichts wider, wonach die Schutzwürdigkeit eines Datensatzes entfällt, wenn – wie bei öffentlich zugänglichen Daten - keine Grundrechtsrelevanz vorliegt,[367] während eine Grundrechtsbeeinträchtigung im Kernbereich privater Lebensgestaltung aufgrund höchster Schutzwürdigkeit zu einem absoluten

365 Vgl. auch Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (54), der wie folgt formuliert: „Die differenzierte Grundrechtssystematik fordert eine entsprechend differenzierte Grundrechtsdogmatik, die die jeweiligen grundrechtlichen Gewährleistungsgehalte herausarbeitet und die Einwirkungsmöglichkeiten in materieller und formaler Hinsicht […] grundrechtsspezifisch bestimmt."

366 Vgl. Europäische Kommission Services, *Technical Document*, S. 31 („the intensity of the interference" mit den datenspezifischen Grundrechten), und Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679), die von „privacy implications of the data" sprechen.

367 Vgl. nur BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 308.

Beweiserhebungs- und -verwertungsverbot führt.[368]

Diese Feststellung sagt jedoch nichts darüber aus, nach welchen konkreten Kriterien die Grundrechtsschutzbetroffenheit oder die Eingriffsintensität gerade im Zusammenhang mit elektronischen Daten zu bestimmen sind. Es leuchtet ein, dass eine gesetzliche Unterscheidung von beispielsweise „besonders schutzwürdigen Daten“, „durchschnittlich schutzwürdigen Daten“ und „weniger schutzwürdigen Daten“ nicht zielführend, weil unpraktikabel wäre. Insbesondere unter den Aspekten der Normenklarheit und der Normenbestimmtheit genügt der Verweis auf die Grundrechtsschutzbetroffenheit und die Eingriffsintensität nicht zur sachgerechten Differenzierung. Sie muss vielmehr auf einem konkreteren Niveau stattfinden, um für die Gesetzgebung hilfreich zu sein.

In der Fachliteratur werden die folgenden Aspekte zur näheren Konkretisierung diskutiert:

b) Abstrakter Dateninhalt

Es erscheint naheliegend, den abstrakten Inhalt eines Datensatzes als konkretes Unterscheidungskriterium für die Datenklassifizierung anzuwenden und beispielsweise in Anlehnung an den aktuellen Vorschlag der Europäischen Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation zwischen elektronischen Inhaltsdaten und elektronischen Metadaten zu unterscheiden.[369]
Die Kategorie der Inhaltsdaten bezöge sich dabei auf den eigentlichen Kern des Datensatzes, auf seine Primärauskunft, die bei Kommunikationsdaten dem Kommunikationsinhalt und bei Maschine-zu-Maschine Kommunikation dem eigentlichen Nachrichtenwert

368 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 277, m.w.N.

369 Der Vorschlag unterscheidet, ausgehend von einem weitestmöglichen Kommunikationsbegriff in Art. 4 Nr. 3 a) des Entwurfes, zwischen elektronischen Kommunikationsinhalten und elektronischen Kommunikationsmetadaten (Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation*, 10.01.2017).

entspricht, während die Metadaten die verbleibenden Sekundärinformationen beinhalten würde, die das informationstechnische System entweder wie beim Zeitstempel automatisch anlegt oder deren Angabe wie bei der IP-Adresse eines Nachrichtenempfängers zur Datenverarbeitung unerlässlich ist.

Was im Datenschutzrecht durchaus sinnvoll erscheint,[370] erfüllt jedoch nicht die Zwecke des Strafverfahrensrechts: Hier hat sich die herkömmliche Gesetzgebung mit der dateninhaltsbezogenen Herangehensweise bereits als unzulänglich erwiesen – der eingeschränkte strafprozessuale Nutzen der Unterscheidung von Bestands-, Verkehrs- und Inhaltsdaten, die alleine auf den abstrakten Inhalt des jeweiligen Datensatzes abstellt, wurde ausführlich dargelegt.

Der Hauptkritikpunkt an einer inhaltsbezogenen Unterscheidung elektronischer Daten ist das Außerachtlassen der Tatsache, dass die Sensibilität, also die rechtliche Schutzwürdigkeit eines Dateninhaltes kein abstraktes, typisches Grundmerkmal eines Datensatzes darstellt. Sie kann je nach konkreter Fallkonstellation deutlich variieren. So können beispielsweise bestimmte Metadaten, aus denen sich der brisante Aufenthaltsort eines Nutzers zu einem bestimmten Zeitpunkt ergibt, durchaus grundrechtssensibler sein als triviale Inhalte einer Massenkommunikation.[371]

Das gilt für alle Datensätze gleichermaßen, egal, ob es sich um Kommunikations- oder Nicht-Kommunikationsdaten handelt. Aus diesem Grund ist, wie dargelegt, auch die Ausweitung der herkömmlichen Unterscheidung von Kommunikationsdaten auf Nicht-Kommunikationsdaten abzulehnen.

Eine Kategorisierung, die dem abstrakten Dateninhalt folgt, unterliegt

370 Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation*, 10.01.2017, S. 2, erläutert ausführlich den datenschutzrechtlichen Bezug des Vorschlags.

371 Zur potentiell hohen Sensibilität von Kommunikationsmetadaten, die nicht den Kommunikationsinhalt selbst betreffen, vgl. Europäische Kommission, *Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation* vom 10.01.2017, S. 5 und 13, mit Hinweis auf die korrespondierende Rechtsprechung des EuGH.

außerdem dem Dilemma, das sich daraus ergibt, dass Daten, die den höchsten Schutz genießen, nicht erhoben werden dürfen, die Feststellung der besonderen Schutzwürdigkeit aber häufig nicht nur ihre Erhebung, sondern zudem ihre Durchsicht erfordert.[372] Mit anderen Worten ist paradoxerweise grundsätzlich eine Erhebung und inhaltliche Kenntnisnahme eines Datensatzes durchzuführen, um verlässlich feststellen zu können, dass ein konkreter Inhalt absolut vor der behördlichen Kenntnisnahme geschützt ist. Der Hinweis, dass in solchen Fällen quasi auf zweiter Stufe immer noch ein Beweisverwertungsverbot greife, trifft zu; er ändert aber nichts daran, dass das ursprünglich bestehende Beweiserhebungsverbot regelmäßig ins Leere läuft.

Der abstrakte Dateninhalt kann daher kein primäres Unterscheidungskriterium für die Datenklassifizierung sein.

c) Datenvolumen

Ein interessanter Ansatz liegt im Verweis auf das in Frage stehende Datenvolumen, das zum einen als solches und zum anderen im Hinblick auf die Möglichkeit der Persönlichkeitsprofilbildung als Unterscheidungsmerkmal diskutiert wird.[373]

Beim Datenvolumen als solches handelt es sich zunächst nur um eine

372 Zu dieser Problematik vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 277 ff., mit der Forderung, einen zweistufigen Kernbereichsschutz dergestalt anzuwenden, dass die Erhebung kernbereichsrelevanter Daten soweit wie möglich unterbleibt und, falls solche Daten erhoben wurden, sie unverzüglich und ausnahmslos gelöscht werden; zur näheren Darstellung vgl. Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (304).

373 Zur Relevanz des betroffenen Datenvolumens: Gesetzesbegründung zur Neufassung der §§ 100a ff. StPO, BT-Ausschussdrucks. 18(6)334, S. 6; für das Datenvolumen als ein mögliches Abgrenzungskriterium von mehreren: Europäische Kommission Services, *Technical Document*, S. 31; unter Hinweis auf die Möglichkeit der Profilbildung und mit der Einschränkung, dass das Datenvolumen jedenfalls eines von mehreren zu berücksichtigenden Kriterien sein könne: Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679).

technische Größe, sodass seine Anwendung mit eindeutigen Mengenvorgaben klar und bestimmt geregelt werden könnte.

Allerdings stünde diesem Vorgehen die Prämisse der Technikneutralität entgegen.
Zudem ist nicht nachvollziehbar, weshalb ein großes Datenvolumen per se rechtlich schutzwürdiger sein sollte als ein kleineres – das Datenvolumen ist kein rechtlich relevantes „abstraktes, typisches Grundmerkmal“ bestimmter Datengruppen.
Nur im konkreten Einzelfall lässt sich feststellen, welche Datenmengen zur Informationserlangung erhoben werden müssen und welches Maß an Datenerhebung mithin erforderlich ist. Diese Frage stellt sich vergleichbar etwa mit der Blutprobenentnahme oder der Beschlagnahme von Schriftstücken allerdings erst im Rahmen der Verhältnismäßigkeitsprüfung und nicht bei der Grundsatzfrage, wie schutzwürdig bestimmte elektronische Daten im Verhältnis zu anderen sind.[374] Hochsensible Einzeldaten sind ebenso denkbar wie triviale Massendaten – und umgekehrt. Gerade unter Berücksichtigung der bereits angesprochenen zunehmenden Trivialisierung der Kommunikation über das Internet gibt es keinen Anhaltspunkt dafür, dass – ungeachtet der möglichen Profilbildung – ein kleiner Datensatz weniger schutzwürdig wäre als ein großer.

Desweiteren ergäben sich bei der Anwendung dieses Kriteriums als Unterscheidungsmerkmal praktische Schwierigkeiten in Bezug auf die Größenfestlegung – welche Datenmenge gälte als klein, welche als groß? Und wie wäre die exponentiell anwachsende absolut verfügbare Datenmenge zu berücksichtigen?

Schließlich bestünde ein Durchsetzungsrisiko bei Auskunftsanfragen an Kommunikationsdienstleister, bei denen im Voraus das erhältliche

374 Es käme daher niemand auf die Idee, unterschiedliche gesetzliche Bedingungen an die Entnahme unterschiedlicher Blutprobenmengen oder an den Umfang eines zu beschlagnahmenden Schriftstückes zu knüpfen. Wenn die rechtlichen Voraussetzungen für eine Entnahme beziehungsweise Beschlagnahme vorliegen, darf soviel Körperflüssigkeit entnommen werden, wie es im konkreten Fall für die Untersuchung notwendig und angemessen ist, und darf das Schriftstück ungeachtet seiner Seitenanzahl beschlagnahmt werden, sofern dies im Einklang mit den Grundsätzen der Verhältnismäßigkeit geschieht.

Datenvolumen nicht abzuschätzen ist. Nach welchen Kriterien und durch wen würde die Datensatzauswahl erfolgen, wenn das grundsätzlich verfügbare Datenvolumen die gesetzliche Obergrenze überschritte?

Das Datenvolumen selbst ist daher aus rechtlichen wie tatsächlichen Gründen kein geeignetes Unterscheidungskriterium.

Hinter dem zweitgenannten Ansatz im Zusammenhang mit dem Datenvolumen steht die Idee, dass die Schutzwürdigkeit einer Gesamtheit von Datensätzen, aus denen darüberhinausgehende Informationen wie beispielsweise Persönlichkeitsprofile erlangt werden können, höher ist, als die Schutzwürdigkeit der jeweiligen Einzeldaten.[375]

Hinsichtlich der Möglichkeit der Profilbildung ist dem Bundesverfassungsgericht darin zuzustimmen, dass sie ein zusätzliches Risiko für einen Eingriff in die Persönlichkeitsrechte des Einzelnen darstellt, das über das des einzelnen Datensatzes hinausgeht.[376] Dieses Risiko ist aber jedem Datensatz immanent und betrifft alle Datensätze gleichermaßen, egal ob groß oder klein. Die Sensibilität der Profilaussage hängt zudem nicht zwingend von der Sensibilität der zugrundeliegenden Einzelinformationen ab, weil sensible Profilaussagen auch aus an sich wenig sensiblen Einzeldaten gewonnen werden können.

Daraus lässt sich Zweierlei schlussfolgern:

Zum einen ist das Risiko einer Profilerstellung selbst kein geeignetes Kriterium, um die jeweilige Sensibilität unterschiedlicher Datensätze zu

375 Vgl. BVerfG, Urteil vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212), m.w.N.; BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 232, 309, mit dem Hinweis, dass in solchen Fällen das Recht auf informationelle Selbstbestimmung betroffen sei; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679).

376 Vgl. nur BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 198 f., m.w.N.

bestimmen, weil grundsätzlich alle Datensätze diesem Risiko unterliegen; vom Risiko der Profilbildung kann nicht auf die Sensibilität eines einzelnen Datensatzes geschlossen werden.

Zum anderen ist das Risiko der Profilbildung und der damit verbundenen weiteren Beeinträchtigung der Persönlichkeitsrechte des Nutzers so realistisch und gravierend, dass es grundsätzlich bei jeder Datenerhebung zu beachten ist. Da es keinen verbindlichen Wert dafür gibt, ab welcher Datenmenge das Risiko überhaupt oder in besonderem Maße besteht, ist es am sinnvollsten im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen, die jeder Ermittlungsmaßnahme voranzugehen hat und durch die erreicht werden soll, dass das zu erlangende Datenvolumen und somit das Risiko der Profilbildung und der damit verbundenen Persönlichkeitsrechtsbeeinträchtigung auf das erforderliche, dem Einzelfall angemessene Minimum reduziert wird.[377]

d) Datenherkunft aus technischer Sicht

Es wäre denkbar, elektronische Beweismittel danach zu unterscheiden, wie sie technisch gesehen entstanden sind, also durch welche elektronische Funktion sie kreiert wurden[378] oder welcher Dienstleistungsart sie zuzuordnen sind[379].[380]

377 Zur Relevanz des Datenvolumens (erst) auf der Ebene der Verhältnismäßigkeitsprüfung und der fehlenden Erforderlichkeit, Daten zu erheben, die für das Verfahren bedeutungslos sind, vgl. BVerfG, Beschluss vom 12.04.2005, 2 BvR 1027/02, zugleich BVerfGE 113, 29, Rn. 109 (zitiert nach juris).

378 Dies liefe im Wesentlichen auf eine Unterscheidung der verfügbaren Datenformate hinaus.

379 Bei der Dienstleistungsart könnte beispielsweise unterschieden werden zwischen den bereits näher erläuterten Diensten IaaS, SaaS und PaaS, in Anlehnung an das TKG und das TMG zwischen Telekommunikationsdiensten und Telemediendiensten oder im Hinblick auf den Ort der Datenverarbeitung zwischen Eigengeräten, individuellen Geräten Dritter und Cloud-Servern.

380 Für die Möglichkeit, die zugrundeliegende Dienstleistungsart jedenfalls als ein Klassifizierungsmerkmal von mehreren zu berücksichtigen: Europäische Kommission Services, *Technical Document*, S. 19; Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679).

Die Anwendung dieser Kriterien im Gesetz widerspräche jedoch der Prämisse der Technikneutralität. Sie würde mit dem rasanten technischen Fortschritt im IT-Bereich binnen kürzester Zeit zudem dazu führen, dass entsprechende Regelungen bestenfalls unvollständig und schlechtestenfalls obsolet würden.

Wichtiger noch: den genannten Kriterien fehlt jeglicher Grundrechtsbezug, weil nicht nachvollziehbar ist, welchen rechtserheblichen Einfluss das Dateiformat oder die zugrundeliegende Dienstleistung haben könnten. Es sind keine Anhaltspunkte dafür ersichtlich, warum diesen durchaus „abstrakten typischen Grundmerkmalen“ eines Datensatzes eine rechtliche Bedeutung zukommen könnte. Warum sollte eine Bilddatei einen anderen Grundrechtsschutz genießen als eine Textdatei – warum ein Festnetzanruf einen anderen als ein unmittelbar vom Telekommunikationsdienstleister ermöglichter Voice-over-IP Anruf?

Praktische Zuordnungsprobleme ergäben sich außerdem daraus, dass hinsichtlich der Dienstleistungsart häufig und auf verschiedenen Ebenen mehrere Dienstleister involviert sind[381] beziehungsweise die Trennlinie zwischen unterschiedlichen Dienstleistern zunehmend verschwimmt, sodass die Klassifizierung schnell an Übersichtlichkeit und Handhabbarkeit verlöre. Dies gilt nicht nur für die bereits erläuterte zunehmend schwierige Abgrenzung von Dienstleistern im Sinne des TKG einerseits und des TMG andererseits, sondern etwa auch im Hinblick auf Hardware-Hersteller, die zunehmend Kommunikationsdienstleistungen anbieten.[382]

Die Datenherkunft aus technischer Sicht entfällt daher aus rechtlichen und tatsächlichen Gründen als taugliches Klassifizierungskriterium.[383]

---

381 Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 23; Hiéramente / Fenina, *Telekommunikationsüberwachung und Cloud Computing, Der § 100a-Beschluss als Nimbus der Legalität?*, StraFo 2015, 365 (S. 2, zitiert nach juris), m.w.N.

382 Vgl. Hiéramente / Pfister, *Datenerhebung beim Hersteller von Mobiltelefonen, Zum Erfordernis des Strukturwandels bei der strafprozessualen Datenerhebung*, StV 2017, 477 (478).

383 Vgl. BVerfG, Urteil vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212): „Die Einordnung einer Leistung unter das Regelungsregime des Telekommunikationsgesetzes oder des Telemediengesetzes bestimmt

e) Datenzustand

Elektronische Daten werden nach ihrem Verarbeitungszustand zum Zeitpunkt des Abrufens in gespeicherte Daten („data in rest“) und Daten im Übermittlungsvorgang („data in transit“) unterteilt. Generell wird im Bereich der Kommunikation gespeicherten Daten ein höherer Schutz zugesprochen als Daten, die gerade übermittelt werden.[384]

Eine Klassifizierung nach dem Muster, wie sie im Katalog der Grundrechte bereits existiert – ausschließlich Daten im Übermittlungsvorgang werden von Art. 10 Abs. 1 GG erfasst, im Übrigen kommen die aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleiteten Grundrechte zum Tragen – brächte keinen Gewinn, weil sie als weiteres technisches Kriterium ohne ergänzende Differenzierung innerhalb der beiden Kategorien keine nähere Abwägung ermöglicht. Mit anderen Worten: die pauschale Einteilung erlaubt eine Zuordnung elektronischer Daten zu bestimmten Grundrechten, sagt jedoch nichts darüber aus, inwieweit die jeweiligen Schutzbereiche tatsächlich betroffen sind, in welchem Verhältnis diese in Bezug auf die Schutzwürdigkeit des jeweiligen Datensatzes zueinander stehen oder wie hoch die Eingriffsintensität bestimmter Ermittlungsmaßnahmen in Bezug auf bestimmte Datensätze ist. In diesem Sinne wird auch in der Gesetzesbegründung zu § 100g StPO festgehalten, dass für die Beurteilung der Eingriffsintensität von Ermittlungsmaßnahmen im Zusammenhang mit Telekommunikationsvorgängen die Qualität der erlangten Daten maßgeblich sei, nicht hingegen, ob sie bereits gespeichert, in Echtzeit erhoben oder künftig anfallen würden.[385]

Die Annahme, dass gespeicherte Datensätze schutzwürdiger seien als solche, die gerade übertragen werden, mag der herrschenden Meinung entsprechen, ist aber bei identischen Parametern im Übrigen rechtlich

---

nicht über die Reichweite des Schutzbereiches des Art. 10 Abs. 1 GG“.

384 Vgl. Gesetzesbegründung zur Neufassung der §§ 100a ff. StPO, BT-Ausschussdrucks. 18(6)334, S. 6, oder die unterschiedlichen gesetzlichen Anforderungen der §§ 100a (für „data in transit“) und 100b (für „data in rest“) StPO.

385 BT-Drucks. 16/5846, S. 50.

nicht zu begründen.

Zudem ergäben sich bei einer solchen Differenzierung praktische Schwierigkeiten der Bestimmung des jeweiligen Datenzustandes.
Dies verdeutlicht zum einen die Konstellation, in denen aus Sicht des Nutzers bestimmte Datensätze, wie beispielsweise Kontaktdaten oder Kalendereinträge, auf dem Smartphone gespeichert sind und diese Daten gleichzeitig wegen eingeräumter Zugriffsrechte durch eine App bemerkt oder unbemerkt an einen Dritten übersandt werden.[386]

Zuordnungsprobleme brächten auch Zugriffe auf die in der Cloud gespeicherte Daten, die, wie bereits erwähnt, aus Sicherheitsgründen automatisiert innerhalb der Cloud von einem Server zum nächsten verschoben werden und daher aus Nutzersicht fix gespeichert sind, sich aber tatsächlich häufig im Übertragungsvorgang befinden.

Wie schwierig und unklar die Bestimmung des aktuellen Datenzustandes ist, zeigt schließlich die Entscheidung des Bundesverfassungsgerichts zur Anwendbarkeit des Art. 10 Abs. 1 GG, der ausschließlich Daten im Übertragungsvorgang erfasst, auf beim E-Mail-Provider gespeicherte Nachrichten im IMAP-Verfahren,[387] selbst wenn diese vom Empfänger bereits gelesen wurden.[388] In der genannten Entscheidung betont das Bundesverfassungsgericht einerseits, dass Art. 10 Abs. 1 GG lediglich auf „laufende Kommunikationsvorgänge“ (also Daten „in transit“) Anwendung finde,[389] dies aber nicht ausschließe, dass die Daten beim Zugriff „ruh[t]en“ und „ein

386 Die hohe Frequenz solcher Datenübermittlungen und ihr Ausmaß auf unerwartet viele Datensätze wurde in der Einführung dieser Arbeit ausführlich geschildert. Es kann daher nicht von einer ausnahmsweisen Situation ausgegangen werden, vielmehr dürfte sie mehr und mehr den Normalfall darstellen.

387 Laut Wikipedia, Suchbegriff *IMAP*, werden beim Internet Message Access Protocol (IMAP) Nachrichten über das Internet beim Provider lediglich abgerufen und verbleiben grundsätzlich dort, werden also weder auf das lokale Gerät des Nutzers übertragen noch beim Provider gelöscht. Das Verfahren bietet den Vorteil, dass auf bereits abgerufene Nachrichten jederzeit erneut und mit jedem beliebigen internetfähigen Gerät zugegriffen werden kann.

388 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43.

389 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 45.

Telekommunikationsvorgang in einem dynamischen Sinne nicht stattfinde“.[390] Damit wird die Grenzlinie zwischen beiden Datenzuständen weiter verwischt. Sie wird gänzlich aufgehoben, wenn das Bundesverfassungsgericht im Folgenden ausführt, dass die „faktischen Herrschaftsverhältnisse“ über die Daten das maßgebliche Anwendungskriterium für Art. 10 GG seien.[391]

In allen Beispielfällen lässt sich trefflich darüber streiten, ob die Daten zum kritischen Zeitpunkt, in dem der behördliche Zugriff erfolgt, als gespeichert oder als im Übertragungsvorgang zu qualifizieren sind.

Für die angestrebte Differenzierung, die rechtlich begründet und gleichzeitig zweckmäßig sein soll, ist der Rückgriff auf den jeweiligen Datenzustand daher ungeeignet.

f) Analogie des Datenschutzrechts

Mit der DS-Richtlinie Strafjustiz, die bis spätestens 06.05.2018 in nationales Recht umzusetzen ist,[392] wird in Übereinstimmung mit der Begriffsverwendung der DS-GVO und des Bundesdatenschutzgesetzes eine Datenklassifizierung in personenbezogene Daten und nicht-personenbezogene Daten vorgenommen, wobei sich der eigentliche Regelungsgegenstand dieser Gesetze ausschließlich auf personenbezogene Daten bezieht.[393] Sie werden in sensible und weniger sensible Datenkategorien unterteilt.[394] Die Unterscheidung beruht im Wesentlichen auf den derzeitigen gesellschaftlichen Wertvor-

390 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 47.
391 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 46.
392 Art. 63 Abs. 1 DS-Richtlinie Strafjustiz.
393 Gemäß Art. 3 Nr. 1 DS-Richtlinie Strafjustiz und Art. 4 Nr. 1 DS-GVO handelt es sich bei personenbezogenen Daten um „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.
394 Schwichtenberg, *Die „kleine Schwester“ der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz*, DuD 2016, 605 (607).

stellungen.[395]

Tatsächlich sind in der StPO Regelungen zu finden, die einzelne der personenbezogenen Datenkategorien aus dem Datenschutzrecht aufgreifen. Beispielhaft sei auf Regelungen wie § 100g StPO zu Standortdaten, § 100j StPO zu Namen und Kennnummern, § 81a StPO zu Gesundheitsdaten, § 81b StPO zu biometrischen Daten und § 81e ff. StPO zu genetischen Daten verwiesen. Bemerkenswerterweise folgen die strafprozessrechtlichen Regelungen jedoch nicht unbedingt der Wertung des Datenschutzrechts, was sich an folgendem Beispiel zeigt: Während im Datenschutzrecht genetische und biometrische Daten gleichrangig als sensibel betrachtet werden,[396] stellt die StPO für die Erlangung und Verwertung erstgenannter Daten in §§ 81e ff. StPO erhebliche Hürden auf, während ein Fingerabdruck als biometrischer Datensatz gemäß § 81b StPO unter äußerst geringen Bedingungen abgenommen und verwendet werden darf.[397]

Ungeachtet der Tatsache, dass es sich im Datenschutzrecht um eine sehr grobe Einteilung handelt, spricht gegen ihre vorbehaltlose Übertragung auf das Strafprozessrecht, dass die datenschutzrechtlichen Regelungen eine – aus datenschutzrechtlicher Sicht und mit dem Fokus auf das Recht auf informationelle Selbstbestimmung konsequente – besondere Schutzwürdigkeit von Daten *über* eine natürliche Person postulieren, die direkt oder indirekt mit deren identitätsstiftenden Merkmalen zusammenhängt. Dabei vernachlässigen sie aber jedenfalls teilweise die strafprozessual gleichfalls relevanten Daten *von* einer natürlichen Person, die durch Art. 10 Abs. 1

395 Hinsichtlich der sensiblen Daten nennen Art. 10 DS-Richtlinie Strafjustiz und Art. 9 Abs. 1 DS-GVO übereinstimmend die „besonderen Kategorien personenbezogener Daten“ und meinen damit solche, „aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen“ sowie „genetische Daten, biometrische Daten […], Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung“.

396 Vgl. Art. 10 DS-Richtlinie Strafjustiz und Art. 9 Abs. 1 DS-GVO.

397 Laut Schwichtenberg, *Die „kleine Schwester“ der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz*, DuD 2016, 605 (608), sehe die StPO lediglich für genetische Daten in §§ 81e ff. StPO spezielle Schutzmechanismen vor, während für alle sonstigen sensiblen personenbezogenen Daten im Sinne des Datenschutzrechts im Strafprozessrecht keine besonderen Anforderungen für ihre Verarbeitung vorgesehen seien.

GG und dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme geschützt werden und häufig nicht die datenschutzrechtlichen Inhaltsanforderungen erfüllen.
Die Einschränkung ergibt sich unter anderem aus der Überlegung, dass das Fernmeldegeheimnis und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme grundsätzlich alle Daten ungeachtet ihres Inhaltes erfassen, während das Datenschutzrecht auf bestimmte Dateninhalte abstellt. Dies ist, wie ausführlich dargestellt, aus strafprozessualer Sicht nicht zielführend.

Ihre uneingeschränkte Übertragung auf das Strafprozessrecht kommt daher nicht in Betracht.[398]

g) Relevanz für das Strafverfahren / Schwere des zugrundeliegenden Deliktes

Zum Teil wird als Klassifizierungsmodell eine Fokussierung auf die strafprozessuale Bedeutung bestimmter Datensätze angedacht, also auf die jeweiligen Informationsbedürfnisse der Strafverfolgungsbehörden.[399] Danach wäre der anzunehmende Grundrechtsschutz umso geringer, je praxisrelevanter bestimmte Datensätze wären; die grobe Einteilung lautete etwa „sehr relevant“, „durchschnittlich relevant“ und „wenig relevant“.

Es handelt sich jedenfalls unter dem Aspekt um ein sachgerechtes Unterscheidungskriterium, dass den Strafverfolgungsbehörden ein erleichterter Zugang zu entscheidenden Beweismitteln gewährt werden sollte, während auf zusätzliche, weniger wichtige Beweismittel möglicherweise auch verzichtet werden kann.

Zweifel an einem solchen Klassifikationsmodell ergeben sich allerdings zum einen daraus, dass zur Vermeidung einer Endlosschleife der

398 So im Ergebnis auch Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679).
399 Svantesson, *Data categorisation and law enforcement access to cloud data*.

Maßstab zur Relevanzbestimmung kein allgemeiner statistischer Wert sein dürfte, weil die statistische Erhebung ihrerseits unterschiedliche Datenkategorien voraussetzen würde: Die Aussage, dass relevant sei, was sich in früheren Fällen als relevant erwiesen habe, bringt keinen Erkenntnisgewinn. Für den Rückgriff auf statistische oder allgemeine Erfahrungswerte müsste vielmehr vorab eine Datenkategorisierung anhand sonstiger Kriterien vorgenommen worden sein, um sodann eine weitere Einteilung anhand des Relevanzkriteriums durchführen zu können. Dieser Ansatz führt daher nicht weiter.

Stellte man hingegen auf die Relevanz des Datensatzes für den konkreten Fall ab, ergäbe sich zum einen das praktische Problem, dass diese vor der Erlangung und Verwertung im laufenden Verfahren nicht verlässlich dargestellt werden könnte. Aus rechtsdogmatischer Sicht wäre zudem zu berücksichtigen, dass bei einer solchen Vorgehensweise die konkreten Umstände des Einzelfalles das maßgebliche Kategorisierungsmerkmal darstellten, sodass schwerlich angenommen werden könnte, es handele sich um ein typisches Merkmal, um ein allgemeines Charakteristikum des betroffenen Datensatzes, das losgelöst vom Einzelfall bestimmbar sei.

Ungeachtet der genannten Umsetzungsprobleme würde die Einordnung eines Datensatzes anhand seiner statistischen oder konkreten Relevanz für das Strafverfahren zu der Situation führen, dass auf der Rechtsfolgenseite einer gesetzlichen Regelung unterschiedlich strenge Eingriffsbedingungen und Voraussetzungen postuliert würden,[400] ohne dass diese einen Bezug zur Eingriffsintensität einzelner Maßnahmen im Hinblick auf den jeweiligen Datensatz aufwiesen. Solche Bedingungen und Voraussetzungen könnten sich beispielsweise auf die Antragsbefugnis oder das Erfordernis der richterlichen Genehmigung beziehen. Datenbezogene Kriterien schieden aus, weil sie, vergleichbar mit der statistischen Erhebung, ihrerseits sonstiger Kategorisierungs-merkmale bedürften, um deren Herleitung es ja gerade geht.

400 Gäbe es keine Unterschiede auf der Rechtsfolgenseite, könnte auf die Datenkategorisierung vollständig verzichtet werden; sie dient alleine dem Zweck, unterschiedliche Regelungen für unterschiedliche Datenarten zu ermöglichen.

Jedenfalls blieben die einschlägigen Grundrechte des Betroffenen völlig außer Betracht, was erkennbar nicht mit der modernen Gesetzgebungslehre vereinbar wäre.

Dies gilt entsprechend für die Erfassung der Schwere des im Einzelfall zugrundeliegenden Deliktes. Es ergäben sich Regelungen nach dem Muster des Deliktes auf der Tatbestandsseite und – datenunabhängiger – Eingriffsvoraussetzungen auf der Rechtsfolgenseite, ohne dass der jeweiligen Datenart eine Bedeutung zukäme. Die Regelungen entsprächen, wenn auf die Schwere des Deliktes als maßgebliches Unterscheidungskriterium abgestellt würde, folgendem Muster: „Wenn es sich um eine durchschnittliche / schwere / besonders schwere Straftat handelt, dürfen elektronische Daten [sämtlich, weil unterschiedslos] unter einfachen / strengeren / besonders strengen Voraussetzungen erhoben werden“.

Die zwingende Schlussfolgerung, dass die Relevanz eines Datensatzes und die Schwere des zugrundeliegenden Deliktes keine geeigneten Unterscheidungskriterien für strafprozessuale Zwecke sind, weil sie die Anforderungen der modernen Gesetzgebungslehre an allgemeine, vom Einzelfall losgelöste Unterscheidungskriterien nicht erfüllen, schließt nicht aus, dass sie in der verfahrensrechtlichen Prüfung dennoch zur Anwendung kommen. Für jede Maßnahme, die abstrakt als Gesetz oder konkret im Einzelfall die Erlangung und Verwertung elektronischer Daten ermöglicht, ist im Rahmen der Verhältnismäßigkeitsprüfung zu klären, ob der entsprechende Datensatz für die Strafverfolgungsarbeit überhaupt hilfreich – relevant – sein könnte und wenn ja, welche behördliche Ermittlungshandlung verhältnismäßig, also zur Aufklärung der konkreten Straftat geeignet, erforderlich und angemessen ist.[401] Für die Bestimmung der Verhältnismäßigkeit der in Frage stehenden Ermittlungshandlung wird eine Abwägung vorgenommen, bei der ihr der in der Regel aus den Allgemeininteressen und den Grundrechten Dritter abgeleitete Zweck und Nutzen dem Grundrechtsschutz des Betroffenen gegenübergestellt wird,[402] sodass den genannten Kriterien

401 Die Klärung der genannten Merkmale entspricht der üblichen Verhältnismäßigkeitsprüfung (vgl. etwa BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 218).

402 Vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07,

– auf dieser Ebene - durchaus eine entscheidende Rolle zukommen kann.

h) Anwendbare Ermittlungsmaßnahmen

Abschließend soll untersucht werden, inwieweit auf die zur Verfügung stehenden Ermittlungsmaßnahmen jedenfalls als eines von mehreren Kriterien abgestellt werden kann.[403]

Es würde danach beispielsweise unterschieden zwischen Daten, die von Dritten herausgegeben werden können, Daten die von den Ermittlungsbehörden offen erhoben werden können und Daten, die durch eine verdeckte Ermittlungsmaßnahme erlangt werden können. Anders als die beiden vorgenannten Unterscheidungskriterien wäre diese Zuordnung nicht vom Einzelfall abhängig, sondern sie würde ein abstraktes, typisches Grundmerkmal eines Datensatzes darstellen.

Bei genauer Betrachtung wird jedoch schnell klar, dass dieser Ansatz die allgemeine Struktur gesetzlicher Regelungen auf den Kopf stellt: die Befugnisse zur Durchführung bestimmter Ermittlungsmaßnahmen sind die Rechtsfolgen einer unterschiedlichen Kategorisierung einer Beweismittelart. Sie können also nicht zugleich deren Grundlage sein, weil sich ansonsten der Zirkelschluss „eine Maßnahme, die rechtlich erlaubt ist, ist rechtlich erlaubt“ ergibt.
In Bezug auf elektronische Daten ist zu berücksichtigen, dass aus technischer Sicht generell alle Daten vom Dateninhaber verlangt oder durch eine verdeckte Maßnahme abgegriffen werden können – die Frage an den Gesetzgeber lautet, inwieweit dies jeweils rechtlich zulässig sein soll, und die Beantwortung dieser Frage hängt, wie ausführlich dargelegt, von der jeweiligen Sensibilität des betroffenen Datensatzes ab.

Die unterschiedlichen Voraussetzungen und Bedingungen einer

zugleich BVerfGE 120, 274, Rn. 227, m.w.N.

403 Vgl. Europäische Kommission Services, *Technical Document*, S. 19, die hinsichtlich der zur Verfügung stehenden Ermittlungsmaßnahmen beispielhaft zwischen Herausgabeverfügungen an den Betroffenen oder an Dritte und selbst durchgeführten Abhörmaßnahmen unterscheiden.

bestimmten Ermittlungsmaßnahme finden ihre Begründung nicht in der jeweiligen Maßnahme als solche, sondern darin, dass dieser Maßnahme eine bestimmte Eingriffsintensität zugesprochen wird, die gerade der Kern des Problems ist, das der diskutierte Ansatz nicht löst.

4. Zwischenergebnis

Es gibt verschiedene Kriterien, nach denen elektronische Daten sortiert und klassifiziert werden können.

Ob sich ein Kriterium zur Unterscheidung eignet, hängt maßgeblich erstens vom Sinn und Zweck der Klassifizierung sowie zweitens davon ab, ob es auf abstrakte typische Grundmerkmale oder auf die Umstände des Einzelfalles abstellt, und drittens davon, ob das Unterscheidungsmerkmal grundrechtlich relevant ist oder nicht.
Zudem gibt es Kriterien, die zwar für sich genommen nicht zielführend sind, als Nebenaspekte aber durchaus Berücksichtigung finden könnten.

Um ein Bild aus dem Sport zu bemühen: Eine Hochsprungleistung ließe sich beispielsweise nach der Sprunghöhe, der Anlaufgeschwindigkeit und Windrichtung oder der Zuschaueranzahl kategorisieren. Während letztgenannte Alternative zwar zur Bestimmung der Werbewirksamkeit geeignet scheint, ist sie offensichtlich ungeeignet und die Sprunghöhe offensichtlich sehr geeignet, um eine sportliche Leistung zu klassifizieren. Die Anlaufparameter hingegen sind dafür zwar nicht ausschlaggebend, beeinflussen die Sprunghöhe aber unmittelbar und können daher gegebenenfalls als punktuelle Indizien für die Sprungleistung herangezogen werden.
Allerdings genügt es nicht, auf die Sprunghöhe als maßgebliches Unterscheidungskriterium zu verweisen, wenn unklar ist, wie diese konkret bemessen werden soll; es bedarf zur Unterscheidung einer konkreten Maßeinheit.

Auf die rechtliche Lage übertragen bedeutet dies zum einen, dass bei der Bestimmung eines geeigneten Unterscheidungskriteriums primär

und sehr genau auf den Sinn und Zweck der vorzunehmenden Unterscheidung geachtet werden muss.
Im Strafprozessrecht liegt der Sinn und Zweck einer Kategorisierung in der abstrahierenden Bestimmung der jeweiligen Grundrechtsschutz-betroffenheit, nach der sich die Zulässigkeit einer Eingriffsmaßnahme richtet. Aus den obigen Überlegungen ergibt sich, dass die Intensität der Grundrechtsschutzbetroffenheit, also die Sensibilität des jeweiligen Datensatzes nach verfassungsrechtlichen Maßstäben das alleinige Klassifizierungsmerkmal für elektronische Daten ist, das auf abstrakte typische Grundmerkmale abstellt. Ausschließlich aus ihr kann die Zulässigkeit unterschiedlicher Ermittlungsmaßnahmen abgeleitet werden.

Allerdings bedarf es, wie bei der Sprunghöhe, der Bestimmung einer Maßeinheit, also eines allgemein anwendbaren Kriteriums, durch das die Menge aller elektronischen Daten konkret kategorisiert werden kann. Die Herleitung eines solchen konkreten Kriteriums ist Gegenstand des folgenden Kapitels, weil die derzeit diskutierten konkreten Unterscheidungsmerkmale die verfassungsrechtlichen Vorgaben nicht erfüllen.

Als ungeeignete Maßstäbe für eine konkrete strafprozessuale Datenklassifizierung wurden der abstrakte Dateninhalt, das Datenvolumen, die Datenherkunft aus technischer Sicht, der aktuelle Datenverarbeitungszustand, die Relevanz der Daten für das Ermittlungsverfahren, die Schwere des zugrundeliegenden Deliktes sowie die konkret anwendbaren Ermittlungsmaßnahmen identifiziert. Diese Kriterien sind einzelfallbezogen, unerheblich für die rechtliche Schutzwürdigkeit eines konkreten Datensatzes oder widersprechen der verfassungsrechtlichen Struktur von Eingriffsermächtigungen.
Für die rechtliche Prüfung sind sie dennoch nicht gänzlich unbeachtlich, da sie teilweise diejenigen Kriterien widerspiegeln, die bei der Verhältnismäßigkeitsprüfung von der Rechtsprechung regelmäßig aufgegriffen werden. Die Anwendung der Kriterien auf der Stufe der Verhältnismäßigkeitsprüfung bekräftigt den hiesigen Ansatz, wonach diese Merkmale nicht geeignet sind, den Grundrechtsbetroffenheit zu

definieren, die vorab und auf einer vorgelagerten Stufe bestimmt werden muss.

Lediglich die datenschutzrechtlichen Kategorien können, vergleichbar mit den Anlaufparametern für die Sprungleistung, eine gewisse Indizwirkung entfalten, wenn es um die Bestimmung der Grundrechtsschutzbetroffenheit geht.[404] Zur Verwendung als alleiniges Abgrenzungsmerkmal genügen sie allerdings nicht.

404 So ausdrücklich für Kontoinhalts- und Kontobewegungsdaten, die datenschutzrechtlich als personenbezogene Daten zu subsumieren sind, als Indizien für eine erhöhte grundrechtliche Schutzwürdigkeit in strafprozessualer Hinsicht: BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 322, m.w.N.

IV. Herleitung einer Neuklassifizierung

Aus den vorherigen Ausführungen ergibt sich die Notwendigkeit einer Klassifizierung elektronischer Beweismittel zu strafprozessualen Zwecken, die sinnvollerweise nicht auf die bisherige Unterscheidung der Kommunikationsdaten zurückgreift, weil diese nicht mehr mit der verfassungsrechtlichen Werteordnung in Einklang steht. Vielmehr ist eine umfassende, sachgerechte Einteilung in dem Rahmen vorzunehmen, den die Grundrechte und die Grundprinzipien der verfassungsmäßigen Ordnung beschreiben.

Es wurde festgestellt, dass dies vorrangig anhand der daten-spezifischen Intensität der Grundrechtsschutzbetroffenheit erfolgen muss.

Gegenstand der folgenden Untersuchung ist daher die Herausarbeitung derjenigen Kriterien, die eine konkrete Bewertung der bislang nur abstrakt dargestellten Intensität der Grundrechtsschutzbetroffenheit erlauben.

Dazu werden zunächst die Schutzbereiche der einzelnen datenspezifischen Grundrechte vorgestellt und genauer dahingehend analysiert, nach welchen Kriterien ein Datensatz im Rahmen eines bestimmten Grundrechts eine höhere oder geringere Schutzwürdigkeit genießt (dazu unter 1.), wobei zwischen grundrechtsspezifischen (a)) und einem grundrechtsübergreifenden (b)) Aspekt, dem absoluten Schutz des Kernbereichs der privaten Lebensgestaltung, unterschieden werden kann.

Sodann werden aus den verschiedenen Aspekten allgemeingültige Aussagen zur Schutzwürdigkeit eines Datensatzes abstrahiert (2.). Mit deren Hilfe erfolgt sodann unter Berücksichtigung der erläuterten Prämissen – umfassende Klassifizierung aller elektronischen Daten, Technikneutralität und Abstraktion statt Katalogauflistung einzelner Datensätze – die eigentliche Neuklassifizierung (3.).

1. Konkretisierung des datenspezifischen Grundrechtsschutzbereiches

a) Datenspezifische Grundrechte[405]

Mit allen traditionellen Beweismitteln haben elektronische Daten gemein, dass nicht nur ein einzelnes, sondern unterschiedliche Rechte und Interessen berührt sein können und inhaltsbezogene Rechte wie beispielsweise das Recht auf unbeobachtete Meinungsäußerung gleichermaßen durch die Verwendung aller Beweismittel tangiert werden können. Daher macht es für die Grundrechtsbetroffenheit keinen Unterschied, ob beispielsweise der Inhalt eines Briefes über den Urkundenbeweis, den Zeugenbeweis, den Sachverständigenbeweis oder als elektronisches Beweismittel in die Hauptverhandlung eingeführt wird. Auch das Recht auf informationelle Selbstbestimmung, das sich auf die Erhebung und Verwendung personenbezogener Daten bezieht, ist zunächst technikneutral.[406]

Selbstverständlich gelten für die Erlangung und Verwertung elektronischer Beweismittel die allgemeinen Verfahrensgrundrechte und -prinzipien, wie sie sich aus dem Rechtsstaatsprinzip oder ausdrücklich aus dem Grundgesetz, der Charta der Grundrechte der Europäischen Union und der Europäischen Menschenrechtskonvention ergeben. Hervorzuheben sind in diesem Zusammenhang die Unschuldsvermutung,[407] das Recht auf ein faires Verfahren,[408] der Grundsatz, dass niemand zur Preisgabe ihn selbst belastender Informationen verpflichtet ist („nemo tenetur“), und das Erfordernis einer gesetzlichen Ermächtigungsgrundlage für alle Eingriffe staatlicher Gewalt in Rechte des Einzelnen, die dem Verhältnismäßigkeits-

405 Die Ausführungen zu den datenspezifischen Grundrechten basieren im Wesentlichen auf der Veröffentlichung Warken, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus*, Teil 1, NZWiSt 2017, 289 (291 ff.).

406 Die Datenerhebung der in Deutschland für 1983 geplanten und 1987 schließlich durchgeführten Volkszählung, in deren unmittelbaren Kontext das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts fällt, durch das das Recht auf informationelle Selbstbestimmung entwickelt wurde (BVerfG, Urteil vom 15.02.1983, 1 BvR 209/83, zugleich BVerfGE 65, 1), erfolgte noch per Hand auf Papierbögen.

407 Vgl. Art. 48 S. 1 GRC.

408 Vgl. Art. 47 S. 2 GRC, Art. 6 EMRK.

grundsatz zu folgen hat.[409]

Im Folgenden sollen nunmehr diejenigen Grundrechte angesprochen werden, die speziell bei elektronischen Beweismitteln zum Tragen kommen. Dies ist neben dem bereits mehrfach erwähnten Fernmeldegeheimnis des Art. 10 Abs. 1 GG (dazu unter aa)) das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seinen besonderen Ausprägungen als Recht auf informationelle Selbstbestimmung (bb)) und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (cc)). Eine kurze Erwähnung finden zudem die Berufsausübungsfreiheit aus Art. 12 Abs. 1 GG, die Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und der Eigentumsschutz des Art. 14 Abs. 1 GG (dd)).

aa) Fernmeldegeheimnis des Art. 10 Abs. 1 GG

Das Bundesverfassungsgericht hat mehrfach die Bedeutung des in Art. 10 Abs. 1 GG verankerten Fernmeldegeheimnisses im Zusammenhang mit elektronischen Beweismitteln betont. Es beinhaltet im Kern den Schutz der räumlich distanzierten Kommunikation, der „Fernkommunikation“,[410] bei der die Kommunikationspartner auf die Informationsübermittlung durch Dritte angewiesen sind.[411] Die grundrechtliche Schutzwürdigkeit dieser besonderen Art der Kommunikation beruht auf der fehlenden Beherrschbarkeit und Überwachungsmöglichkeit des Übertragungsvorganges, aus denen auf erleichterte Zugriffsmöglichkeiten Dritter und damit auch staatlicher Behörden geschlossen wird.[412] Grundrechtlich relevant sind also die spezifischen Risiken, die sich aus der Nutzung einer Fernmeldeeinrichtung als Kommunikationsmedium ergeben.[413] Sie stellen sich ausschließlich dann, wenn der Grundrechtsträger entscheidet, einen Datensatz über ein Medium zu übermitteln, zu

409 Vgl. Art. 52 Abs. 1 S. 2 GRC.
410 Vgl. nur BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 290, m.w.N.
411 BVerfG, Urteil vom 02.03.2006, 2 BvR 2099/04, zugleich BVerfGE 115, 166, Rn. 64 f., m.w.N.
412 BVerfG, Urteil vom 02.03.2006, 2 BvR 2099/04, zugleich BVerfGE 115, 166, Rn. 76.
413 BVerfG, Urteil vom 02.03.2006, 2 BvR 2099/04, zugleich BVerfGE 115, 166, Rn. 73, 81.

dessen Nutzung er aus technischer Sicht zwingend auf die Mithilfe eines Dritten angewiesen ist.

Der Grundrechtsschutz umfasst die unkörperliche Übermittlung von Informationen an individuelle Empfänger mithilfe des Telekommunikationsverkehrs medienunabhängig[414] – somit auch durch Kommunikationsdienste des Internets und nicht beschränkt auf den Telekommunikationsbegriff des TKG –[415] und ungeachtet der konkreten Ausdrucksform[416] unabhängig von der Frage, ob der staatliche Eingriff auf der Übertragungsstrecke oder am Endgerät stattfindet.[417] Das Fernmeldegeheimnis bezieht sich in erster Linie auf den Kommunikationsinhalt, sei er privater, geschäftlicher, politischer oder sonstiger Natur, daneben aber auch auf die Kommunikationsumstände[418] und somit unterschiedslos auf alle Daten, die sich auf die Tatsache der Kommunikation an sich, ihre Verbindungsmerkmale und ihren Inhalt beziehen.[419] Sie sind unmittelbar mit dem Kommunikationsteilnehmer verknüpft und daher als personenbezogene Daten zu qualifizieren.

Der Schutzbereich des Art. 10 Abs. 1 GG betrifft allerdings ausschließlich die laufende Kommunikation, er endet in dem Moment, in dem die Information beim Empfänger endgültig angekommen[420] und der Übertragungsvorgang beendet ist.[421] Nach dem Sinn und Zweck der

414 So ausdrücklich BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212).
415 BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212).
416 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 43, m.w.N.
417 Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (300).
418 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 44, m.w.N.; BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212), m.w.N., nennt als Beispiele für die näheren Kommunikationsumstände sowohl „die Tatsache der Kommunikation als auch […] die Verbindungsdaten über Teilnehmer, Anschlüsse und Nummern, unter welchen die Teilnehmer miteinander in Kontakt treten […] Hierzu zählen auch IP-Adressen“.
419 BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212).
420 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 45, m.w.N.
421 Inhaltlich sind Art. 7 GRC und Art. 8 Abs. 1 EMRK insoweit umfassender, als ganz allgemein die „Achtung [der] Kommunikation“ beziehungsweise die „Achtung [der] Korrespondenz“ gewährleistet wird. Art. 11 Abs. 1 S. 2 GRC gewährt zudem explizit die Freiheit, „Informationen und Ideen ohne

Norm bedeutet die endgültige Ankunft beim Empfänger die Begründung dessen alleiniger Zugriffsgewalt. Sie fehlt beispielsweise bei E-Mail-Postfächern, auf die über das IMAP-Verfahren nur mithilfe einer Internetverbindung zugegriffen werden kann; dies gilt – grundsätzlich ohne zeitliche Begrenzung -[422] selbst dann, wenn der Empfänger die Nachrichten bereits gelesen hat,[423] da der E-Mail-Provider in diesen Fällen sowohl technisch in der Lage als auch rechtlich dazu befugt ist, sich unter bestimmten Voraussetzungen Zugriff auf die Nachrichten zu verschaffen.[424]

Der Schutz des Fernmeldegeheimnisses gilt gegenüber staatlicher Kenntnisnahme unabhängig davon, ob diese verdeckt oder offen erfolgt.[425] Während eine staatliche Kenntnisnahme der Kommunikationsdaten von den Kommunikationspartnern nicht erwartet werden muss, impliziert die Einschaltung eines Dritten zur Informationsübermittlung, dass dieser notwendig Kenntnis der Verbindungsmerkmale erhält, da diese sich unmittelbar auf seine Leistungserbringung beziehen. Dies ist offensichtlich, da beispielsweise die Datenübermittlung ohne Angabe eindeutiger Kenndaten der Kommunikationspartner unmöglich ist und die Kommunikationsdauer maßgeblich den Leistungsumfang bestimmt.
Allerdings beinhaltet die Eingehung eines Teilnehmer- oder Benutzerverhältnisses im Telekommunikationsbereich keine Einwilligung der Kommunikationspartner in den Zugriff des Übermittlungsdienstes auf den Kommunikationsinhalt; das gilt selbst

---

behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben“.

422 Sieber, *Gutachten zum 69. DJT*, S. 110, m.w.N.

423 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 48.

424 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 46 f., mit dem bereits zitierten Hinweis, dass dieser Auffassung nicht entgegenstehe, dass der Telekommunikationsvorgang „in einem dynamischen Sinn“ nicht stattfinde, während die Daten auf dem Mailserver des Providers ruhten; Brodowski, *Strafprozessualer Zugriff auf E-Mail-Kommunikation # zugleich Besprechung zu BVerfG, Beschl. v. 16.06.2009 # 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.03.2009 # 1StR 76/09*, JR 2009, 402 (404), m.w.N.

425 Vgl. BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 94, mit dem Hinweis darauf, dass anlässlich der Sicherstellung von beim Provider gespeicherten E-Mails, die einen Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG darstellt, der Betroffene „im Regelfall zuvor“ von den Strafverfolgungsbehörden zu unterrichten sei.

dann, wenn dieser Zugriff erkennbar technisch möglich ist.[426]

Art. 10 Abs. 1 GG findet hingegen für solche Informationen, die aufgrund der freiwilligen Gestattung eines der Kommunikationspartner zur Teilnahme am Kommunikationsprozess erlangt werden, keine Anwendung. Das gilt selbst dann, wenn es sich beim Dritten um eine staatliche Behörde handelt und der weitere Kommunikationspartner keine Kenntnis von der Teilnahme des Dritten hat.[427] Dies wird damit begründet, dass das Fernmeldegeheimnis mit dem Fokus auf den übertragungsspezifischen Risiken nicht das Vertrauen in die Verlässlichkeit des Kommunikationspartners schützt.[428]

Aus der Gesamtbetrachtung all dieser Aspekte ergibt sich, dass Art. 10 Abs. 1 GG keine Aussage zur unterschiedlichen Schutzwürdigkeit einzelner Datensätze, die im Rahmen einer laufenden Kommunikation anfallen, trifft. Auch sind keine Hinweise darauf erkennbar, in welchem Verhältnis die Sensibilität aktuell kommunizierter Daten im Verhältnis zu der lokal verarbeiteter oder gespeicherter steht; das Fernmeldegeheimnis gestattet keine Feststellung der Art, dass von ihm erfasste Daten eine höhere oder geringere Schutzwürdigkeit als sonstige Daten haben.

Vielmehr lautet die Kernaussage des Fernmeldegeheimnisses, dass Informationen, die aus dem Herrschaftsbereich des Verfügungsbefugten herausgetragen werden, grundsätzlich weiterhin dem Geheimnisschutz unterfallen und nicht deshalb als unbeschränkt zugänglich betrachtet werden dürfen, nur weil sie ja ohnehin zur Übermittlung an einen Diensteerbringer bekanntgegeben werden.[429]

426 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 56.

427 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 293.

428 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 290 f. Zur grundsätzlichen Anerkennung eines in rechtlicher Hinsicht schutzwürdigen Vertrauens in die Identität und Wahrhaftigkeit des Kommunikationspartners vgl. die folgenden Ausführungen zum Schutzbereich des Rechts auf informationelle Selbstbestimmung.

429 In Zeiten, in denen persönlich aufgegebene Telegramme noch eine größere Rolle für die Fernkommunikation spielten und – immerhin bis Mitte 1966 (s. Wikipedia, Suchbegriff *Vermittlungsstelle*) - Telefonverbindungen über „das Fräulein vom Amt“ liefen, konnte

Allerdings schützt Art. 10 Abs. 1 GG grundsätzlich nicht vor einem entsprechenden Vertrauensbruch des Kommunikationspartners.

bb) Recht auf informationelle Selbstbestimmung

Subsidiär zu Art. 10 Abs. 1 GG, also für die Fälle, in denen der Schutzbereich des Fernmeldegeheimnisses nicht betroffen ist, greift das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete allgemeine Persönlichkeitsrecht zugunsten des Betroffenen.[430]
In Bezug auf die Erlangung und Verwertung von persönlichen Daten hat das Bundesverfassungsgericht im Volkszählungsurteil bereits 1983 hieraus das Recht auf informationelle Selbstbestimmung entwickelt.[431] Es umfasst „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[432]

Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden, sondern erfasst auch solche personenbezogenen Daten, die für sich genommen nur einen geringen Informationsgehalt haben.[433] Auch wenn das Recht unabhängig vom jeweiligen Datenformat besteht, werden in der Praxis persönliche Daten heute überwiegend bereits

durchaus argumentiert werden, dass die offensichtliche Möglichkeit der inhaltlichen Kenntnisnahme durch die Übermittlungsstelle einer, wenn auch nicht unbedingt beabsichtigten, so doch bewussten Aufhebung des Geheimnisschutzes gleichkam. Dieser Auffassung widersprach Art. 10 GG bereits in seiner ursprünglichen Fassung vom 23.05.1949 (BGBl. I S. 1). Heute, bei digitaler Datenübermittlung und dem weitverbreiteten Einsatz von Ende-zu-Ende Verschlüsselung ergibt sich diese Bedeutung des Art. 10 GG nicht mehr ohne Weiteres.

430 So ausdrücklich für „außerhalb eines laufenden Kommunikationsinhaltes im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherte Inhalte und Umstände der Kommunikation": BVerfG, Beschluss 25.07.2007, 2 BvR 2282/06, Rn. 8 (zitiert nach juris); außerdem für alle „Verbindungsdaten, die nach Abschluss eines Kommunikationsvorganges […] aufgezeichnet und gespeichert werden": BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212), m.w.N.

431 BVerfG, Urteil vom 15.02.1983, 1 BvR 209/83, zugleich BVerfGE 65, 1; parallel dazu gewährt Art. 8 Abs. 1 GRC allgemein den Schutz personenbezogener Daten.

432 BVerfG, Urteil vom 15.02.1983, 1 BvR 209/83, zugleich BVerfGE 65, 1, Leitsätze 1 und 2.

433 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 198, m.w.N.

digital erhoben oder, sofern dies nicht der Fall ist, jedenfalls digitalisiert gespeichert. Der Zugriff auf persönliche Daten und damit der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung betrifft daher de facto nahezu ausschließlich elektronische Daten.

Der Begriff der persönlichen Daten wird in Anlehnung an das Bundesdatenschutzgesetz sehr weit verstanden; er umfasst sämtliche Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.[434] Umfasst werden solche Daten, die unmittelbar der Privatsphäre des Betroffenen zuzuordnen sind, und solche, die im Kontext ihrer Entstehung oder einer möglichen Verknüpfung mit anderen Daten jedenfalls einen punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen aufweisen[435].[436]

Um eine wahre Selbstbestimmung zu gewährleisten, darf der Informationsgehalt des betroffenen Datensatzes bei der Frage, ob überhaupt das Selbstbestimmungsrecht tangiert ist, keine Rolle spielen; auf ihn kommt es, jedenfalls solange es sich um personenbezogene Daten handelt, für die Eröffnung des Grundrechtsschutzes nicht an.[437] Die Sensibilität eines Datensatzes und damit der Grad der grundrechtlichen Schutzwürdigkeit hängt vielmehr vom konkreten Kontext ab,[438] insbesondere von der Bedeutung, die die Information für den Betroffenen hat und die sie durch Einbeziehung in andere Zusammenhänge gewinnen kann.[439] Dabei können auch

434 BVerfG, Urteil vom 15.02.1983, 1 BvR 209/83, zugleich BVerfGE 65, 1, Rn. 147 (zitiert nach juris); vgl. auch EuGH, Urteil vom 19.10.2016 („Breyer“), C-582/14, für die Einordnung einer dynamischen IP-Adresse als personenbezogenes Datum, wenn mithilfe rechtlicher Mittel die betreffende Person anhand weiterer, gegebenenfalls von Dritten erhältlicher Zusatzinformationen bestimmt werden kann.

435 Gemäß BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 202, liegt ein solch punktueller Bezug beispielsweise bei Daten einer nicht vernetzten elektronischen Steuerungsanlage der Haustechnik vor. Auch diesbezüglich, so das Bundesverfassungsgericht, könne ein vom Recht auf informationelle Selbstbestimmung geschütztes berechtigtes Geheimhaltungsinteresse des Betroffenen bestehen.

436 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 197.

437 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 198, m.w.N.

438 BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, zugleich BVerfGE 130, 151, Rn. 122, m.w.N.

439 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich

flüchtige oder nur temporär gespeicherte Daten eine besondere Relevanz für die Persönlichkeit des Betroffenen aufweisen oder – etwa als Passwort - einen Zugriff auf weitere, besonders sensible Daten ermöglichen.[440]

Das Recht auf informationelle Selbstbestimmung schließt neben der Verfügungsbefugnis über das Ob der Datenerlangung und -verwertung durch Dritte auch die Entscheidungsbefugnis darüber ein, wem dies gestattet wird.
Dabei kann je nach den Umständen des Einzelfalles das Vertrauen in die Identität und die Motivation des Dritten selbst ein vom informationellen Selbstbestimmungsrecht umfasstes schutzwürdiges Vertrauen des Betroffenen ergeben.[441]

Eine besondere Ausprägung des Grundrechts im Hinblick auf elektronische Daten liegt schließlich in der zielgerichteten Erfassung von im Einzelnen jeweils rechtmäßig zugänglichen Daten, um diese gegebenenfalls unter Hinzuziehung weiterer Daten auszuwerten und dadurch ein Persönlichkeitsprofil des Betroffenen zu erstellen.[442] Dieser Punkt hat für die Datenklassifizierung allerdings keine Bedeutung, weil er eine Handlungsebene betrifft, die über der Datenerlangung und der einfachen Verwertung liegt; er bezieht sich gleichsam auf alle personenbezogenen Daten und hat daher auf ihre originäre Klassifizierung keinen Einfluss.

cc) Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Mit der Entwicklung dieses Grundrechts hat das Bundesverfassungsgericht erstmals im Jahr 2008 auf die Lücken des Grundrechtsschutzes

BVerfGE 120, 274, Rn. 197.

440 BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, zugleich BVerfGE 130, 151, Rn. 236

441 Vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 311, mit einer negativen Abgrenzung; kritisch dazu: Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (305); Sieber, *Gutachten zum 69. DJT*, S. 125 f.

442 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 309.

hinsichtlich der Nutzung informationstechnischer Systeme reagiert.[443] Nach Auffassung des Bundesverfassungsgerichts trage das Recht auf informationelle Selbstbestimmung denjenigen Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergäben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen sei und dabei dem System persönliche Daten anvertraue oder schon allein durch dessen Nutzung zwangsläufig liefere.[444] Im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse entstünden neuartige Gefährdungen und Schutzlücken, denen das allgemeine Persönlichkeitsrecht dadurch begegne, dass es die Vertraulichkeit und Integrität informationstechnischer Systeme gewährleiste.[445] Das Bundesverfassungsgericht führt weiter aus: „Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten“.[446]

Der Schutzbereich des allgemeinen Persönlichkeitsrechts wird also insoweit erweitert, als keine bestimmten personenbezogenen Daten betroffen sein müssen, sondern Maßnahmen erfasst werden, die ganz

443 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274.

444 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 200; Di Fabio, *Die algorithmische Person*, spricht von einer „präzedenzlose[n] Risikolage für die Durchleuchtung des Menschen“ und „Analyse- und Rekonstruktionsmöglichkeiten in neuer Qualität, so dass die bloße Quantität riesiger Datenmengen und zahlloser digitaler Spuren in eine Qualität hochleistungsfähiger Auswertungsmöglichkeiten“ umschlage.

445 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 169.

446 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 201; Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (302), weist darauf hin, dass der Schutz der Vertraulichkeit informationstechnischer Systeme bereits durch das Recht auf informationelle Selbstbestimmung hinreichend gewährleistet sei, allerdings sei die Betonung der Integrität solcher Systeme davon getrennt zu sehen und könne dazu führen, den Schutzbereich des Rechts „verdinglicht zu begreifen“.

allgemein die Nutzung von Leistungen, Funktionen und Speicherinhalten des Systems anstreben.[447] Im Fokus steht ausschließlich das System als solches unter dem Aspekt des Nutzerinteresses daran, dass, wenn der Nutzer davon ausgehen darf, dass er das System „als eigenes nutzt“ und darüber „selbstbestimmt verfügt“,[448] die dort vorhandenen Daten in ihrer Gesamtheit vertraulich und die Integrität des Systems unangetastet bleiben.[449] Damit werden für die Eröffnung des Grundrechtsschutzes sämtliche Daten im System unabhängig von ihrem Inhalt oder ihrer Wichtigkeit erfasst,[450] selbst wenn sich der Nutzer ihrer Erzeugung nicht bewusst ist.[451] Umgekehrt ist eine reine Internetaufklärung, also eine Kenntnisnahme öffentlich zugänglicher Informationen jenseits der als eigene genutzten informationstechnischen Systeme durch staatliche Behörden, grundrechtlich nicht relevant.[452]

Der Grundrechtsschutz bezieht sich nicht auf die Erhebung einzelner Daten,[453] sondern greift dort, wo das informationstechnische System alleine oder in seiner technischen Vernetzung Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten kann, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein

447 Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (303).

448 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 206; zur Problematik der Bedingung, dass das System „als eigenes“ genutzt werden müsse: Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (303).

449 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 204.

450 Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (302 f.).

451 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 178.

452 Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (305).

453 Diese wird, wie Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (301), zutreffend feststellt, jedenfalls und damit vorrangig vom Recht auf informationelle Selbstbestimmung erfasst.

aussagekräftiges Bild der Persönlichkeit zu erhalten.[454] Dies sei, so das Bundesverfassungsgericht, beispielsweise anzunehmen bei Personalcomputern und solchen Mobiltelefonen oder elektronischen Terminkalendern, „die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können“.[455] Aus der „können“-Formulierung wird deutlich, dass es nicht auf den konkreten Dateninhalt des Systems ankommt, sondern vielmehr nur auf seine Datenspeicher- und -verarbeitungskapazität.[456] Allerdings muss es sich potentiell um „personenbezogene“[457], „persönlichkeitsrelevante“[458] oder „persönliche“[459] Daten handeln. Das Bundesverfassungsgericht verwendet diese Begriffe ohne erkennbaren Unterschied und differenziert innerhalb der Gruppe „alle[r] Daten“, aus denen „sich ein umfassendes Bild vom Nutzer des Systems ergeben kann“,[460] weiter zwischen personenbezogenen Daten „mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen“[461] und Daten, „die seiner Privatsphäre zuzuordnen sind“[462].

Die Integrität des Systems ist datenunabhängig geschützt und spielt daher für datenspezifische Eingriffe lediglich im Rahmen der Verhältnismäßigkeitsprüfung eine Rolle. Demnach sind datenspezifische Eingriffe so vorzunehmen, dass die Integrität des betroffenen Systems so wenig wie möglich angetastet wird Diesen Gedanken greift § 100a Abs. 5 S. 1 Nr. 2 und 3, S. 2 StPO ausdrücklich auf. Danach ist sicherzustellen, dass „an dem informationstechnischen

454 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 203.
455 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 203.
456 Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (302).
457 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 203.
458 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 189.
459 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 200.
460 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 197.
461 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 202.
462 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 197.

System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Änderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden“; zudem ist das zur Kommunikationsüberwachung eingesetzte Mittel „nach dem Stand der Technik gegen unbefugte Nutzung zu schützen“.

dd) Berufs-, Wohnungs- und Eigentumsschutz (Art. 12 – 14 GG)

Art. 12 Abs. 1 GG, der die Berufsausübungs- und Organisationsfreiheit gewährt, spielt im Zusammenhang mit elektronischen Daten nur für behördliche Auskunfts- und Mitwirkungsverlangen an einen Kommunikations- oder Informationsdienstleister eine Rolle,[463] da die Informationen darüber, wie er bei ihm anfallende beziehungsweise ihm anvertraute Daten konkret verarbeitet, entsprechenden Grundrechtsschutz genießen.[464]

Die Art. 13 Abs. 1 und 14 Abs. 1 GG und ihre jeweiligen Pendants der GRC und der EMRK, die die Unverletzlichkeit der Wohnung und den Schutz des Eigentums gewährleisten,[465] weisen hingegen keinen speziellen Bezug zu elektronischen Beweismitteln auf[466] und sind nach der Rechtsprechung des Bundesverfassungsgerichts von vorneherein nicht betroffen, soweit es um die Sicherstellung, die Beschlagnahme oder die Durchsicht von Daten geht, die auf dem Server eines Providers, also extern, gespeichert sind, selbst wenn darauf mit einem Gerät in der Wohnung des Betroffenen zugegriffen werden kann.[467]

463 So ausdrücklich für klassische TKÜ-Maßnahmen gemäß § 100a StPO a.F.: BGH, Beschluss vom 20.08.2015, StB 7/15, Rn. 7 (zitiert nach juris).

464 Vgl. Sieber, *Kurzgutachten*, S. 5.

465 Für Art. 13 Abs. 1 GG: Art. 7 GRC und Art. 8 Abs. 1 EMRK; für Art. 14 Abs. 1 GG: Art. 17 GRC und Art. 1 Abs. 1 des Zusatzprotokolls zur EMRK.

466 So ausdrücklich für Art. 13 GG: BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 370/07, zugleich BVerfGE 120, 274, Rn. 194, m.w.N.

467 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 370/07, zugleich BVerfGE 120, 274, Rn. 194;
a.A. Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (301), zur Betroffenheit des Schutzbereiches von Art. 13 Abs. 1 GG jedenfalls für die Konstellation, in der sich das überwachte informationstechnische System innerhalb einer Wohnung befindet. Hier allerdings stellt sich die Frage, was vom Begriff des informationstechnischen Systems erfasst wird: Handelt es sich um Datenverarbeitungsgeräte, Speichermedien oder Daten an sich, die sich ausschließlich in der

b) Absoluter Schutz des Kernbereichs der privaten Lebensgestaltung

Unabhängig von den einzelnen datenspezifischen Schutzbereichen hat die Rechtsprechung eine Datenklasse herausgestellt, die eine besondere grundrechtliche Behandlung erfährt. Es handelt sich dabei um Daten, die den Kernbereich der privaten Lebensgestaltung betreffen.

Wie das Bundesverfassungsgericht im Urteil zum „Großen Lauschangriff“ erstmals 2004 ausführlich formuliert hat, folgt aus der in Art. 1 Abs. 1 GG verbürgten Unantastbarkeit der Menschenwürde zum Schutz der individuellen Entfaltung ein unantastbarer Kernbereich privater Lebensgestaltung, dessen Zugang staatlichen Stellen verwehrt ist.[468] Dieser Schutz ist absolut und bewirkt folglich ein unbedingtes Beweiserhebungs- und -verwertungsverbot auch für entsprechende Datensätze. Er dient der freien Entfaltung der Persönlichkeit,[469] zu deren Kernbereich die Möglichkeit gehört, „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen“.[470] Die

Wohnung befinden beziehungsweise ausschließlich dort anfallen, so ist der Schutzbereich des Art. 13 Abs. 1 GG wie bei allen anderen Beweismitteln betroffen, sodass sich keine Besonderheit ergibt. Befinden sich die Gegenstände oder Daten jedoch außerhalb der Wohnung und sind lediglich von dieser aus über das Internet zugänglich, ist regelmäßig davon auszugehen, dass der Zugang aus technischer Sicht auch von anderen Orten aus erfolgen kann und nicht nur auf die Wohnung beschränkt ist. Für diesen Fall ist die Bemühung des Art. 13 Abs. 1 GG nicht überzeugend.

468 BVerfG, Urteil vom 03.03.2004, 1 BvR 2378/98, zugleich BVerfGE 109, 279, Rn. 120, für den Fall der akustischen Wohnraumüberwachung; vgl. auch BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 271, m.w.N.
Dass es einen solch rechtlich schützenswerten Kernbereich der Persönlichkeit überhaupt gibt, wurde bereits 1957, im sogenannten Elfes-Urteil, festgestellt (BVerfG, Urteil vom 16.01.1957, 1 BvR 253/56, zugleich BVerfGE 6, 32). Mit dem am 24.08.2017 in Kraft getretenen § 100d StPO greift der Gesetzgeber nunmehr erstmals den Kernbereichsschutz explizit auf und verfolgt den Vorgaben des Bundesverfassungsgerichts gemäß einen zweistufigen Schutz auf Datenerhebungs- und Datenverwertungsebene.

469 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 271.

470 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 271, m.w.N.

Schutzwirkung erstreckt sich auf alle Grundrechte gleichermaßen und damit auf elektronische Daten ebenso wie auf nicht-elektronische.

Im Hinblick auf informationstechnische Systeme wird sowohl die Anlegung und Speicherung elektronischer Daten mit entsprechendem Inhalt als auch deren nichtöffentliche[471] Übertragung an bestimmte Kommunikationspartner im Rahmen einer vertraulichen Kommunikation erfasst.[472]

Ob ein Dateninhalt – unabhängig von seiner Weitergabe – einen höchstpersönlichen Charakter aufweist, hängt von den Besonderheiten des Einzelfalles ab[473] und kann regelmäßig erst nach seiner Durchsicht verlässlich beurteilt werden.[474] Allerdings werden Dateninhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten, nicht vom geschützten Kernbereich erfasst.[475]

Im Falle einer Datenweitergabe an Dritte sind für die Beantwortung der Frage, ob der Kernbereich privater Lebensgestaltung betroffen ist, neben dem Dateninhalt weitere Umstände des Einzelfalles entscheidend. In der bis 23.08.2017 gültigen Fassung des § 100c Abs. 4 S. 2 StPO fand sich - gesetzlich ausdrücklich normiert - die widerlegbare Annahme, dass Gespräche in Betriebs- oder Geschäftsräumen nicht diesem Kernbereich unterfielen. Diese Regelung wurde mit dem Hinweis des Gesetzgebers, dass es tatsächlich auf die Umstände des

---

471 BVerfG, Urteil vom 03.03.2004, 1 BvR 2378/98, zugleich BVerfGE 109, 279, Rn. 138.

472 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 272.

473 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 90, m.w.N.

474 BVerfG, Urteil vom 03.03.2004, 1 BvR 2378/98, zugleich BVerfGE 109, 279, Rn. 138.
Zur Problematik und rechtlichen Konsequenz, die sich daraus ergibt, dass sich die Schutzwürdigkeit in der Regel erst nach der Prüfung des Dateninhaltes feststellen lässt: BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 277, m.w.N.; Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (304).

475 Vgl. BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 90, m.w.N.; Hauck, in: Löwe-Rosenberg, *StPO*, § 100c, Rn. 43 (zitiert nach juris).

Einzelfalles ankomme und Betriebs- und Geschäftsräume nicht generell vom Kernbereich der privaten Lebensgestaltung ausgeschlossen werden könnten, ersatzlos aufgehoben.[476]

Maßgeblich wird es auf die Qualifikation des Kommunikationspartners als Person des höchstpersönlichen Vertrauens ankommen.[477] Deren Kreis deckt sich nur teilweise mit den Zeugnisverweigerungsberechtigten der StPO, bestimmt sich nicht nach formalen Kriterien wie etwa dem Verwandtschaftsverhältnis und kann neben Familien- und Haushaltsangehörigen auch enge persönliche Freunde einbeziehen.[478] Umgekehrt kann daraus geschlossen werden, dass die öffentliche Bekanntgabe selbst intimster Inhalte an einen nicht näher eingrenzbaren potentiellen Empfängerkreis nicht dem unantastbaren Kernbereich privater Lebensgestaltung zuzuordnen ist und folglich nicht dessen absoluten Schutz genießt.

2. Zusammenführung der Kriterien

Aus der Betrachtung der speziell datenrelevanten Grundrechtsschutzbereiche und der Kriterien, die ihre Betroffenheit bestimmen, lassen sich für die Kategorisierung allgemeine, grundrechtsübergreifende Aussagen treffen (dazu unter a)) und abstrahierende Schlussfolgerungen ziehen (b)), die beide schließlich als konkrete Unterscheidungskriterien zusammengeführt werden können (c)).

a) Allgemeine Feststellungen

Aus der Betrachtung der datenspezifischen Grundrechte lassen sich folgende allgemeinen Aussagen schlussfolgern:

aa) Personenbezogene Daten

Es sind nur solche Datensätze schutzwürdig, die dem betroffenen

476 Vgl. Gesetzesbegründung, BT-Ausschussdrucks. 18(6)334, S. 27, m.w.N.
477 BVerfG, Urteil vom 03.03.2004, 1 BvR 2378/98, zugleich BVerfGE 109, 279, Rn. 146 ff.
478 BVerfG, Urteil vom 20.04.2016, 1 BvR 966/09 und 1 BvR 1140/09, zugleich BVerfGE 141, 220, Rn. 121, m.w.N.

Grundrechtsträger zuzurechnen sind. Das ergibt sich aus der übereinstimmenden Bezugnahme aller datenspezifischen Grundrechte auf personenbezogene Daten: beim Fernmeldegeheimnis oder dem Recht auf Vertraulichkeit und Integrität eines informationstechnischen Systems mittelbar über die Verknüpfung mit einem konkreten Telekommunikationsvorgang oder einem konkreten eigenen System, oder unmittelbar, wie bei der Definition des Rechts auf informationelle Selbstbestimmung. Schließlich weist auch der Kernbereichsschutz einen eindeutigen personenbezogen Inhalt auf.

Der Begriff der personenbezogenen Daten wird ähnlich wie im Datenschutzrecht auch im Strafverfahrensrecht weit gefasst. Er bezieht sich auf alle Informationen über oder von einer bestimmten oder bestimmbaren Person. Umfasst werden damit insbesondere auch alle Daten, die der Betroffene extern, also beispielsweise in der Cloud, verarbeitet oder speichert. Es ist erforderlich, aber auch ausreichend, dass der Betroffene eine entsprechende Datenverarbeitung zurechenbar initiiert; er muss sie nicht mit seinen eigenen geistigen und körperlichen Mitteln vornehmen. Es genügt, wenn er die Entstehung der Daten oder ihre Übermittlung zurechenbar veranlasst; dazu kann er beliebig viele Algorithmen und Geräte zwischenschalten. Desweiteren ist es für die Eröffnung des Grundrechtsschutzes unerheblich, ob der entsprechende Datensatz nur einen punktuellen Bezug zu einem bestimmten Lebensbereich aufweist oder die Privatsphäre des Einzelnen betrifft.

Daraus ist in logischer Konsequenz zu schließen, dass auch Daten, die im Internet der Dinge entstehen, personenbezogene Daten sein können. Das gilt gleichsam für automatisiert hergestellte und lokal verbleibende Daten als auch für automatisiert hergestellte und sodann – aufgrund entsprechender Programmierung – an eine Person oder einen Rechner zur weiteren Verarbeitung übertragene Datensätze. Konkret sind hiermit Informationen angesprochen, die in der Maschine-zu-Mensch beziehungsweise der Maschine-zu-Maschine Kommunikation ausgetauscht werden.

Als Beispiel sei auf eine auf einem Privatgrundstück installierte digitale Überwachungskamera verwiesen, deren Aufnahmefunktion an einen Bewegungsmelder gekoppelt ist. Ihre automatisiert generierten Aufnahmedaten sind personenbezogene Daten im Hinblick auf den Grundstücksbesitzer, der die Kamera installiert hat, unabhängig davon, ob sie ohne regelmäßiges Auslesen lediglich auf dem Gerät gespeichert werden, möglicherweise aufgrund entsprechender Programmierung einen akustischen Alarm eines weiteren Gerätes auslösen oder alternativ an einen menschlichen Adressaten etwa bei der nächsten Polizeidienststelle weitergeleitet werden. In allen (und weiteren denkbaren Fällen) ist ihre Entstehung auf den Entschluss einer Person, den Grundstücksbesitzer, zurückzuführen.

Auch wenn für den Einzelfall Zuordnungsschwierigkeiten insbesondere von Datensätzen aus dem Bereich des Internets der Dinge zu einer bestimmten oder bestimmbaren Person zu erwarten sind,[479] ist nicht zu verkennen, dass jegliche Datenverarbeitung auf einer Programmierung beruht, deren Einsatz letztlich auf einer menschlichen Entscheidung basiert.[480] In jeder Konstellation, in der diese Entscheidung einem bestimmten Grundrechtsträger zuzurechnen ist, ist der betreffende Datensatz als personenbezogene Information zu qualifizieren.

bb) Verfahrensrechtliche Stellung des Grundrechtsträgers

Im Strafermittlungsverfahren sind vorwiegend solche personenbezogenen Daten von Bedeutung, die sich auf den Verdächtigen / Beschuldigten beziehen. Häufig können allerdings auch unverdächtige Dritte, namentlich das Opfer oder gänzlich Unbeteiligte (etwa bei der Funkzellenabfrage) betroffen sein. Für sie gilt der datenspezifische Grundrechtsschutz gleichermaßen.

---

479 Zuordnungsschwierigkeiten können sich insbesondere dann ergeben, wenn die Datenentstehung oder -verarbeitung nicht bewusst, sondern unbewusst, nur mittelbar oder unbefugt initiiert wird, außerdem in Fällen, in denen sie von der Entscheidung beziehungsweise von der Mitwirkung mehrerer Personen abhängt.

480 Mason, *Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now – But they Don`t Know it,* Computer and Telecommunications Law Review, 2017, Volume 23, Issue 8, S. 213 (214), m.w.N.

Ein Eingriff in die Rechte unverdächtiger Dritter ist nach höchstrichterlicher Rechtsprechung in besonderem Maße rechtfertigungsbedürftig,[481] was auf der Ebene der Verhältnismäßigkeit zu prüfen ist. Umgekehrt bedeutet dies, dass die Schutzwürdigkeit, also die Sensibilität eines personenbezogenen Datensatzes unabhängig davon ist, welche Stellung die betreffende Person im konkreten Strafverfahren hat; die verfahrensrechtliche Position wird erst auf anderer Ebene relevant, wenn es um die fallbezogene Zulässigkeit einer Ermittlungsmaßnahme geht. Folgerichtig bedarf es bei der Datenklassifizierung keiner Unterscheidung hinsichtlich der Verfahrensstellung des Grundrechtsträgers.

Schließlich kommt es für die Datenklassifizierung wegen des maßgeblichen Personenbezuges nicht darauf an, wer Zugang zu den Daten gewähren kann. Der jeweilige Grundrechtsschutz vor staatlicher Datenerlangung und -verwertung gilt im Verhältnis zum Grundrechtsträger unabhängig davon, ob sich die relevanten Daten bei ihm oder bei (irgend-)einem Dritten, sei es einer Privatperson oder einem Dienstleister, befinden.

Mit dieser Feststellung wird allerdings keine Aussage zu der Frage getroffen, ob und gegebenenfalls unter welchen Umständen der Grundrechtsträger oder ein Dritter zur Duldung oder aktiven Mitwirkung bei der Datenübermittlung an die Strafverfolgungsbehörde verpflichtet werden kann. Die Beantwortung dieser Frage hängt neben der allein grundrechtsträgerbezogenen Schutzwürdigkeit eines Datensatzes unter anderem auch davon ab, welche weiteren Rechte von einer konkreten Datenübermittlung tangiert sein können. Zu denken ist in diesem Zusammenhang insbesondere an das Grundrecht des Verdächtigen, sich nicht selbst belasten zu müssen. Hinsichtlich Dritter kommen vorrangig Persönlichkeitsrechte des Opfers und die Berufsausübungsfreiheit eines Dienstleisters in Frage; für einen Eingriff in diese Rechte ist eine gesonderte Eingriffsgrundlage erforderlich. Auch das Prinzip des Zeugnisverweigerungsrechts steht gesondert neben dem datenspezifischen Grundrechtsschutz des Betroffenen.

481 Vgl. etwa BVerfG, Beschluss vom 12.04.2005, 2 BvR 1027/02, zugleich BVerfGE 113, 29, Rn. 112 (zitiert nach juris).

cc) Unerheblichkeit des Datenzustands

Auch wenn generell unterstellt wird, dass gespeicherte Daten schutzwürdiger wären als solche, die zum Zeitpunkt der staatlichen Maßnahme übermittelt werden,[482] ist dies rechtsdogmatisch nicht zu begründen. Möglicherweise stammt die Vorstellung aus dem prä-digitalen Zeitalter, in dem das in ein Telefon gesprochene Wort flüchtig war und schriftliche („gespeicherte“) Aufzeichnungen jedenfalls bei verschlossenen Briefen eine erhöhte Vertraulichkeit indizierten. Der Kommunikationsteilnehmer konnte daher durch die Wahl des Kommunikationsmittels jedenfalls bedingt sein Geheimhaltungs-interesse nach außen zum Ausdruck bringen.

Das gilt bei modernen Kommunikationsmitteln nicht mehr, bei denen – siehe das zuvor erwähnte OSI-7-Schichten Modell – Sprach- und Schriftnachrichten einheitlich verarbeitet, übermittelt und gespeichert werden. Aus Sicht des Nutzers hängt es aufgrund der häufig unbemerkt und vielfältig stattfindenden Datenverarbeitungsprozesse bereits in einem einzelnen Gerät vom Zufall ab, welcher Datenzustand gerade besteht und ob bestimmte Datensätze wie beispielsweise vorhandene Kontaktdaten durch eine App momentan verarbeitet und an einen Dienstleister gesendet werden. Ganz offensichtlich wird diese vom Nutzer nicht zu beeinflussende Unsicherheit bei vielen Cloud-Diensten, bei denen aus Nutzersicht die Daten gespeichert werden, also „in rest“ sind, während der Dienstleister aus Sicherheitsgründen permanente, automatisierte Verschiebungen der Daten vornimmt, sodass sie regelmäßig „in transit“ von einem Server zum nächsten sind und damit nur als Echtzeitdaten erhoben werden können.

Durch die bereits erläuterte Entscheidung des Bundes-verfassungsgerichts zur Bestimmung des Datenzustandes bei der Speicherung von E-Mails beim Provider im IMAP-Verfahren[483] wird das maßgebliche Unterscheidungskriterium zudem von der technischen

482 Vgl. beispielsweise Gesetzesbegründung zur Neufassung der §§ 100a ff. StPO, BT-Ausschussdrucks. 18(6)334, S. 6.
483 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43.

Ebene auf die der „faktischen Herrschaft“ übertragen; darauf, ob die Daten tatsächlich ruhen oder nicht, soll es nach der zitierten Entscheidung für die Unterscheidung zwischen gespeicherten Daten und solchen im Übertragungsvorgang nicht mehr ankommen.

Aus den genannten Beispielen wird deutlich, dass der Nutzer in vielen Fällen bei elektronischen Daten weder Kenntnis über noch eine Einflussmöglichkeit auf den aktuellen Zustand seiner Daten hat. Dieser hängt häufig vom Zufall und / oder komplexen rechtlichen Würdigungen ab.

Dass verschiedene Grundrechte bei unterschiedlichen Datenzuständen zur Anwendung kommen, erlaubt lediglich die Schlussfolgerung, dass Daten in allen Zuständen grundrechtlich geschützt sind; eine Rangordnung kann daraus insbesondere unter Berücksichtigung der dargestellten Zufälligkeit nicht abgeleitet werden.

b) Abstrahierende Schlussfolgerungen

Im Folgenden werden die Kernsätze der erörterten datenspezifischen Grundrechte, die für die Bestimmung unterschiedlicher Eingriffsintensität relevant sind, analysiert und, soweit möglich, abstrahiert.

aa) Keine gesetzliche Vorgabe zur Sensibilität eines Datensatzes – subjektiver Maßstab

Für alle drei datenspezifischen Grundrechte wurde festgestellt, dass sich ihr jeweiliger Schutz auf alle personenbezogenen Daten unabhängig von ihrem Inhalt bezieht. Die Umstände einer Telekommunikation unterfallen ebenso wie der Kommunikationsinhalt dem Grundrechtsschutz, das Recht auf informationelle Selbstbestimmung ist nicht beschränkt auf Daten, die ihrer Art nach besonders sensibel sind, sondern bezieht auch Daten „mit nur geringem Informationsgehalt“ ein, und das Recht auf Vertraulichkeit und Integrität eines informationstechnischen Systems erfasst sämtliche Daten unabhängig von ihrem Inhalt und ihrer Wichtigkeit, unabhängig

davon, ob sie nur einen punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen aufweisen oder seine Privatsphäre tangieren.
Innerhalb der Gruppe der personenbezogenen Daten ist es grundsätzlich unerheblich, ob die Daten vom Betroffenen stammen oder sich inhaltlich auf ihn beziehen.
Zusammenfassend lässt sich schlussfolgern, dass die verfassungsrechtliche Ordnung keine Sensibilitätseinordnung für bestimmte Dateninhalte vorgibt.

Dort, wo es für das Maß der Grundrechtsschutzbetroffenheit auf die Sensibilität eines Datensatzes ankommt – namentlich beim Recht auf informationelle Selbstbestimmung und beim Kernbereichsschutz -, hängt ihre Bestimmung immer von den Umständen des Einzelfalles und damit maßgeblich davon ab, welche Bedeutung der Dateninhalt für den Betroffenen hat beziehungsweise welche Bedeutung er durch Einbeziehung in andere Zusammenhänge gewinnen kann. Der Maßstab der Datensensibilität ist also immer ein rein subjektiver.

bb) Verhalten des Datenberechtigten

Die verfassungsrechtlich verwendeten Begriffe „Geheimnis“, „Selbstbestimmung“ und „Vertraulichkeit“ weisen darauf hin, dass der Schutzbereich der Grundrechte und damit die Schutzwürdigkeit der ihm unterfallenden geschützten Objekte nicht nach rein objektiven Maßstäben bestimmt werden kann. Vielmehr liegt es subjektiv in der Hand des Grundrechtsträgers, ob sein Wissen, seine Meinung oder sein Werturteil als „geheim“ oder „vertraulich“ zu qualifizieren ist und wem er die faktische Herrschaft über die Daten einräumt.

Daraus und aus der Überlegung, dass die Grundrechte letztlich ebenso wie der Kernbereichsschutz der persönlichen Entfaltung dienen, lässt sich schlussfolgern, dass der Grundrechtsträger durch sein Verhalten den konkreten Umfang seines Grundrechtsschutzes selbst beeinflussen kann. Insbesondere schließt die Gewährung der persönlichen Entfaltung die Möglichkeit ein, ein Wissen, eine Meinung oder ein

Werturteil an Dritte weiterzugeben - oder auch nicht.

Bezogen auf personenbezogene Daten bedeutet dies, dass der Grad ihrer Weitergabe an Dritte durch den Betroffenen unmittelbaren Einfluss auf ihre grundrechtliche Schutzwürdigkeit haben kann. Dabei gibt es keine schwarz-weiß Abgrenzung zwischen „schutzwürdig“ und „nicht schutzwürdig“, sondern vielmehr einen fließenden Übergang. Es hängt maßgeblich vom erwarteten Verhalten des Dritten ab, inwieweit die Vertraulichkeit oder das Geheimnis durch den Berechtigten selbst bewusst aufgehoben werden.

Dem absolut geschützten Kernbereich der privaten Lebensgestaltung als einer Extremsituation, in der die Informationsweitergabe aus rechtlicher Sicht keine Aufhebung des Geheimnisses oder der Vertraulichkeit beinhaltet, steht die umgekehrte Extremsituation gegenüber, in der die Information wahllos an eine unbestimmte Vielzahl von Empfängern mitgeteilt wird. Wer letzteres tut, wird sich schwerlich darauf berufen können, dass es sich bei der mitgeteilten Information noch um ein Geheimnis oder etwas Vertrauliches handele.

Auch wenn die Abgrenzung im Einzelfall schwierig sein kann und von den konkreten Umständen abhängt, so hat sich zu Recht die Auffassung durchgesetzt, dass jedenfalls solche Daten, die, unabhängig von der Intimität oder ursprünglichen Bekanntheit ihres Inhaltes, vom Grundrechtsträger in freier Entscheidung jedermann oder zumindest einem nicht weiter individualisierbaren Personenkreis zugänglich gemacht werden, keinen besonderen Schutz vor staatlicher Kenntnisnahme genießen.[484]
Dabei ist es unerheblich, ob der Betroffene etwa durch Bereitstellung von Dateninhalten auf seinem Webserver technische Vorkehrungen dafür trifft, dass die Daten öffentlich zugänglich von jeglichem Dritten erhoben werden können,[485] oder ob er die Daten konkret an einen

484 Vgl. nur BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Leitsatz 5 und Rn. 308; Art. 10 lit. c) DS-Richtlinie Strafjustiz.
485 Vgl. nur BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 306 ff.

Empfänger sendet, dessen Identität ihm gleichgültig ist.[486] In beiden Fällen gibt der Betroffene, seine selbstbestimmte Entscheidung vorausgesetzt, durch sein Verhalten den entsprechenden Grundrechtsschutz auf.

Dies gilt entsprechend, wenn die Informationsweitergabe direkt an die Ermittlungsbehörde erfolgt, weil der Datenberechtigte dadurch zu erkennen gibt, dass er mit der Kenntnisnahme und Verwertung durch die staatlichen Stellen einverstanden ist. Vergleichbar mit der Beschuldigtenaussage setzt eine selbstbestimmte Entscheidung zur Preisgabe von Datensätzen allerdings voraus, dass der Betroffene zutreffend seine entsprechenden Rechte und Pflichten beurteilen kann und sich möglicher Konsequenzen bewusst ist; gegebenenfalls ist er entsprechend zu belehren. Es handelt sich insoweit aber nicht um ein spezifisches Problem elektronischer Daten.

cc) Berechtigte Erwartungshaltung der Vertraulichkeitswahrung

Während Art. 10 Abs. 1 GG keinen verfassungsrechtlichen Schutz hinsichtlich der Motivation und Redlichkeit des Kommunikationspartners gewährt, greift das Recht auf informationelle Selbstbestimmung dafür nur in besonders begründeten Ausnahmefällen, in denen von staatlicher Seite beim Absender eine konkrete, unzutreffende Vorstellung über die Identität und Motivation bewirkt wurde. Auch der Kernbereichsschutz stellt besondere Anforderungen an die Person des Informationsempfängers, die sich alleine aus seiner persönlichen Beziehung zum Datenberechtigten ergeben.
Umgekehrt ist unter Art. 10 Abs. 1 GG jedenfalls für den geschäftsmäßig tätigen Nachrichtenübermittler davon auszugehen, dass seine Einschaltung keine Zustimmung der Kommunikationspartner zur Kenntnisnahme des Kommunikationsinhaltes beinhaltet.

---

486 Das gilt nach BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 309, insbesondere in den Fällen, in denen sich eine staatliche Stelle unter einer Legende auf eine Kommunikation mit einem Grundrechtsträger einlässt, es sei denn, dass sie dabei ein schutzwürdiges Vertrauen des Betroffenen in ihre Identität und Motivation ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde.

Aus diesen Kernaussagen lässt sich zum einen schließen, dass der kommunizierende Datenberechtigte grundsätzlich selbst das Risiko trägt, wie sein Kommunikationspartner mit der erlangten Information umgeht. Das schließt insbesondere eine Weitergabe an Dritte ein, die der Datenberechtigte nicht mehr kontrollieren kann, sobald er die Information einmal herausgegeben hat.
Folgerichtig genießen Daten, auf die mit Zustimmung des Datenberechtigten öffentlich, also ohne jegliche Zugangsbeschränkung, zugegriffen werden kann, auch aus diesem Grund keinen datenspezifischen Schutz vor behördlicher Erlangung und Verwertung.

Nur in besonders begründeten Ausnahmefällen erkennt die Rechtsordnung den Schutz einer bestimmten Erwartungshaltung gegenüber dem Kommunikationspartner auf Einhaltung der Vertraulichkeit an. Solche Ausnahmefälle erfordern eine besondere Beziehung zwischen den Beteiligten, die sich aus der persönlichen Nähe oder einer entsprechenden vertraglichen Grundlage ergeben kann.
Die Schutzwürdigkeit steigt mit dem Grad des Vertrauens, den der Betroffene berechtigterweise dem Informationsempfänger entgegenbringen darf, wobei sich das Vertrauen gleichsam auf die Motivation als auch die Identität des Gegenübers bezieht. Als Extrempole stehen sich dabei persönlich nicht bekannte, anonyme Adressaten und höchstpersönliche, natürliche Vertrauenspersonen gegenüber. Die konkrete Feststellung der berechtigten Erwartungshaltung richtet sich nach den Umständen des Einzelfalles, wobei folgende – nicht abschließende - Überlegungen eine Rolle spielen können:

Je geringer die Anzahl der Datenempfänger, desto eher besteht die Möglichkeit eines besonders schützenswerten Vertrauensverhältnisses.

Ein besonderes Vertrauensverhältnis, von dem auf eine berechtigte Erwartungshaltung zu schließen ist, kann potentiell sowohl im Hinblick auf natürliche Personen als auch auf juristischen Personen (etwa eine Bank, eine Anwaltskanzlei oder eine Gemeinschaftspraxis) angenommen werden. Bei natürlichen Personen ist der mögliche

Adressatenkreis nicht auf zeugnisverweigerungsberechtigte Personen beschränkt, sondern schließt auch besonders nahestehende Dritte und enge Freunde ein.[487] Umgekehrt besteht nicht in jedem Fall per se ein besonderes Vertrauensverhältnis zu allen im konkreten Fall zeugnisverweigerungsberechtigten Personen. Handelt es sich, wie häufig in Bezug auf eine juristische Person, um einen geschäftlichen Kontakt, dürfte der zugrundeliegenden vertraglichen Ausgestaltung maßgebliches Gewicht für die Bewertung eines besonderen Vertrauens zukommen.

Schließlich ist die Überprüfung der Motivation und der Identität des Gegenübers nach höchstrichterlicher Rechtsprechung als ein weiteres mögliches Kriterium für die Annahme eines besonderen Vertrauens-verhältnisses zu berücksichtigen.[488] Fehlt eine entsprechende Möglichkeit oder wird sie vom Betroffenen nicht wahrgenommen, spricht dies gegen ein solches.

Daneben gibt es Standardsituationen, wie etwa bei der Einschaltung eines Kommunikationsdienstleisters, für die aufgrund der Bedeutung solcher Dienste und der strengen gesetzlichen Reglementierungen, denen ihre vertragliche Ausgestaltung unterliegt, die Wahrung der Vertraulichkeit des zu übermittelnden Nachrichteninhaltes als berechtigte Erwartungshaltung rechtlich anerkannt ist. Dass eine entsprechende Erwartungshaltung rechtlich anerkannt ist, spiegelt sich unter anderem in § 206 StGB, der eine Verletzung des Post- oder Fernmeldegeheimnisses unter Strafe stellt, wider.

Der Ansatz der berechtigten Erwartungshaltung spiegelt sich schließlich auch in der Anwendbarkeitsvoraussetzung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme wider, wonach der Schutzbereich nur dann eröffnet ist, wenn der Nutzer berechtigterweise davon ausgehen darf, das System als eigenes, also gegenüber Dritten zugangsbeschränkt, zu nutzen.

---

487 BVerfG, Urteil vom 20.04.2016, 1 BvR 966/09 und 1 BvR 1140/09, zugleich BVerfGE 141, 220, Rn. 121, m.w.N.

488 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 311.

Zusammenfassend lässt sich festhalten, dass die berechtigte Erwartungshaltung der Vertraulichkeitswahrung das maßgebliche Kriterium zur Bestimmung der Sensibilität eines Datensatzes und damit für die Grundrechtsschutzbetroffenheit einer entsprechenden Eingriffsmaßnahme darstellt.[489] Ob eine bestimmte Erwartungshandlung als berechtigt zu qualifizieren ist, hängt wesentlich vom Verhalten des Datenberechtigten und seinem Verhältnis zum Kommunikationspartner ab.

c) Konkrete Zusammenführung der erarbeiteten Kriterien

Nicht-personenbezogene Daten genießen keinen besonderen verfassungsrechtlichen Schutz. Sie sind ohne weitere Voraussetzungen für die Strafverfolgungsbehörden zugänglich und verwertbar.

Personenbezogene Daten können direkt oder mittelbar dem Grundrechtsträger zuzurechnen sein. Für ihre grundrechtliche Schutzwürdigkeit und damit ihre strafprozessuale Zugänglichkeit und Verwertbarkeit gilt Folgendes:

Die subjektive Bedeutungszumessung und die berechtigte Erwartungshaltung des Betroffenen bestimmen die Sensibilität eines Datensatzes, nicht sein objektiver Inhalt. An dieser Stelle liegt der dogmatische Bruch der herkömmlichen Klassifizierung der Kommunikationsdaten, weil sie unterstellt, dass Verkehrsdaten allgemein weniger sensibel und damit weniger schutzwürdig wären als Kommunikationsinhaltsdaten. Dies kann aus Sicht des Grundrechtsträgers aber ganz anders sein und, wie gezeigt, beim heutigen Kommunikationsverhalten nicht mehr generell unterstellt werden. Gesellschaftliche Wertungen, wie sie sich beispielsweise in den besonderen Kategorien des Datenschutzrechts niederschlagen, haben für die Bestimmung der Sensibilität eines

489 Zur Bedeutung der berechtigten Erwartungshaltung als einem wichtigen Faktor bei der Frage, ob eine Maßnahme das Privatleben beziehungsweise die Korrespondenzfreiheit aus Art. 8 EMRK betrifft, vgl. EGMR, Urteil vom 05.09.2017 („Bărbulesu v. Romania“), appl. no. 61496/08, Rn. 73, m.w.N.: „a reasonable expectation of privacy is a significant though not necessarily conclusive factor“; zuletzt auch EGMR, Urteil vom 24.04.2018 („Benedik v. Slovenia“), appl. no. 62357/14, Rn. 115 ff.

Datensatzes höchstens eine Indizwirkung, sind aber keinesfalls ausschlaggebend. Der Betroffene entscheidet selbstbestimmt darüber, welche seiner Daten als höchstpersönlich-intim, privat, beschränkt oder unbeschränkt für Dritte zugänglich sein sollen.

Seine Festlegung, die, je öffentlicher eine Information verbreitet wird, umso irreversibler ist, manifestiert sich im Umfang der selbstbestimmten Verbreitung: je weiter ein Datensatz an Dritte verteilt wird und je weniger die Zuverlässigkeit des Empfängers im Hinblick auf den Umgang mit der Information beurteilt werden kann, desto weniger kann der Betroffene berechtigterweise davon ausgehen, dass seine Information geheim und vertraulich bleibt, und desto weniger verfügt er im Weiteren selbstbestimmt darüber. Entsprechend sinkt die datenspezifische grundrechtliche Schutzwürdigkeit.
In allen Fällen der Datenweitergabe trägt grundsätzlich allein der Datenberechtigte das Risiko des Vertraulichkeitsbruches durch den Informationsempfänger.

Daher genießen Datensätze, die der Datenberechtigte selbstbestimmt öffentlich zugänglich macht, keinen besonderen Grundrechtsschutz. Dies hat zur Folge, dass die Kenntnisnahme und Verwertung der so verbreiteten Daten durch staatliche Stellen grundsätzlich keiner gesonderten Ermächtigungsgrundlage bedarf, auch wenn es sich um personenbezogene Daten handelt.[490]
Dies gilt entsprechend für die selbstbestimmte, freiwillige Preisgabe einer Information an die Strafverfolgungsbehörde durch den Datenberechtigten, der mit der Preisgabe den Geheimnis- und Vertraulichkeitsschutz gegenüber der staatlichen Stelle aufhebt.
Erfolgt die Informationsübermittlung ohne behördliche Veranlassung durch einen Dritten, der berechtigt Zugang zu den Daten hat, so entfällt der besondere Grundrechtsschutz des Datenberechtigten ebenfalls, weil die Informationsweitergabe genau das Risiko verwirklicht, das der Datenberechtigte mit der Preisgabe beziehungsweise mit der Zugangsmöglichkeit für den Dritten eingegangen ist und

490 Vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 308 ff.; Sieber, *Gutachten zum 69. DJT*, S. 125.

das er selbst trägt. Dies gilt jedenfalls dann, wenn die Informationsübermittlung rechtmäßig, das heißt weder vertrags- noch gesetzeswidrig erfolgt.

Ein Minimum an verfassungsrechtlichem Schutz erfahren solche Daten, die der Datenberechtigte einem nur begrenzten Empfängerkreis mitteilt, ohne dass er dessen Identität und Motivation näher prüft oder näher prüfen kann.
Die vom Grundrechtsträger eingeräumte beschränkte Zugänglichkeit der Daten erlaubt eine berechtigte Erwartungshaltung allerdings in nur sehr beschränktem Maße im Hinblick darauf, dass die Informationen trotz der Weitergabe weiterhin geheim und vertraulich bleiben. Die beschränkte rechtliche Anerkennung einer bestimmten Erwartungshaltung führt dazu, dass die strafprozessuale Erlangung und Verwertung solcher Daten an ein Mindestmaß an gesetzlichen Voraussetzungen zu binden ist.

Sensibler und damit rechtlich schutzwürdiger sind Daten zu qualifizieren, die ausschließlich an solche Personen bekannt gegeben werden, in deren Identität und Motivation der Datenberechtigte ein berechtigtes Vertrauen setzt. Dies kann durch persönliche Beziehungen und, insbesondere bei juristischen Personen, durch entsprechende vertragliche Ausgestaltungen begründet werden. Mit der Anerkennung des berechtigten Vertrauens wird dem Umstand Rechnung getragen, dass mit ihm ein signifikant reduziertes Risiko des Geheimnisverrates und des Vertraulichkeitsbruches einhergeht.
Für die Zulässigkeit der Erlangung und Verwertung entsprechender Daten durch die Strafverfolgungsbehörden sind daher höhere Anforderungen zu stellen, als für diejenigen der zuvor beschriebenen Gruppe.

Die nächsthöhere Stufe erfasst solche Daten, die der Grundrechtsträger erst gar nicht an Dritte weitergibt, wodurch das Risiko des Geheimnisverrates und des Vertraulichkeitsbruches ausgeschlossen wird. Der Begriff der Weitergabe meint die Informationsübermittlung zur Kenntnisnahme, sodass ein Nachrichteninhalt, der an

einen Telekommunikationsdienstleister zur technischen Übermittlung etwa in den Cloud-Speicher überlassen wird, weiterhin als „nicht weitergegeben“ zu qualifizieren ist.
An die Erlangung und Verwertung solcher Daten durch die Strafverfolgungsbehörden sind die strengsten Bedingungen zu knüpfen, unabhängig davon, wo sich die Daten konkret befinden.

Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, die also vom Grundrechtsträger als höchstpersönlich-intim betrachtet und, wenn überhaupt, nur an einzelne, ausgewählte Personen des höchstpersönlichen Vertrauens weitergegeben werden, genießen einen absoluten Erhebungs- und Verwertungsschutz.

3. Anwendung der erarbeiteten Kriterien und tabellarische Übersicht

Die Anwendung der entwickelten Kriterien führt unter Beachtung der dargestellten Prämissen zu folgender Kategorisierung elektronischer Beweismittel:

a) Kernbereich privater Lebensgestaltung

Unantastbar und mit dem höchsten Grad an Schutzwürdigkeit sind Daten zu bewerten, die den Kernbereich privater Lebensgestaltung betreffen.

b) Geheime Daten

Außerhalb dieses Bereiches genießen solche personenbezogenen Daten einen größtmöglichen Schutz, die nach dem Willen des Grundrechtsträgers nicht für Dritte zugänglich sein sollen. Sie werden als geheime Daten bezeichnet. Sie umfassen beispielsweise unabhängig von ihrem Inhalt alle nur lokal auf den Geräten des Betroffenen gespeicherten Daten sowie Inhalte, die lediglich zur Speicherung auf einen Cloudserver übertragen werden.

c) Vertrauliche Daten

Eine etwas abgestufte Schutzwürdigkeit betrifft vertrauliche Daten, die, ohne Kernbereichsdaten zu sein, ausschließlich solchen Personen mitgeteilt werden, in deren Motivation und Identität der Absender ein berechtigtes, besonders schutzwürdiges Vertrauen setzt.

d) Beschränkt zugängliche Daten

Dahinter sind beschränkt zugängliche Daten zu nennen, die sich von den vertraulichen Daten durch das fehlende besonders schutzwürdige Vertrauen in die Motivation und Identität des Empfängers unterscheiden. Sie schließen neben herkömmlichen Kommunikations-inhaltsdaten insbesondere solche Daten ein, die aufgrund der gewählten Übermittlungsart notwendig an den oder die daran beteiligten Dienstleister mitzuteilen sind oder in unmittelbarem Zusammenhang damit entstehen.

e) Unbeschränkt zugängliche Daten

Aus Sicht der Strafverfolgungsbehörden unbeschränkt zugängliche Daten schließlich genießen keinen besonderen datenspezifischen Grundrechtsschutz und betreffen neben nicht-personenbezogenen und personenbezogenen öffentlich zugänglichen Daten auch solche, die vom Grundrechtsträger oder Dritten, die berechtigt Zugang zu den Daten haben, selbstbestimmt und rechtmäßig an die Strafverfolgungsbehörde mitgeteilt werden.

Tabellarische Übersicht

Kernbereichsdaten	Daten, die den Kernbereich privater Lebensgestaltung betreffen
Geheime Daten (ohne Kernbereichsdaten)	• personenbezogen • nach dem Willen des Betroffenen nicht für Dritte zugänglich
Vertrauliche Daten (ohne Kernbereichsdaten)	• personenbezogen • mitgeteilt an individuelle(n) Dritte(n) • besonders schutzwürdiges Vertrauen in die Motivation und Identität des Empfängers
Beschränkt zugängliche Daten (ohne Kernbereichsdaten)	• personenbezogen • mitgeteilt an individuelle(n) Dritte(n)
Unbeschränkt zugängliche Daten	Alternative Voraussetzungen: • nicht-personenbezogen • öffentlich zugänglich • selbstbestimmte, freiwillige Mitteilung des Datenberechtigten an die Strafverfolgungsbehörde • rechtmäßige Preisgabe durch Dritten

V. Abstrakte Gegenüberstellung der herkömmlichen und der neuen Klassifizierung

1. Erfassung sämtlicher Datensätze

Ein herausragendes Merkmal der Neuklassifikation im Vergleich zur herkömmlichen ist ihr holistischer Ansatz, der die Erfassung sämtlicher Datensätze erlaubt. Anders als bei der bisherigen Einteilung stellen sich daher beispielsweise keine Probleme mit dem Kommunikationsbegriff, mit der Eigennutzung von Cloud-Diensten oder mit Datensätzen, die im Rahmen des Internets der Dinge anfallen.

2. Entwicklung der Klassifizierung in Fortführung der Rechtsprechung des Bundesverfassungsgerichts

Ein weiterer wesentlicher Unterschied liegt in ihrer Herleitung und den sich daraus ergebenden Konsequenzen. Die Herleitung des vorgestellten Kategorisierungsmodells erfolgt rein dogmatisch und führt strenggenommen nur die Aussagen des Bundesverfassungsgerichts zur Schutzwürdigkeit einzelner Datensätze, die jeweils dem äußersten Sensibilitätsspektrum entstammen, konsequent für den Zwischenbereich fort. Sie ist deshalb auf die konkreten strafprozessualen Fragestellungen abgestimmt und richtet sich nicht nach den Bedürfnissen außenstehender Dritter (namentlich der Telekommunikationsdienstleister).

3. Technikunabhängigkeit der Neuklassifizierung

Aufgrund der dogmatischen Herleitung ist die hier vorgeschlagene Klassifizierung technikunabhängig. Die Unabhängigkeit von der zukünftigen Entwicklung in der Informationstechnik und damit zusammenhängender Dienstleistungsmodelle gewährleistet in zeitlicher Hinsicht eine Stabilität, die die herkömmliche dienstleistungsorientierte Katalogauflistung nicht leisten kann.

4. Verzicht auf eine Unterscheidung nach den Dienstleistern

Die einheitliche Entwicklung des neuen Modells und seine grundsätzliche Anwendbarkeit auf jeden Dateninhaber macht die Unterscheidung zwischen TKG- und TMG-Dienstleistern obsolet und vermeidet dadurch Unstimmigkeiten, wie sie derzeit bestehen.

5. Verzicht auf eine Katalogauflistung

Durch den Verzicht auf die Einzelauflistung verschiedener Datensätze, wie sie derzeit über die Verweise auf das TKG für Kommunikationsdaten vorgenommen wird, ergibt sich insoweit eine Erleichterung bei der praktischen Anwendung, als sämtliche Verkehrsdaten und regelmäßig alle Bestandsdaten unabhängig vom Dienstleister einheitlich der Kategorie der beschränkt zugänglichen Daten unterfallen. Diese Kategorie kann zudem in Abhängigkeit vom Informationsempfänger auch klassische Kommunikationsinhaltsdaten erfassen. Damit wird dem Umstand Rechnung getragen, dass heutzutage Kommunikationsinhaltsdaten nicht mehr per se als schutzwürdiger im Vergleich zu Kommunikationsmetadaten einzuordnen sind.

6. Klassifizierung nach dem Datenberechtigten

Hinsichtlich der Kommunikationsinhaltsdaten bietet die Neuklassifikation einen differenzierteren Ansatz als die herkömmliche Einteilung, indem sie den Bereich zwischen Kernbereichsdaten und öffentlich zugänglichen Daten dreifach untergliedert. Für diese Untergliederung wird maßgeblich auf den Datenberechtigten abgestellt – alleine auf sein Verhalten und sein Verhältnis zum Kommunikationspartner kommt es an -, sodass die grundrechtlich vorgegebenen Begriffe des Geheimnisses, der Selbstbestimmung und der Vertraulichkeit klarer berücksichtigt werden. Dadurch, dass diese Begriffe mit dem Umfang der Datenweitergabe und dem persönlichen Verhältnis zum Datenempfänger verknüpft werden, kommen objektive Abgrenzungskriterien zur Anwendung, die eine praktikable Handhabung ermöglichen.

VI. Ausgewählte Beispiele der Zuordnung im neuen und im herkömmlichen Klassifikationsmodell

Die folgende konkrete Gegenüberstellung dient zum einen dem besseren Verständnis der vorgeschlagenen Einteilung. Zum andern soll sie Gemeinsamkeiten und Unterschiede der Klassifikationsmodelle verdeutlichen und dadurch letztlich auch den Nutzen der Neuklassifizierung untermauern. Kernbereichsdaten werden nicht erwähnt, weil es diesbezüglich keine Unterschiede gibt. Zur besseren Lesbarkeit werden für die neuen Kategorien folgende Bezeichnungen verwendet:

Kat. I: Kernbereichsdaten
Kat. II: Geheime Daten
Kat. III: Vertrauliche Daten
Kat. IV: Beschränkt zugängliche Daten
Kat. V: Unbeschränkt zugängliche Daten

Datenart	Einordnung im neuen Modell	Erfassung in der StPO
Mitgeteilter Name des Telefonnutzers	Kat. IV	§ 100j StPO („Bestandsdaten“)
Mitgeteilter Name des Social Media - Nutzers	Kat. IV	nicht erfasst
Echtzeit-Verbindungsdaten elektronischer Kommunikation	Je Einzelfall: Kat. IV, V	§ 100a StPO
Beim Provider gespeicherte Verbindungsdaten des Telefon- / Mobilfunknutzers	Kat. IV	§ 100g StPO („Verkehrsdaten“)
Beim Provider gespeicherte Verbindungsdaten des E-Mail-Nutzers	Kat. IV	§§ 94 f. StPO *
Beim Provider gespeicherte Verbindungsdaten des Social Media - Nutzers	Kat. IV	nicht erfasst

Beim Nutzer gespeicherte Verbindungsdaten elektronischer Kommunikation	Kat. IV	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Echtzeit-Signalisierungsdaten	Kat. IV	§ 100g Abs. 1 S. 3 StPO („Verkehrsdaten“)
Beim Provider gespeicherte Signalisierungsdaten	Kat. IV	nicht erfasst
International Mobile Equipment Identity (IMEI, zur eindeutigen Geräteidentifizierung)	Kat. IV	§ 100g StPO („Verkehrsdaten“)
International Mobile Subscriber Identity (IMSI, zur eindeutigen Teilnehmeridentifizierung)	Kat. IV	§ 100g StPO („Verkehrsdaten“)
Personal Unblocking Key (PUK, zur lokalen Entsperrung der SIM-Karte)	Kat. II	§ 100j Abs. 1 S. 2 StPO („Bestandsdaten“)
Inhaltsdaten ausschließlich zur Speicherung (lokal oder in der Cloud)	Kat. II	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Echtzeit-Nachrichteninhalt für individuelle(n) Empfänger	Je Einzelfall: Kat. III, IV	§ 100a StPO
Beim Provider gespeicherter Nachrichteninhalt für individuelle(n) Empfänger	Je Einzelfall: Kat. III, IV	§§ 94 f. StPO *
Beim Nutzer gespeicherter Nachrichteninhalt für individuelle(n) Empfänger	Je Einzelfall: Kat. III, IV	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Echtzeit-Posting-Inhalt an offene Gruppe	Kat. V	§ 100a StPO (Erlangung während des Datentransfers) **
Beim Provider gespeicherter Posting-Inhalt an offene Gruppe	Kat. V	§§ 94 f. StPO *
Beim Nutzer gespeicherter Posting-Inhalt an offene Gruppe	Kat. V	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)

Inhaltsdaten Fitnessband zur ausschließlichen Speicherung (lokal oder in der Cloud)	Kat. II	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Inhaltsdaten Fitnessband zur Auswertung an Hausarzt	Kat. III	§§ 94 f., 97 StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Inhaltsdaten Fitnessband zur Auswertung durch App-Provider	Kat. IV	§§ 94 f. StPO * (offene Maßnahme), § 100b StPO (verdeckte Maßnahme)
Inhaltsdaten Fitnessband auf frei zugänglicher Website	Kat. V	**

* Das Bundesverfassungsgericht hält die §§ 94 f. StPO in Bezug auf die Sicherung und Beschlagnahme elektronischer Daten auf jeden Dateninhaber für anwendbar, wenn

- die Maßnahme offen und nicht heimlich erfolgt,
- die Daten nur punktuell und auf den Ermittlungszweck begrenzt erhoben werden,
- es sich um Daten außerhalb eines laufenden Kommunikations-vorganges handelt und
- der Betroffene eine Einwirkungsmöglichkeit auf den Datenbestand hat.[491]

** Bei Zugriff nach Beendigung des Datentransfers, wenn die Daten unbeschränkt zugänglich sind: keine gesonderte Regelung in der StPO; nach h.M: Rückgriff auf § 161 StPO.

491 Vgl. BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 75, für gespeicherte E-Mails auf dem Server des Providers; BVerfG, Urteil vom 02.03.2006, 2 BvR 2099/04, zugleich BVerfGE 115, 166, Rn. 94 ff., für jegliche Daten, die beim Endnutzer gespeichert sind.

E. Kohärenz der neuen Klassifikation elektronischer Daten mit bestehenden Klassifikationen analoger Daten

Im Folgenden wird dargestellt, was elektronische von analogen Daten unterscheidet (dazu unter I.) und wie analoge Daten in der StPO kategorisiert werden (II.). Abschließend wird erläutert, in welchem Verhältnis die Analog-Kategorien zu den für die elektronischen Beweismittel herausgearbeiteten stehen (III.).

I. Unterscheidung zwischen elektronischen und analogen Daten

Der Schwerpunkt der bisherigen Ausführungen liegt bei elektronischen Daten, die verstanden werden als „jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form“.[492] Analoge Daten bedeutet damit jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem ungeeigneten Form – kurzum alles, woraus in der realen Welt (im Unterschied zur virtuellen Welt) Informationen gewonnen werden können.

Das Strafprozessrecht kennt zwei analoge primäre Informationsquellen: Personen und Gegenstände.
Aus beiden können verfahrensrelevante Hinweise gewonnen werden. Die Informationen werden durch die Vernehmung der Person, die Beschuldigter, Zeuge oder Sachverständiger sein kann, und die Inaugenscheinnahme des Objektes (mit der Verlesung eines Schriftstückes als besonderem Fall der Inaugenscheinnahme) erlangt. Gegebenenfalls bedarf es zur Interpretation und zur richtigen Schlussfolgerung aus den erlangten Informationen, den Anknüpfungstatsachen, besonderer Sachkenntnis, die im Bedarfsfall auf Sekundärebene durch Sachverständige zur Verfügung gestellt wird.

492 Definition aus Teil A III, Begrenzung des Untersuchungsgegenstandes.

II. Strafprozessuale Kategorisierung analoger Daten und die zugrundeliegenden verfassungsrechtlichen Wertungen

Bereits zu Anfang dieser Arbeit wurde herausgestellt, dass die strafprozessualen Normierungen die gegenständlichen Beweismittel in unterschiedlichen Gruppen zusammenfassen. Das gilt auch hinsichtlich der personenbezogenen Beweismittel. Die Differenzierung dient in allen Fällen dazu, wesentlich Gleiches von wesentlich Ungleichem zu trennen. Allerdings fehlt es in der StPO an einer systematischen Nennung der Unterscheidungskriterien und der einzelnen Kategorien; beides ergibt sich nur indirekt aus den verschiedenen Normierungen, aus denen die Eingriffsbefugnisse abgeleitet werden.

1. Unterschiedliche Personen-Klassen

Abhängig von der Verfahrensstellung differenziert die StPO zwischen dem Verdächtigen / Beschuldigten, dem Zeugen und dem Sachverständigen, wobei der Verdächtige / Beschuldigte insbesondere wegen des nemo-tenetur Grundsatzes eine sehr spezifische Rolle als Beweismittel spielt. Zu einer aktiven Mitwirkung an der Wahrheitserforschung ist er nicht verpflichtet. Die dem gegenüberstehenden Kategorien des Zeugen einerseits und des Sachverständigen andererseits erfahren gemäß § 76 StPO eine weitgehend identische Behandlung.

Eine detailliertere und weitaus wichtigere Unterscheidung des personenbezogenen Beweismittels Zeuge / Sachverständiger trifft das Gesetz anhand des Kriteriums des jeweiligen persönlichen Verhältnisses zum Beschuldigten:[493]

§ 48 Abs. 1 S. 2 StPO schreibt eine grundsätzlich umfassende Aussagepflicht vor, die über § 70 StPO mit Ordnungsmitteln erzwungen werden kann. Die generelle Aussagepflicht stellt mithin den Regelfall dar, der gilt, wenn keine der beiden fallunabhängigen Ausnahmesituationen vorliegen.

493 Die folgenden Ausführungen beziehen sich auf den Zeugen und gelten gemäß § 76 Abs. 1 StPO entsprechend für den Sachverständigen.

Die erste Ausnahmesituation wird in § 52 StPO angesprochen, der näher definierten Angehörigen des Beschuldigten ein Zeugnis- beziehungsweise Gutachtenverweigerungsrecht einräumt.

Daneben gewähren §§ 53 f. StPO den Berufsgeheimnisträgern und ihren Gehilfen ein Zeugnis- beziehungsweise Gutachtenverweigerungsrecht, sofern nicht der Betroffene die Verschwiegenheitsverpflichtung aufgehoben hat.

Ohne auf die Genese und Begründung der jeweiligen Normen im Einzelnen eingehen zu wollen, ergibt sich aus den genannten Regelungen eine Werteordnung des Gesetzgebers, wonach der „normale“ Zeuge / Sachverständige generell zur Auskunft verpflichtet ist, während bei Angehörigen ein besonders schützenswertes Näheverhältnis angenommen wird und geheime Informationen, die nur dem Betroffenen und seinem Berufsgeheimnisträger (beziehungsweise dessen Gehilfen) bekannt sind, nach der Rechtsordnung grundsätzlich geheim bleiben dürfen, sofern der Datenberechtigte dies wünscht.

2. Unterschiedliche Klassen von Gegenständen

Ähnlich wie beim Zeugen gelten für alle Gegenstände, die keiner spezialgesetzlichen Regelung unterliegen, die Generalklauseln der §§ 94 f StPO, die eine verhältnismäßig einfache Erlangung und Verwertung des Beweismittels erlauben. Objektbezogen differenziert die StPO allerdings in vielfältiger Weise und im Wesentlichen mit folgenden Spezialvorschriften:

§§ 81a ff. StPO betreffen Informationen, die aus der Betrachtung und Untersuchung des menschlichen Körpers erlangt werden können. Geregelt werden die unterschiedlich strengen Voraussetzungen für die Tatsachenerlangung und -verwertung durch die Erfassung und Auswertung von Körpermerkmalen, Blutproben und sonstiger Körperzellen.
Offensichtlich spielen hier das Recht auf körperliche Unversehrtheit aus

Art. 2 Abs. 2 GG und die unmittelbare Verknüpfung des Körpers mit der individuellen Persönlichkeit, die es zu schützen gilt, eine erhebliche Rolle bei der Frage, was als wesentlich gleich beziehungsweise wesentlich ungleich zu qualifizieren ist. Daneben kommt aber auch zum Tragen, wie offensichtlich oder äußerlich wahrnehmbar die jeweiligen Informationen sind und wieviel Einfluss der Betroffene auf das jeweilige Merkmal hat.

Die nächste Differenzierung innerhalb der gegenständlichen Beweismittel betrifft die Gruppe der Schriftstücke, für deren Erlangung wie folgt unterschieden wird:
§ 96 StPO erkennt als besonders regelungsbedürftige Gruppe amtlich verwahrte Schriftstücke an und verlangt bestimmte Zustimmungserfordernisse für die Erhebung der den Schriftstücken innewohnenden Informationen.
§ 97 Abs. 1 StPO normiert ein weitreichendes Beschlagnahmeverbot für schriftliche Korrespondenz zwischen dem Beschuldigten und den nach §§ 52 f. StPO zeugnisverweigerungsberechtigten Personen sowie für Aufzeichnungen und Ähnliches der Berufsgeheimnisträger und ihrer Gehilfen.
§§ 99 f. StPO hingegen erlaubt die Beschlagnahme von Postsendungen und Telegrammen an oder von sonstigen Personen grundsätzlich, stellt aber im Vergleich zur allgemeinen Beschlagnahme erhöhte formelle Anforderungen an die Datenerhebung.
Mit Ausnahme der amtlich verwahrten Schriftstücke als speziellem Sonderfall entspricht die Einteilung ganz eng den Wertungen, die für Zeugen Anwendung finden, und berücksichtigt zudem das grundrechtliche Brief- und Postgeheimnis aus Art. 10 GG.

Unterschiedliche Orte, in denen sich verfahrensrelevante Hinweise befinden können, werden geregelt in
§§ 100c, 102 f. StPO mit Wohnungen und sonstigen Räumen des Beschuldigten und Dritter,
§§ 100f und 100h StPO, die sich auf Orte „außerhalb von Wohnungen“ beziehen, und
§ 104 StPO, der im Hinblick auf nächtliche Durchsuchungen

Wohnungen, Geschäftsräume und das befriedete Besitztum als wesentlich Gleiches qualifiziert und dieser Gruppe „Räume, die zur Nachtzeit jedermann zugänglich sind“ oder die der Polizei als kriminelle Schlupfwinkel für Personen und Sachen bekannt sind, als ihrerseits wesentlich Gleiches gegenüberstellt.

Für die getroffene Unterscheidung kommt speziell der besondere grundrechtliche Schutz der Wohnung (im weiten Sinne) zum Tragen, aber auch der Ansatz, dass derjenige, der seine Räume zur Nachtzeit öffentlich zugänglich macht, keine berechtigte Schutzerwartung mehr haben kann. Und wer den räumlichen Schutzbereich in kriminell relevanter Weise nutzt, verliert nach der Wertung des Gesetzgebers vollständig den speziellen Grundrechtsschutz des Art. 13 GG.

Ein weiteres, sehr spezielles wesentlich ungleiches Einzelobjekt nennt § 108 StPO, der sich auf Gegenstände, die den Schwangerschaftsabbruch einer Patientin betreffen, bezieht. Dies ist § 218 StGB geschuldet.

Abschließend sei erwähnt, dass die StPO auch nach dinglichen Trägern elektronischer Daten differenziert, etwa in § 98b StPO („Datenträger“ zur Datenübermittlung), § 100a f. StPO („informationstechnisches System“), § 100i StPO („Mobilfunkendgeräte“) und § 110 Abs. 3 StPO („elektronisches Speichermedium“).
Während bei §§ 98b und 110 Abs. 3 StPO erkennbar ist, dass die relevante Informationsdarstellung in den elektronischen Daten an sich liegt und der Gegenstand nur der physikalische Ablageort ist, verwischen die §§ 100a f. und 100i StPO diese Trennung: soweit es nicht um die Inaugenscheinnahme des informationstechnischen Systems oder des Mobilfunkendgerätes geht, sind die Beweismittel nicht die dinglichen Geräte, sondern die dort gespeicherten Daten. Die Regelungen der §§ 100a f., 100i StPO beziehen sich also tatsächlich auf unterschiedliche Gruppen elektronischer Daten und nicht auf analog erhältliche Informationen.

III. Verhältnis der Kategorisierungen zueinander

Zunächst ist festzustellen, dass jegliche Kategorisierung von Beweismitteln in der StPO ganz im Sinne der modernen Gesetzgebungslehre dazu dient, Fallgruppen zu bilden, durch die wesentlich Gleiches zusammengefasst und einheitlich anders als wesentlich Ungleiches geregelt wird.
Informationen, die den Kernbereich der privaten Lebensgestaltung betreffen, genießen einen absoluten Schutz und dürfen unabhängig vom zur Verfügung stehenden Beweismittel nicht erhoben und verwertet werden.

An den Gruppen der biometrischen Daten, der unterschiedlich geregelten Orte und der Postsendungen zeigt sich besonders deutlich, welchen Einfluss die einschlägigen Grundrechte auf die Klassifizierung haben; die genannten Beweismittelkategorien sind unbestreitbar wesentlich von Art. 2 Abs. 2, 13 Abs. 1 und 10 Abs. 1 GG geprägt.

Daneben zeigt sich klassenübergreifend eine gewisse Grundaussage, die mit dem Selbstbestimmungsrecht zusammenhängt: Wer personenbezogene Informationen dadurch nach außen trägt, dass er sie durch Handlungen in der Öffentlichkeit, durch Mitteilungen an Dritte oder durch unbeschränkten Zugang zu bestimmten Orten offenbart, genießt hinsichtlich der betroffenen Daten einen geringeren grundrechtlichen Schutz als für solche Informationen, die überhaupt nicht weitergegeben werden.

Wie hoch der verbleibende Schutz ist, richtet sich vornehmlich nach dem persönlichen Verhältnis des Betroffenen zu demjenigen, dem die Information zugänglich gemacht wird: die geringste Schutzwürdigkeit wird dort angenommen, wo die Information öffentlich zugänglich ist.
Wer per Post mit einer konkreten Person kommuniziert, ist im Vergleich dazu schutzwürdiger. Der Austausch mit Personen, zu denen ein besonderes Näheverhältnis besteht (beziehungsweise vom Gesetz ohne Prüfung des Einzelfalles unterstellt wird), erfährt zusätzlichen Schutz und erreicht sein relatives Maximum, wenn sich das besondere

Näheverhältnis aus der Beziehung zu einem Berufsgeheimnisträger ergibt.

Diese Staffelung wird besonders deutlich bei den Regelungen für Zeugen und für Schriftstücke; die Parallelen zur vorgeschlagenen Kategorisierung der elektronischen Daten sind unübersehbar. Das liegt vor allem daran, dass bei diesen Beweismitteln mit dem Recht auf informationelle Selbstbestimmung und demjenigen aus Art. 10 Abs. 1 GG dieselben spezifischen Grundrechte die Hauptrolle für die Bestimmung des wesentlich Gleichen spielen und der verfassungsrechtliche Wert des Vertraulichkeitsschutzes jeweils stark zur Geltung kommt.

Dass die bereits in der StPO angelegten Klassifizierungen nicht eins-zu-eins auf elektronische Daten übertragen werden können, liegt zum einen daran, dass es, wie gezeigt, bislang keine systematische Sortierung mit eindeutiger Begriffsverwendung gibt.
Zudem fehlt elektronischer Kommunikation regelmäßig die äußere Form, die etwa eine Postsendung aufweist oder die das persönliche Verhältnis zum Empfänger einer Kommunikation erkennen lässt, und die dort zur Bestimmung der Schutzwürdigkeit relevant ist.
Vor allem aber beziehen sich elektronische Beweismittel zunehmend auf Nicht-Kommunikationsdaten (also vom Datenberechtigten nicht mitgeteilte oder Maschine-zu-Maschine Daten), deren unterschiedliche Schutzwürdigkeit von den Wertungen der analogen Beweismittel nicht unmittelbar erfasst wird. Stattdessen kommt hier, wie auch für alle anderen elektronischen Daten, das spezifische Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme zur Anwendung, das für die Bestimmung des wesentlich Gleichen ebenfalls zu berücksichtigen ist.

Auch wenn die Wertungsmaßstäbe vergleichbar sind und sich in großen Teilen überlappen, dürfen die jeweiligen grundrechtlichen Besonderheiten der einzelnen Beweismittel nicht vernachlässigt werden.

Zusammenfassend lässt sich festhalten, dass es einer gesonderten Einteilung elektronischer Beweismittel bedarf, weil die Unterscheidungskriterien, die für analoge Beweismittel zur Anwendung kommen, nicht vollständig den verfassungsrechtlichen Anforderungen an die Differenzierungsmerkmale elektronischer Daten entsprechen. Dass die vorgestellte Klassifikation elektronischer Daten in weiten Teilen vergleichbare Aussagen trifft wie diejenigen für analoge Daten, ist der Werteordnung des Grundgesetzes und den verfassungsrechtlichen Grundprinzipien zuzuschreiben, die den Rahmen für sämtliche Kategorisierungen abstecken, und lässt auf die Systemstimmigkeit des neuen Modells schließen.

F. Vorschlag für eine Neukonzipierung der StPO zum Umgang mit elektronischen Daten

Im Folgenden soll in einem gesetzlichen Musterentwurf die Anwendbarkeit des neuen Klassifikationsmodells demonstriert (dazu unter I.) und im Detail erläutert werden (II.).

I. Musterentwurf für die systematische Einbindung elektronischer Beweismittel in die StPO

7a. Abschnitt: Computerdaten

§ 93a	Unbeschränkt zugängliche Computerdaten
§ 93b	Datenauskunft von Dritten
§ 93c	Beauskunftung geheimer Computerdaten
§ 93d	Beauskunftung vertraulicher Computerdaten
§ 93e	Beauskunftung beschränkt zugänglicher Computerdaten
§ 93f	Zuordnung bei unklarem Sachverhalt
§ 93g	Antrags- und Anordnungsbefugnis für die Beauskunftungsanordnung
§ 93h	Rechtsfolgen der Beauskunftungsanordnung
§ 93i	Datensicherung und Sichtung
§ 93j	Rückgabe des Speichermediums
§ 93k	Verdeckte Eingriffe in informationstechnische Systeme
§ 93l	Verdeckte Erhebung geheimer Daten
§ 93m	Verdeckte Erhebung vertraulicher Daten
§ 93n	Verdeckte Erhebung beschränkt zugänglicher Daten
§ 93o	Antrags- und Anordnungsbefugnis für verdeckte Eingriffe in informationstechnische Systeme, Dauer
§ 93p	Kernbereich privater Lebensgestaltung und Zeugnisverweigerungsberechtigte
§ 93q	Einführung in die Hauptverhandlung
§ 93r	Schutz der Integrität und Authentizität von Computerdaten
§ 93s	Datenkennzeichnung, Verwertung der erhobenen Daten zu sonstigen Zwecken
§ 93t	Benachrichtigung und Datenlöschung

§ 93a Unbeschränkt zugängliche Computerdaten

Nicht-personenbezogene Computerdaten, öffentlich zugängliche gespeicherte Computerdaten und solche, die von demjenigen, der berechtigt Zugriff auf sie hat, rechtmäßig mitteilt werden, (unbeschränkt zugängliche Computerdaten) dürfen durch Übertragung in ein informationstechnisches System der Strafverfolgungsbehörde erhoben und für das weitere Verfahren verwertet werden, soweit sie für die Untersuchung von Bedeutung sein können.

§ 93b Datenauskunft von Dritten

(1) Über sonstige Computerdaten darf von demjenigen, der Zugriff auf solche Daten hat, Auskunft verlangt und dürfen die entsprechenden Daten für das weitere Verfahren verwendet werden. Dies gilt nicht

1. für Daten, die den Kernbereich privater Lebensgestaltung betreffen, oder
2. für Daten, die eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen betreffen, soweit die Datenerhebung voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte.

(2) Die Beauskunftung kann durch elektronische Übersendung, durch Übersendung eines Speichermediums, auf dem die Computerdaten gespeichert sind, oder dadurch erfolgen, dass der Betroffene der zuständigen Strafverfolgungsbehörde Zugriff auf sein informations-technisches System zur Erhebung der angefragten Daten gestattet.

(3) Erfolgt die Beauskunftung nicht freiwillig oder handelt es sich bei dem Betroffenen um eine Person, der aufgrund sonstiger gesetzlicher Vorschriften eine freiwillige Beauskunftung untersagt ist, so bedarf es der Anordnung der Beauskunftung. Gegenüber dem Beschuldigten ist die Anordnung unzulässig.

§ 93c Beauskunftung geheimer Computerdaten

Die Beauskunftung und Verwertbarkeit solcher Computerdaten, von deren Inhalt nach dem Willen des Datenberechtigten Dritte keine

Kenntnis erlangen sollen, (geheime Daten) darf angeordnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass der Datenberechtigte als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § [100a Absatz 2] bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat,
2. aus bestimmten Tatsachen zu schließen ist, dass der Dateninhalt für die Untersuchung Bedeutung hat, und
3. die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

§ 93d Beauskunftung vertraulicher Computerdaten

Die Beauskunftung und Verwertbarkeit solcher Computerdaten, von deren Inhalt nach dem Willen des Datenberechtigten ausschließlich solche Personen Kenntnis erlangen dürfen, zu denen ein besonders schutzwürdiges Vertrauensverhältnis besteht, (vertrauliche Daten) darf angeordnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass der Datenberechtigte als Täter oder Teilnehmer
   a) eine in § [100a Absatz 2] bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, oder
   b) eine Straftat durch den Einsatz seines informations-technischen Systems begangen hat,
2. aus bestimmten Tatsachen zu schließen ist, dass der Dateninhalt für die Untersuchung Bedeutung hat, und
3. die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung des zugrundeliegenden Vertrauensverhältnisses steht.

§ 93e Beauskunftung beschränkt zugänglicher Computerdaten

(1) Die Beauskunftung und Verwertbarkeit solcher Computerdaten, von deren Inhalt nach dem Willen des datenberechtigten Beschuldigten sonstige Dritte Kenntnis erlangen dürfen, ohne dass es sich um

öffentlich zugänglich gespeicherte Daten handelt, (beschränkt zugängliche Daten) darf angeordnet werden, wenn aus bestimmten Tatsachen zu schließen ist, dass der Dateninhalt für die Untersuchung Bedeutung hat.

(2) Personenbezogene Daten Dritter dürfen nur beauskunftet werden, soweit dies aus technischen Gründen zur Erreichung des Zweckes nach Absatz 1 unvermeidbar ist.

§ 93f Zuordnung bei unklarem Sachverhalt

Sofern Zweifel darüber bestehen, welcher der vorgenannten Kategorien die verlangten Daten zuzuordnen sind, finden die jeweils strengeren Anforderungen Anwendung.

§ 93g Antrags- und Anordnungsbefugnis für Beauskunftungsanordnung

(1) Ein Antrag auf Anordnung gemäß § 93c oder § 93d kann nur von der Staatsanwaltschaft, ein Antrag auf Anordnung gemäß § 93e kann von der Staatsanwaltschaft oder ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) gestellt werden.

(2) Die Anordnung gemäß § 93c bis § 93e darf nur durch das Gericht erfolgen. Bei Gefahr im Verzug kann die Anordnung der Beauskunftung auch durch die Staatsanwaltschaft und im Falle des § 93e außerdem auch durch ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) erfolgen; die gerichtliche Entscheidung über die Beauskunftungspflicht und die Verwertbarkeit der zu erlangenden Daten ist unverzüglich nachzuholen.

§ 93h Rechtsfolgen der Beauskunftungsanordnung

(1) Aufgrund der Anordnung hat die verlangte Beauskunftung unverzüglich zu erfolgen.

(2) Im Falle der Weigerung können gegen den Auskunftsverpflichteten die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Dies gilt nicht bei Personen, die zur Verweigerung des

Zeugnisses berechtigt sind.

(3) Steht aufgrund der vorliegenden Tatsachen fest, dass die verlangten Daten auf einem bestimmten Speichermedium gespeichert sind, und ist zu besorgen, dass sie verändert oder gelöscht werden, darf das Speichermedium zum Zwecke der Datensicherung nach den allgemeinen Vorschriften sichergestellt und beschlagnahmt werden. Steht aufgrund der konkreten Umstände des Einzelfalles fest, dass sich auf dem sichergestellten und beschlagnahmten Speichermedium keine weiteren Daten befinden, die nicht von der Beauskunftungsanordnung erfasst sind, so dürfen alle vorhandenen Daten durch Übertragung in ein informationstechnisches System der Strafverfolgungsbehörde erhoben werden.

§ 93i Datensicherung und Sichtung

(1) Daten, auf die zugegriffen werden kann aufgrund

1. einer Beauskunftung gemäß § 93e, die gemäß § 93e Absatz 2 auch persönliche Daten Dritter umfasst,
2. einer Sicherstellung oder Beschlagnahme des Speichermediums gemäß § 93h Absatz 3 Satz 1 oder
3. einer nach sonstigen Vorschriften zulässigen Maßnahme

sind durch Übertragung in ein informationstechnisches System der Strafverfolgungsbehörde vorläufig zu sichern.

(2) Im Falle des Absatzes 1 Nummer 1 dürfen die persönlichen Daten Dritter nur für den automatisierten Abgleich mit bestimmten, auf den Täter vermutlich zutreffenden technischen Prüfungsmerkmalen verwendet werden. Sie sind danach unverzüglich zu löschen.

(3) Die gesicherten Daten im Sinne des Absatzes 1 Nummer 2 und 3 sind zu sichten. Das Bundesministerium der Justiz und für Verbraucherschutz und die Landesregierungen bestimmen für ihren jeweiligen Geschäftsbereich durch Rechtsverordnung die jeweils zuständigen Sichtungsstellen sowie die näheren Einzelheiten der Durchführung.

(4) Im Falle des Absatzes 1 Nummer 2 dient die Sichtung ausschließlich der Feststellung, ob sich weitere Daten auf dem Speichermedium befinden, die nicht von der Beauskunftungsanordnung erfasst sind. Ist dies der Fall und hat der Betroffene gegen die Beschlagnahme ausdrücklich Widerspruch erhoben, so ist das beschlagnahmte Speichermedium unverzüglich an den Betroffenen zurückzugeben.
Die Daten, die nicht von der Beauskunftungsanordnung erfasst werden, sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(5) Im Falle des Absatzes 1 Nummer 3 dient die Sichtung der unverzüglich zu beantragenden gerichtlichen Feststellung, inwieweit die gesicherten Daten erhoben und für das weitere Verfahren verwendet werden dürfen. §§ 93b Absatz 1, 93c bis 93f, 93g Absatz 1 gelten entsprechend. Die gesicherten Daten, die nach diesen Vorschriften weder erhoben noch verwertet werden dürfen, sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

§ 93j Rückgabe des Speichermediums

Erfolgt die Beauskunftung durch Übersendung eines Speichermediums, so ist dieses nach der Sicherung und Erhebung der Daten unverzüglich zurückzugeben.

§ 93k Verdeckte Eingriffe in informationstechnische Systeme

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein vom Betroffenen genutztes informationstechnisches System eingegriffen, dürfen Datenverarbeitungsprozesse darin überwacht und dürfen Daten daraus erhoben und für das weitere Verfahren verwendet werden, es sei denn, dass tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.

(2) Die Maßnahme darf sich nur gegen den Beschuldigten richten und darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden, es sei denn, es handelt sich um eine Person im Sinne

des § 53.

(3) Die Maßnahme ist unverzüglich zu unterbrechen, wenn sich während ihrer Durchführung Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind, erfasst werden oder dass ein Fall des § 53 vorliegt. Bei Wegfall dieser Anhaltspunkte darf die Maßnahme fortgeführt werden; die Anordnung der Fortführung trifft die Staatsanwaltschaft.

(4) Vor dem Einsatz des technischen Mittels ist technisch sicherzustellen, dass

1. soweit technisch möglich, Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, nicht erhoben werden,
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden und
4. das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist.

(5) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. seine Bezeichnung und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

§ 93l Verdeckte Erhebung geheimer Daten

Lässt sich aufgrund der Art des betroffenen informationstechnischen Systems und aufgrund des einzusetzenden technischen Mittels nicht ausschließen, dass durch die Maßnahme eine Überwachung und Erhebung geheimer Daten im Sinne des § 93c ermöglicht wird, so darf

sie nur durchgeführt werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass der Datenberechtigte als Täter oder Teilnehmer eine auch im Einzelfall besonders schwerwiegende Straftat gemäß § [100b Abs. 2] begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und
2. die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

§ 93m Verdeckte Erhebung vertraulicher Daten

Lässt sich aufgrund der Art des betroffenen informationstechnischen Systems und aufgrund des einzusetzenden technischen Mittels nicht ausschließen, dass durch die Maßnahme eine Überwachung und Erhebung vertraulicher Daten im Sinne des § 93d ermöglicht wird, so darf sie nur durchgeführt werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass der Datenberechtigte als Täter oder Teilnehmer eine auch im Einzelfall schwerwiegende Straftat gemäß § [100a Abs. 2] begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat,
2. die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und
3. die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung des zugrundeliegenden Vertrauensverhältnisses steht.

§ 93n Verdeckte Erhebung beschränkt zugänglicher Daten

Lässt sich aufgrund der Art des betroffenen informationstechnischen Systems und aufgrund des einzusetzenden technischen Mittels sicherstellen, dass durch die Maßnahme eine Überwachung und Erhebung lediglich beschränkt zugänglicher Daten im Sinne des § 93e ermöglicht wird, so darf sie durchgeführt werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass der

Datenberechtigte als Täter oder Teilnehmer eine auch im Einzelfall erhebliche Straftat, insbesondere eine in § [100a Abs. 2] bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und

2. die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

§ 93o Antrags- und Anordnungsbefugnis für verdeckte Eingriffe in informationstechnische Systeme, Dauer

(1) Maßnahmen nach § 93l dürfen nur auf Antrag der Staatsanwaltschaft durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts angeordnet werden, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Bei Gefahr im Verzug kann diese Anordnung auch durch den Vorsitzenden getroffen werden. Dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

(2) Maßnahmen nach §§ 93m und 93n dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(3) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind

anzugeben: [§ 100e Abs. 5]

(4) In der Begründung der Anordnung oder Verlängerung von Maßnahmen nach den §§ 93l bis 93n sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben:

1. die bestimmten Tatsachen, die den Verdacht begründen, und
2. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

(5) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die Staatsanwaltschaft veranlasst wurde. Die Anordnung des Abbruchs einer Maßnahme nach § 93l kann auch durch den Vorsitzenden erfolgen.

§ 93p Kernbereich privater Lebensgestaltung und Zeugnisverweigerungsberechtigte

(1) Daten, die den Kernbereich der persönlichen Lebensgestaltung betreffen und im Rahmen einer Maßnahme gemäß §§ 93b bis 93e, 93i und 93k bis 93n erhoben wurden, sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(2) Für Daten, die Personen im Sinne des § 53 betreffen und entgegen §§ 93b Absatz 1 Nummer 2 und 93k Absatz 2 erhoben wurden, gilt Absatz 1 entsprechend.

§ 93q Einführung in die Hauptverhandlung

(1) Computerdaten, die als elektronische Beweismittel verwendet werden können, sind in laienverständlicher aussagekräftiger Form in die Hauptverhandlung einzuführen. Soweit dadurch Schriftstücke, Ausdrucke oder sonstige Augenscheinsobjekte entstehen, gelten die

diesbezüglichen allgemeinen Vorschriften entsprechend.

(2) Bei der erforderlichen Umwandlung der elektronischen Beweismittel in andere Formate oder ihre Wiedergabe in einem geeigneten informationstechnischen System ist nach dem Stand der Technik eine lückenlose Beweiskette sicherzustellen.

§ 93r Schutz der Integrität und Authentizität von Computerdaten

(1) Für sämtliche Maßnahmen, die die Sicherung, Erhebung oder sonstige Verarbeitung von Computerdaten betreffen, sind Vorkehrungen zu treffen, die nach dem Stand der Technik die Integrität und Authentizität der Daten gewährleisten.

(2) Computerdaten, die als Beweismittel in Betracht kommen, sind, sobald der Zugriff auf sie möglich ist, nach dem Stand der Technik vor unbefugter Veränderung, Löschung oder Kenntnisnahme zu schützen.

(3) Notwendige Datenveränderungen sind so vorzunehmen, dass sie nachvollziehbar bleiben. Sie sind kenntlich zu machen.

(4) Das Bundesministerium der Justiz und für Verbraucherschutz und die Landesregierungen können für ihren jeweiligen Geschäftsbereich durch Rechtsverordnung nähere Einzelheiten der Durchführung bestimmen und konkrete Verfahren zulassen, die die Integrität und Authentizität zu verarbeitender Computerdaten sicherstellen.

§ 93s Datenkennzeichnung, Verwertung der erhobenen Daten zu sonstigen Zwecken

(1) Personenbezogene Daten, die durch Maßnahmen nach §§ 93l bis 93n erhoben wurden, sind entsprechend zu kennzeichnen. Die Kennzeichnung ist nach einer Übermittlung an eine andere Stelle aufrechtzuerhalten.

(2) Für die Verwertung der durch eine Maßnahme nach §§ 93c bis 93e gewonnenen personenbezogenen Daten zu sonstigen Zwecken gilt §

[101a Absätze 4 und 5] entsprechend. Für die Verwertung der durch eine Maßnahme nach §§ 93l bis 93n gewonnenen personenbezogenen Daten zu sonstigen Zwecken gilt § [100e Absatz 6] entsprechend.

§ 93t Benachrichtigung und Datenlöschung

(1) Für die Benachrichtigung des von einer Maßnahme nach §§ 93c bis 93n Betroffenen gilt § [101 Absätze 4 bis 7] entsprechend.

(2) Für die Löschung des von einer Maßnahme nach §§ 93c bis 93n Betroffenen gilt § [101 Absatz 8] entsprechend.

II. Erläuterungen zum Musterentwurf

Der vorliegende Vorschlag dient als ein Beispiel für die konzeptionelle Einbindung elektronischer Daten als Beweismittel in der StPO. Auch unter Berücksichtigung der wesentlichen Eckpunkte – namentlich der entwickelten Datenkategorisierung zur Erfassung von „wesentlich Gleichem“ und „wesentlich Ungleichem“, der verfassungsrechtlichen Schlüsselprinzipien für eine gute Gesetzgebung[494] und der formellen Empfehlungen der modernen Gesetzgebungslehre[495] – verbleibt für die konkrete Ausgestaltung ein gesetzgeberischer Spielraum mit vielen Gestaltungsmöglichkeiten,[496] wobei insbesondere die Eingriffsvoraussetzungen (Schwere des Deliktes, Schwere des Tatverdachtes, Zweck der Maßnahme) und die Antrags- und Anordnungsbefugnisse unterschiedlich gewichtet werden können.

Aufgrund der noch andauernden aktuellen Entwicklungen auf EU-Ebene zum Thema grenzüberschreitender Zugriff auf elektronische Beweismittel beschränkt sich der Musterentwurf auf rein nationale Sachverhalte.

Vor diesem Hintergrund gelten folgende Erläuterungen zum erarbeiteten Vorschlag:

1. Die vorgeschlagene Einführung eines neuen Abschnittes in die StPO („7a. Abschnitt“) verdeutlicht, dass der Strengbeweiskanon um ein weiteres Element erweitert wird. Die Einfügung empfiehlt sich aus thematischer Sicht hinter den Beweismitteln Sachverständige und Augenschein im 7. Abschnitt und vor einzelnen Zwangsmaßnahmen (Beschlagnahme, Überwachung

494 Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 201, beschreibt folgende Schlagworte: Erforderlichkeit, Balance der Vor- und Nachteile, Transparenz und Teilnahme, Zuständigkeit und Kompetenzklarheit, Einfachheit, Konsistenz und Kohärenz, Systemkonformität und Stabilität; vgl. auch Schneider, *Gesetzgebung*, S. 33 ff.

495 Vgl. Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 210 ff., zu Struktur, Aufbau, inhaltlicher Gliederung und Ausdruck eines „guten“ Gesetzes.

496 Insbesondere zum Gestaltungsspielraum hinsichtlich der Regelungsdichte und -detailliertheit: Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (54 f.).

des Fernmeldeverkehrs etc.) im 8. Abschnitt; sie bietet zudem die Möglichkeit, den Umgang mit elektronischen Daten umfassend in „§ 93-er“-Vorschriften zu regeln.

2. Soweit auf bestehende Regelungen der StPO Bezug genommen wird, sind diese in eckige Klammern gesetzt.

3. Die Grobeinteilung des Entwurfes sieht fünf Blöcke vor, von denen die vier ersten mögliche Ermittlungsmaßnahmen im Zusammenhang mit elektronischen Beweismitteln erfassen – die direkte, offene Datenerhebung durch die Ermittlungsbehörden, die Beauskunftung durch Dritte, die Datensicherung und -sichtung sowie die verdeckte Datenerhebung -, während der Schlussteil allgemeine Grundsatz- und Verfahrensregelungen für alle genannten Maßnahmen betrifft.

4. Die zulässigen Maßnahmen innerhalb eines Blockes richten sich ausschließlich nach der dogmatisch begründeten Datenkategorisierung. Bisherige Begriffe wie Bestands- oder Verkehrsdaten, denen rechtsfremde Unterscheidungskriterien zugrundeliegen, werden daher ebenso wenig aufgegriffen wie die Differenzierung von gespeicherten Daten und solchen aus einem laufenden Übertragungsvorgang.

5. Die vorgeschlagenen Regelungen erlauben vergleichbare Datenerhebungen, wie sie bereits heute praktiziert werden, stellen diese jedoch auf eine explizite gesetzliche Grundlage, die nicht nur umfassend, sondern wegen ihrer Technikneutralität auch unabhängig vom technischen Fortschritt zukunftsbeständig ist.

6. Eine sorgfältige Abwägung der Eingriffsvoraussetzungen, die zwischen offenen und verdeckten Maßnahmen unterscheidet und die die beim direkten Gerätezugriff technisch bedingten Gefahren der Datenveränderung berücksichtigt, gewährleistet die Wahrung der Verhältnismäßigkeit auf Gesetzesebene,[497] während weitere Aspekte bei der Durchführung der konkreten Maßnahme nach allgemeinen Maßstäben zu berücksichtigen sein werden.

   Für den konkreten Einzelfall wird beispielsweise zu prüfen sein,

497 Zur Bedeutung dieser Kriterien für die Prüfung der Verhältnismäßigkeit: BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 68; BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 370/07, zugleich BVerfGE 120, 274, Rn. 239.

ob die Ermittlungsmaßnahme punktuell oder längerfristig erfolgt, ob der Verwendungszweck der zu erlangenden Daten bereits bei der Erhebung bestimmt ist oder nicht, und ob der Betroffene über Einwirkungsmöglichkeiten auf seinen Datenbestand verfügt.[498] Daneben spielen der Anlass der Datenabfrage[499] und das zu erlangende Datenvolumen[500] eine bedeutende Rolle.

7. Mit der Verwendung der Begriffe Computerdaten, öffentlich zugängliche gespeicherte Computerdaten und informationstechnisches System wird an die entsprechenden, umfassenden Definitionen der Cybercrime-Konvention und der AAIS-Richtlinie angeknüpft, wobei zur besseren Lesbarkeit für Computerdaten auch das Synonym Daten gebraucht wird.

8. § 93a beinhaltet eine Legaldefinition der unbeschränkt zugänglichen Computerdaten und der Datenerhebung und sieht für die Erhebung und Verwertung solcher Daten eine generelle Zulässigkeit vor.

9. § 93b Abs. 1 erlaubt grundsätzlich die Erfragung elektronischer Beweismittel von Dritten und die nachfolgende Verwertung aller sonstigen Computerdaten mit Ausnahme der Kernbereichsdaten und, in Anlehnung an § 100g Abs. 4 StPO, der Daten, die Personen im Sinne des § 53 StPO betreffen. Damit erübrigt sich die bisherige Unterscheidung von Telekommunikations- und sonstigen Dienstleistern.[501]

   Absatz 2 der Norm stellt klar, dass die Beauskunftung auf unterschiedliche Art erfolgen kann.

10. Für den Fall, dass die Beauskunftung nicht freiwillig erfolgt oder die Auskunftsperson insbesondere aufgrund datenschutzrechtlicher Vorschriften an einer freiwilligen Datenübermittlung rechtlich gehindert ist – das betrifft vor allem die enorm praxisrelevanten Telekommunikations- und Telemedien-Dienstleister -,

498 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 68.
499 BVerfG, Beschluss vom 13.11.2010, 2 BvR 1124/10, WM 2011, 211 (212).
500 BVerfG, Beschluss vom 16.06.2009, 2 BvR 902/06, zugleich BVerfGE 124, 43, Rn. 68.
501 Zur Fragwürdigkeit dieser Unterscheidung und ihrer negativen Konsequenzen für das Ermittlungsverfahren vgl. Hiéramente / Pfister, *Datenerhebung beim Hersteller von Mobiltelefonen, Zum Erfordernis des Strukturwandels bei der strafprozessualen Datenerhebung*, StV 2017, 477 (478 ff.).

sieht der Entwurf die Anordnung der Beauskunftung für die Begründung einer gesetzlichen Handlungspflicht vor.

11. § 93c nennt die konkreten Voraussetzungen einer Beauskunftungsanordnung für geheime Daten, die zudem legaldefiniert werden. Da solche Daten per definitionem nicht an Dritte zur Kenntnisnahme mitgeteilt werden und eine Anordnung gegenüber dem Beschuldigten wegen des nemo-tenetur Grundsatzes nicht zulässig ist, kommen als Verpflichtete nur Anbieter von Speicherdiensten, namentlich von Cloud-Speicherdiensten in Betracht.

    Die inhaltlichen Anordnungsvoraussetzungen entsprechen im Wesentlichen denen des § 100a StPO.

12. § 93d nimmt den Begriff der vertraulichen Daten auf und gestattet eine Beauskunftungsanordnung nicht nur in den mit § 100a StPO vergleichbaren Fällen, sondern auch, wenn – vergleichbar mit § 100g StPO – die zugrundeliegende Tat durch den Einsatz eines informationstechnischen Systems begangen wurde. Gleichzeitig wird aus Gründen der Verhältnismäßigkeit die Notwendigkeit der Beachtung des konkreten Vertrauensverhältnisses explizit hervorgehoben.

13. § 93e betrifft die Beauskunftungsanordnung für beschränkt zugängliche Daten, die legaldefiniert werden. Sie ist inhaltlich an die Postbeschlagnahme und Brieföffnung gemäß §§ 99 f. StPO angelehnt, die nur geringe inhaltliche Anforderungen stellen, obgleich ein Brief durchaus sehr vertrauliche Inhalte haben kann. Da im Rahmen des § 93e auch Funkzellendaten erfasst werden, ist die ausdrückliche Gestattung der Datenerhebung unbeteiligter Dritter in Absatz 2 aufgenommen und auf das notwendige Maß begrenzt.

14. § 93f dient dem Schutz des Datenberechtigten, indem vorgeschrieben wird, dass bei Zweifeln über die zutreffende Datenkategorie die jeweils strikteren Voraussetzungen für eine Beauskunftungsanordnung erfüllt sein müssen.

15. § 93g regelt die Antragsbefugnis und die Anordnungsbefugnis für eine Beauskunftung bei Gefahr im Verzug jeweils in Abhängigkeit von der zutreffenden Datenkategorie und stellt gleichzeitig klar,

dass die Anordnung letztendlich immer durch das Gericht vorzunehmen beziehungsweise zu bestätigen ist.

16. § 93h Abs. 1 sieht als Rechtsfolge einer Beauskunftungsanordnung die unverzügliche Handlungspflicht des Adressaten vor. Diese Klarstellung ist aus datenschutzrechtlichen Gründen notwendig und führt gleichzeitig dazu, dass eine „Quick-Freeze“ Anordnung gegenüber Dienstleistern entbehrlich ist.

    Absatz 2 sieht durch den Verweis auf § 70 StPO Sanktionen für die Nichtbefolgung vor und nimmt davon ausdrücklich diejenigen aus, denen ein Zeugnisverweigerungsrecht zusteht.

17. Daneben gibt Absatz 3 die Möglichkeit, bei verweigerter Beauskunftung und der Gefahr der zwischenzeitlichen Datenmanipulation das Datenspeichermedium (den USB-Stick, die Kamera, das Smartphone etc.) nach den allgemeinen Vorschriften sicherzustellen und zu beschlagnahmen, um dadurch den Datenbestand zu sichern und zu erheben.

18. § 93i führt die Instrumente der Datensicherung und der Sichtung ein. Die Datensicherung ist – vergleichbar mit der Sicherstellung beweglicher Sachen - als Vorstufe vor der Entscheidung über die endgültige Erhebung konzipiert.[502] Sie bezieht sich auf die Daten, die durch eine zulässige Maßnahme erlangt werden, deren endgültige Erhebung aber entweder nicht erforderlich oder zwar denkbar, aber jedenfalls noch nicht entschieden ist, weil ihre Sensibilität und damit die Voraussetzungen ihrer Erhebung noch nicht bestimmt werden konnten. Die erste Fallgruppe, in der nachträglich „aussortiert“ werden muss, betrifft beispielsweise Daten unbeteiligter Dritter, die etwa bei der Funkzellenabfrage aus technischen Gründen mitbeauskunftet werden, aber auch für das Ermittlungsverfahren unerhebliche Daten, die über das konkrete Beauskunftungsverlangen hinaus übersandt werden. Daten, auf die die Strafverfolgungsbehörde bereits faktisch Zugriff hat und die gegebenenfalls zu erheben sind, betreffen zum Beispiel möglicherweise sonstige vorhandene Daten auf einem gemäß § 93h beschlagnahmten Speichermedium,

502 Zur Bedeutung der „Auswertungsphase“ jedenfalls bei Kernbereichsdaten vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 277.

unbekannte Daten, die sich auf einem beschlagnahmten Datenträger befinden, oder Daten, die während einer Hausdurchsuchung „live“ auf dem Rechner des Betroffenen erkennbar sind.

19. Die Datensicherung entspricht durch das Merkmal der Übertragung in ein informationstechnisches System der Strafverfolgungsbehörde der Datenerhebung, hat im Unterschied dazu allerdings nur einen vorläufigen Charakter.
Funkzellendaten unbeteiligter Dritter dürfen in Anlehnung an §§ 98b, 100i Abs. 2 StPO lediglich zum automatischen Abgleich gesichert werden und sind danach unverzüglich zu löschen; die sonstigen unbekannten Daten sind - vergleichbar mit der Durchsicht des § 110 StPO – zu sichten.

20. § 93i Abs. 3 enthält ähnlich wie §§ 484 Abs. 3 und 41a Abs. 2 a.F. StPO eine Verordnungsermächtigung für die nähere Ausgestaltung des Sichtungsverfahrens.

21. § 93i Abs. 4 und 5 konkretisieren, wie im Falle beschlagnahmter Datenträger oder sonstiger Erlangung unbekannter Daten die Sichtung vorzunehmen ist.

22. Die Rückgabe des Speichermediums, durch dessen Übersendung eine Beauskunftung ausgeführt wurde, ist entsprechend § 98b Abs. 3 StPO in § 93j geregelt.

23. § 93k regelt die grundsätzliche Gestattung verdeckter Eingriffe in informationstechnische Systeme. Damit werden die derzeitigen §§ 100a f. StPO zusammengeführt, ohne dass dadurch § 100a für die reine TKÜ obsolet würde: dort, wo keine Voice-over-IP Telefonie stattfindet, besteht weiterhin ein Anwendungsfall für die klassische Telefonüberwachung, zu deren Durchführung die Ermittlungsbehörden auf die Unterstützung der Telekommunikationsdienstleister angewiesen sind. Bei der Internettelefonie bedarf es dieser Unterstützung nicht, weil die Überwachung durch Einbringen entsprechender Spähsoftware unmittelbar durch die Ermittlungsbehörde erfolgen kann. Die denkbare rechtspolitische Alternative, dass Dienstleister gesetzlich zur Unterstützung einer solchen Maßnahme verpflichtet werden sollten (und damit eine „Backdoor“-Regelung einzuführen wäre),

wird im vorliegenden Entwurf nicht aufgegriffen.[503]

Die Voraussetzungen der einzelnen Maßnahmen richten sich, wie schon bei der Beauskunftung durch Dritte, ausschließlich nach dem hergeleiteten Datenklassifikationsmodell. Eine Unterscheidung zwischen der Erhebung gespeicherter oder Echtzeit-Daten ist damit überflüssig.

24. § 93k Abs. 2 beschreibt die von einer solchen Maßnahme zulässigerweise Betroffenen und berücksichtigt die Wertungen der §§ 100b Abs. 3 und 100d Abs. 5 StPO.

25. In § 93k Abs. 3 finden sich entsprechend § 100d Abs. 4 StPO Regelungen dazu, wie zu verfahren ist, wenn während einer zulässigen Maßnahme die weitere Datenerhebung unzulässig wird.

26. In Anlehnung an § 100a Abs. 5 StPO legt § 93k Abs. 4 die technischen Anforderungen an das einzusetzende technische Mittel fest, um die Durchführung eines möglichst schonenden Eingriffes mit minimaler Beeinträchtigung zu gewährleisten. Maßgeblich ist hierbei immer der aktuelle Stand der Technik.

27. § 93k Abs. 5 sieht wie § 100a Abs. 6 Protokollierungspflichten bei der Durchführung jeder verdeckten Datenerhebung vor.

28. Die verdeckte Erhebung geheimer Daten darf gemäß § 93l unter vergleichbaren Bedingungen wie die online-Durchsuchung nach § 100b StPO durchgeführt werden.

29. Die inhaltlichen Anforderungen für die verdeckte Erhebung vertraulicher Daten entsprechen gemäß § 93m denen des § 100a StPO und erfordern zusätzlich eine besondere Berücksichtigung des konkreten Vertrauensverhältnisses.

30. Bei beschränkt zugänglichen Daten schließlich kommt eine verdeckte Erhebung gemäß § 93n entsprechend den Voraussetzungen des § 100i StPO (Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten) in Betracht. Das ist sachgerecht, weil es sich bei den in § 100i StPO geregelten Daten um beschränkt zugängliche Daten im Sinne der Neuklassifikation handelt.

31. Durch die ausdrückliche Bezugnahme des § 100i StPO auf den

503 Zur Diskussion um die Einführung einer solchen Backdoor-Regelung vgl. Gollasch, *De Maizière will Ausspähen von Privat-Autos, Computern und Smart-TVs ermöglichen*.

Straftatenkatalog des § 100a StPO und die Regelung des § 93m kann eine Quellen-Telekommunikationsüberwachung auf demselben Schutzniveau wie bisher unter § 100a StPO durchgeführt werden, wobei durch den Musterentwurf zusätzlich das konkrete Vertrauensverhältnis ausdrücklich zu berücksichtigen ist.

32. § 93o Abs. 1 und 2 regelt die Antrags- und Anordnungsbefugnis sowie die Anordnungsdauer für die verdeckte Erhebung geheimer Daten entsprechend derjenigen für Maßnahmen nach § 100b StPO und die für die vertraulichen und beschränkt zugänglichen Daten einheitlich wie für § 100a StPO.

    Die formellen Anforderungen an die Anordnung für jede verdeckte Datenerhebung in § 93o Abs. 3 und 4 entspricht § 100e Abs. 4 und 5 StPO. Gleiches gilt für die Beendigung einer Maßnahme gemäß § 93o Abs. 5 wie § 100e Abs. 5 StPO.

33. Der besondere Schutz des Kernbereichs privater Lebensgestaltung und der in § 53 StPO genannten zeugnisverweigerungsberechtigten Personen spiegelt sich in Anlehnung an § 100d Abs. 2 und 5 StPO in § 93p wider, der auf alle vorgeschlagenen Ermittlungsmaßnahmen Anwendung findet.

34. § 93q gibt allgemein Auskunft darüber, wie elektronische Beweismittel in die Hauptverhandlung einzuführen sind – nämlich in laienverständlicher aussagekräftiger Form. Gleichzeitig wird gefordert, dass jede Aufbereitung der ursprünglichen Daten in diese Form nachvollziehbar und eine lückenlose Beweiskette darstellbar sein muss. Damit wird dem Umstand Rechnung getragen, dass jede Umwandlung das Risiko einer Datenveränderung in sich birgt.

35. § 93r Abs. 1 bis 3 sehen zwingende Vorkehrungen zum Schutz der Integrität und Authentizität eines Datensatzes vor, deren Bedeutung und bisher nur punktuelle gesetzliche Erfassung bereits ausführlich dargestellt wurden. Es ist unumgänglich, dass die Integritäts- und Authentizitätssicherung für alle elektronischen Beweismittel und nicht nur, wie bisher, im Rahmen einzelner Maßnahmen gilt.

    Abs. 4 enthält eine Verordnungsermächtigung zur näheren technischen und organisatorischen Ausgestaltung.

36. Die Regelungen des § 93s zur Datenkennzeichnung und zur Verwertung der erhobenen Daten zu sonstigen Zwecken entsprechen den gesetzlichen Wertungen der §§ 101 Abs. 3, 101a Abs. 3 und 100e Abs. 6 StPO.

37. § 93t, der sich auf die Benachrichtigung des Betroffenen und die Datenlöschung bezieht, folgt der gesetzgeberischen Entscheidung in § 101 Abs. 4 bis 8 StPO.

38. Bei Übernahme des vorliegenden Entwurfes durch den Gesetzgeber wären neben den einschlägigen Datenschutzbestimmungen und den Vorschriften des TKG jedenfalls folgende Regelungen redaktionell anzupassen beziehungsweise zu streichen:

    §§ 98b, 100a, 100b, 100d, 100e, 100g, 100i, 100j, 101, 101a, 101b und 110 Abs. 3 StPO.

G. Fazit

Die bisherigen Ausführungen belegen Folgendes:

(1) Die derzeitige Erfassung elektronischer Daten durch die StPO ist unzureichend und dringend reformbedürftig.

(2) Erforderliche neue Normierungen, durch die wesentlich Gleiches gleich und wesentlich Ungleiches ungleich geregelt werden kann, erfordern eine Datenkategorisierung, die sich nach rechtlich relevanten, typischen Grundmerkmalen der Daten richtet.

(3) Die bereits vorhandenen Kategorisierungen für analoge Beweismittel in der StPO lassen sich nicht direkt auf elektronische Daten übertragen.

(4) Anhand der verfassungsrechtlichen Vorgaben kann ein neues Klassifikationsmodell herausgearbeitet werden, das maßgeblich auf dem **Unterscheidungskriterium der berechtigten Erwartungshaltung der Vertraulichkeitswahrung des Datensubjekts** beruht.

(5) Die neu entwickelte Klassifizierung elektronischer Beweismittel führt zu folgenden Datenkategorien, geordnet nach zunehmender rechtlicher Schutzwürdigkeit:

- **unbeschränkt zugängliche Daten,**
- **beschränkt zugängliche Daten,**
- **vertrauliche Daten,**
- **geheime Daten und**
- **Kernbereichsdaten.**

(6) Die vergleichbaren Wertungen und weitgehend übereinstimmenden Schlussfolgerungen mit den Klassifikationen analoger Beweismittel belegen die Kohärenz und Systemstimmigkeit des neu entwickelten Modells.

H. Ausblick

I. Neukonzeptionierung der StPO

Diese Arbeit geht einen ersten, notwendigen Schritt in Richtung einer konzeptionellen Einbindung elektronischer Beweismittel in die Systematik der StPO, die sich nicht nur auf die Anerkennung elektronischer Daten als eigenständiges Beweismittel im Strengbeweiskanon sondern auch auf ihre Erlangung und ihre konkrete Einführung in die Hauptverhandlung beziehen sollte.

Sie gibt dem Gesetzgeber ein Instrument an die Hand, mit dem hinsichtlich sämtlicher datenbezogener strafprozessualer Eingriffsmaßnahmen – seien es Vorgänge mit Beteiligung Dritter, seien es unmittelbare Handlungen allein der Strafverfolgungsbehörden - einschließlich der gerichtlichen Datenverwertung unterschiedliche Voraussetzungen normiert werden können, die der unterschiedlichen Schutzwürdigkeit elektronischer Datensätze gerecht werden.
Damit ist nicht ausgeschlossen, dass unterschiedliche Datenkategorien identischen Maßnahmen unterliegen, solange gewährleistet ist, dass die Bedingungen hierfür der Schutzwürdigkeit der jeweils höherrangigen Kategorie entsprechen.

Dass die Anwendung der neuen Kategorisierung sinnvoll als Instrument einer entsprechenden Gesetzgebung eingesetzt werden kann, verdeutlicht der vorgelegte Musterentwurf.

II. Anwendung zur Beweiswürdigung

Eine mittelbare Anwendung der erarbeiteten Grundsätze im Bereich der Beweiswürdigung empfiehlt sich bereits vor der Schaffung gesetzlicher Normierungen. Solange konkrete gesetzliche Regelungen zur Gewährleistung der Integrität und Authentizität eines im Strafverfahren präsentierten elektronischen Datensatzes fehlen, kann daran gedacht werden, gestaffelte Anforderungen an den jeweiligen Nachweis zu stellen, indem im Grundsatz (also mit der Möglichkeit der

Abweichung im Einzelfall) unterstellt werden könnte, dass die Nachweiserfordernisse umso geringer sind, je weniger sensibel ein bestimmter Datensatz ist.

Beispielsweise könnte bei unbeschränkt zugänglichen Daten im Regelfall der explizite Nachweis der Integrität und Authentizität des Datensatzes entbehrlich sein, während insbesondere für die Präsentation geheimer Daten grundsätzlich der Nachweis einer lückenlosen Beweiskette gefordert werden könnte. Eine zukünftige gesetzliche Regelung könnte dies aufgreifen und je nach Datenkategorie bestimmte Sicherungsvorgaben wie zertifizierte forensische Verfahren, sachverständige Überprüfung oder Ähnliches verlangen.

III. Anwendung zum Umgang mit Big Data

Denkbar wäre zudem, die vorgestellten Datenklassen bei der Frage, wie mit Big Data umgegangen werden kann, zu berücksichtigen. Falls diesbezüglich eine Limitierung der zu sichtenden Datenmenge in Betracht käme, könnte die unterschiedliche Sensibilität von Datensätzen unterschiedliche Kriterien für die Auswahlbeschränkung begründen und zum Beispiel striktere Beschränkungsmöglichkeiten für sensiblere Daten postulieren – oder umgekehrt.

IV. Anwendung auf Regelungen zur Vorratsdatenspeicherung

Desweiteren sollte der Sensibilitätsgrad eines Datensatzes ein wesentliches Abwägungskriterium für die Frage der Daten-speicherungsrechte und -pflichten sein, deren gesetzliche Normierung spätestens seit der „Tele2 / Watson“ - Entscheidung des Europäischen Gerichtshofes vom Gesetzgeber überprüft und möglicherweise angepasst werden muss.[504] Jedenfalls in diesem Zusammenhang kann das neue Klassifizierungsmodell über die StPO hinaus auch im Verwaltungs- und Zivilrecht zur Anwendung kommen.

504 EuGH, Urteil vom 21.12.2016 („Tele2 / Watson“), Az. C-203/15 und C-698/15.

V. Anwendung zur Einzelfallabwägung

Daneben ist zu erwägen, die Neuklassifizierung im bestehenden Rechtsrahmen als Hilfe für die konkrete Einzelfallabwägung einzusetzen, da sich aus ihr unmittelbare Aussagen zur relativen Schutzwürdigkeit einzelner Datensätze erlauben.

VI. Anwendung auf EU-Level

Im Idealfall könnte die Neuklassifizierung – vergleichbar mit dem vom Bundesverfassungsgericht 2008 konstituierten Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme[505] - sukzessive inhaltlich in den anderen EU-Mitgliedstaaten übernommen werden.[506] Eine Gelegenheit, dem „unübersehbaren Trend zur Rechtsvereinheitlichung“[507] auf EU-Ebene zu folgen, böte die aktuelle Rechtsentwicklung im Bereich des strafprozessualen grenzüberschreitenden Zugangs zu elektronischen Beweismitteln. Die allgemein zunehmende Verzahnung von Europarecht und nationalem Recht und die wachsende Verknüpfung rechtlicher Regelungen in den mitgliedstaatlichen Ordnungen untereinander legen weitere Bemühungen um wechselseitige Abstimmungen der Rechtsordnungen nahe.[508] Das gilt insbesondere dort, wo das Territorialitätsprinzip zunehmend an seine Grenzen stößt[509] und die nationalen Strafverfolgungsbehörden mehr

505 BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274. Auf die Schutzwürdigkeit dieses neuen Grundrechts nimmt etwa Art. 5 Abs. 1 lit. f der DS-GVO vom 27.04.2016 explizit Bezug.

506 Ausdrücklich für das Erfordernis einer globalen Neuklassifizierung elektronischer Daten, die sich, ähnlich wie in dieser Arbeit vertreten, nach der Eingriffsintensität in die Rechte des Datenschutzes und der Privatsphäre („privacy“) und nicht nach den technikabhängigen, praktischen Bedürfnissen der Dienstleister richten sollte: Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (679); allgemein für ein internationales Rahmenabkommen („general framework“) über den grenzüberschreitenden Zugang der Strafverfolgungsbehörden zu jedenfalls bestimmten elektronischen Daten: Internet & Jurisdiction Policy Network, *Cross Border Access to User Data*, S. 4 und 8.

507 So Karpen, *Gesetzgebungslehre – neu evaluiert*, S. 94.

508 Hoffmann-Riem, *Gesetz und Gesetzesvorbehalt im Umbruch, Zur Qualitäts-Gewährleistung durch Normen*, AöR, Bd. 130 (2005), 5 (65).

509 Obgleich das Territorialitätsprinzip gemäß Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 8, weiterhin die

und mehr auf Unterstützung aus dem Ausland angewiesen sind.

Eine länderübergreifende Regelung, die eine gemeinsame Begriffsverwendung voraussetzt, wird zunehmend unumgänglich. Das zeigt auch der Ruf der Europäischen Kommission Services nach einer harmonisierten, erweiterten Datenklassifikation.[510] Wie die Berichte der Europäischen Kommission zum durchgeführten Expertenprozess[511] und insbesondere die Auswertung des dazugehörigen Fragebogens[512] zeigen, weisen die EU-Mitgliedstaaten vergleichbare Ansätze auf, da sie, sofern dort eine Datenklassifikation vorgenommen wird, einheitlich auf die Sensibilität eines Datensatzes Bezug nehmen und – einheitlich – die herkömmliche Einteilung von Kommunikationsdaten, über die Konsens herrscht, nicht hinterfragen. Dabei wäre eine aus den spezifischen Grundrechten abgeleitete Datenkategorisierung, wie sie in dieser Arbeit vorgeschlagen wird, in allen EU-Mitgliedstaaten möglich, weil sie, wie ein Blick auf die Charta der Grundrechte der Europäischen Union und die Europäische Menschenrechtskonvention zeigt, über vergleichbare grundrechtliche Werteordnungen verfügen.

VII. Normierte Begrifflichkeit im internationalen Kontext

Selbst ohne eine vergleichbare rechtliche Ausgestaltung im Ausland läge der Vorteil einer Neuklassifizierung im Hinblick auf die internationale Zusammenarbeit jedenfalls darin, dass diejenigen Missverständnisse vermieden würden, die aufgrund des unterschiedlichen Verständnisses der derzeit allgemein verwendeten Begriffe entstehen.

---

maßgebliche Grundlage strafrechtlicher Ermittlungstätigkeit sei, führe es aufgrund der beschriebenen Besonderheiten elektronischer Beweismittel in ihrem Zusammenhang teilweise zu unerwünschten, teilweise gar „absurden“ Situationen (so Svantesson / van Zwieten, *Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution*, Computer Law & Security Review, Volume 32, Issue 5, October 2016, S. 671 (678)), wenn „das Cloud-Modell des 21. Jahrhunderts“ auf die „verfahrensrechtlichen Methoden des 20. Jahrhunderts“ treffe (Koops / Goodwin, *Cyberspace, the cloud and cross-border criminal investigations,* S. 7).

510 Europäische Kommission Services, *Technical Document*, S. 18 f.

511 Europäische Kommission, *Progress Report,* 07.12.2016, und Europäische Kommission Services, *Technical Document*.

512 Europäische Kommission, *Summary of Member States replies to the questionnaire on e-evidence*.

VIII. Ausgestaltung der unbestimmten Rechtsbegriffe

Trotz objektiv bestimmbarer Abgrenzungskriterien ist davon auszugehen, dass bei Anwendung der vorgeschlagenen Neuklassifizierung in der Praxis zunächst Abgrenzungsschwierigkeiten auftreten werden, die insbesondere die Kategorien der Kernbereichsdaten, der vertraulichen Daten und der beschränkt zugänglichen Daten betreffen könnten.
Die Verwendung dieser unbestimmten Rechtsbegriffe an sich ist dabei unproblematisch, da sie nicht so weit gehen, dass verbleibende Ungewissheiten die Vorhersehbarkeit und Justitiabilität des staatlichen Handelns gefährden würden:[513] Die genannten Abgrenzungsprobleme bestehen durchaus bereits heute, wenn es um die Zuordnung eines Datensatzes geht, der nahe am oder gerade im absolut geschützten Kernbereich liegt.

Eine höchstrichterliche Klärung wäre insbesondere im Zusammenhang mit der Schutzwürdigkeit des Vertrauens im virtuellen Raum wünschenswert, aber auch zur Bedeutung des Einsatzes von Verschlüsselung und zum Auseinanderfallen von Handlung, Intention und Erwartungshaltung des Datenberechtigten.

1. Schutzwürdiges Vertrauen im Cyberspace

Allerdings wird schon seit einigen Jahren diskutiert, ob überhaupt und, wenn ja, unter welchen Voraussetzungen ein schutzwürdiges Vertrauen in einen Internet-Kommunikationspartner entstehen kann, dessen Identität und Wahrhaftigkeit nicht überprüfbar ist.[514] Es ist zu erwarten, dass sich wie für die bereits bekannten Konstellationen mit weiteren höchstrichterlichen Entscheidungen verlässliche Kriterien herausbilden, die die Einordnung eines bestimmten Datensatzes erleichtern werden,

513 Zu dieser Voraussetzung für die Zulässigkeit der Verwendung unbestimmter Rechtsbegriffe vgl. BVerfG, Urteil vom 27.02.2008, 1 BvR 595/07 und 1 BvR 370/07, zugleich BVerfGE 120, 274, Rn. 210, m.w.N.; vgl. auch Schneider, *Gesetzgebung*, S. 45.

514 Diese Diskussion wurde bereits 2008 geführt; vgl. Hornung, *Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“*, CR 2008, 299 (305).

zumal daran zu denken wäre, dass bei Kommunikationsdaten eine bestimmte Empfängergruppe ein besonderes Vertrauensverhältnis oder eine Kernbereichsbetroffenheit widerleglich indizieren oder ausschließen könnte.

2. Bedeutung des Einsatzes von Verschlüsselung

Eine weitere spannende Frage betrifft den Einsatz von Verschlüsselungsalgorithmen. Dem bewussten Einsatz solcher Programme für eine konkrete, spezifische Datenübermittlung wird möglicherweise im Hinblick auf die Vertraulichkeit der Datenübermittlung eine andere Bedeutung zukommen, als der unbewussten und für jegliche Datenübertragung vom Dienstleister standardmäßig vorgegebenen Anwendung.

3. Auseinanderfallen von Handlung, Intention und Erwartungshaltung des Datenberechtigten

Ein weiteres Feld, das näher untersucht werden sollte, betrifft die Grenzfälle, in denen die Handlung des Datenberechtigten nicht mit seiner Erwartungshaltung korrespondiert. Dies gilt beispielsweise für versehentlich oder durch unbefugte Dritte nach außen mitgeteilte Daten oder für solche, die trotz gegenteiliger Absicht nicht an Dritte übermittelt wurden. Möglicherweise können für Teilaspekte dieser Fragen Parallelen zum untauglichen oder fehlgeschlagenen Versuch gezogen werden.

IX. Zurechenbarkeit spezieller Datensätze

Außerdem sollte ein zukünftiger Untersuchungsschwerpunkt auf der Zurechenbarkeit eines Datensatzes zu einem bestimmten Grundrechtsträger liegen.

Wenn, wie postuliert, für die Datenkategorisierung maßgeblich auf den Datenberechtigten abzustellen ist, bedarf es der Klärung, nach welchen Kriterien dieser im Internet der Dinge, namentlich bei Maschine-zu-

Maschine Kommunikation, wo die eigentliche Datenkreierung häufig nur mittelbar und unter Beteiligung mehrerer Personen initiiert wird, zu bestimmen ist.
Auch die Zuordnung von Daten, die innerhalb einer juristischen Person, eines Verbandes oder einer sonstigen Personengruppe entstehen, birgt Schwierigkeiten insbesondere dann, wenn es um die Kriterien geht, nach denen ein besonderes Vertrauensverhältnis zum Datenempfänger geprüft werden könnte.
Schließlich stellt sich die Frage nach der Zurechenbarkeit von Profildaten, die, da sie das Ergebnis einer gesonderten Algorithmus-anwendung sind, nicht ohne weiteres mit den gesammelten Einzeldaten gleichgesetzt werden können.

X. Haftungsfragen

Ergänzend und unabhängig von der Art des verwendeten Klassifikationsmodells ist zu klären, welche haftungs- und verwertungsrechtlichen Folgen eine unberechtigte oder fehlerhafte Datenübermittlung oder eine irgendwie geartete Datenmanipulation hat.

Die Beantwortung all dieser – nicht abschließenden – Fragen und Probleme erfordert ein strafprozessuales Umdenken im Hinblick auf elektronische Beweismittel und ein Sich-Einlassen auf einen neuen Denkansatz, den diese Arbeit anstoßen möchte.

Danke

Eine Dissertation schreibt man zwar für sich alleine, aber nicht ohne Begleitung. Auf meinem Weg zum Ziel wurde ich von Menschen begleitet, die dadurch einen Anteil an der Arbeit erlangten und denen ich ganz herzlich dafür danke.

Mein allererster Dank gilt Herrn Prof. Dr. Dannecker, der mir sein unbedingtes Vertrauen geschenkt und mir die perfekte Mischung aus individueller Förderung, wertvoller fachlicher Unterstützung und der Einräumung des notwendigen persönlichen Freiraumes angeboten hat - und der dabei immer den strategischen Blick für das große Ganze hatte. Ihre wertvollen Anregungen, lieber Herr Prof. Dr. Dannecker, haben die Qualität meiner Arbeit maßgeblich beeinflusst.

Außerdem danke ich Ihnen, liebe Frau Bock, die Sie mir für alle organisatorischen Fragen jederzeit so freundlich und hilfsbereit, absolut zuverlässig und äußerst kompetent zur Seite standen!

Regelmäßige „coffee breaks“ mit meinen in jeder Hinsicht außerordentlichen und großartigen Kollegen der Cybercrime Unit der Europäischen Kommission führten nicht nur zum höchst interessanten und informativen fachlichen Austausch, sondern letztlich zum konkreten Thema dieser Dissertation. Ich bin gespannt, wohin die Reise in Österreich, Finnland, Italien, Spanien und auf Malta geht!
Ein großes Dankeschön gebührt zudem den höchst kompetenten Mitarbeitern der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg und insbesondere ihrem damaligen Leiter, Herrn Tencz, für Ihre Gesprächsbereitschaft, Ihr offenes Ohr und Ihre Unterstützung – Ihre Begeisterung für alle Themen rund um Cybercrime ist ansteckend!

Keine fachliche, wohl aber herausragende moralische und tatkräftige Unterstützung habe ich durch Euch, liebe Anja und liebe Marijke, erfahren. Euer echtes Interesse an dem für Euch fachfremden

Thema und Euer uneingeschränktes und immer wieder geäußertes „Du schaffst das!“ haben mich durch die gesamte Promotionszeit getragen. Und die beste Entspannung nach einem langen Arbeits- oder Forschungstag habe ich oft genug bei einem spontanen Treffen mit Euch gefunden – Eure herzliche Gastfreundschaft ist unvergleichlich!

Unterstützt habt Ihr mich auch, liebe MiCoMa. Ich bin sehr dankbar für Eure Begeisterung für das Projekt „CW 4.0“, für Eure Nachsicht, wenn ich in Eurer Anwesenheit gedanklich tief im Cyberspace versunken war, und für Eure Geduld an unzähligen Wochenend-, Feier- und Ferientagen, an denen ich schon vor dem Frühstück am Schreibtisch saß. Ich wünsche mir, dass meine Promotion Euch eine Ermutigung dafür ist, im Leben auch mal ungewöhnliche Wege einzuschlagen und Eure Träume nicht zu früh aufzugeben – promovieren kann man auch noch mit 39 ;-)

Schließlich danke ich meinem Mann. Markus, Deinen Beitrag zu dieser Arbeit auch nur in annähernd angemessener Form zu beschreiben, würde ihren Umfang mindestens verdoppeln. Du hast initiiert, diskutiert, gelesen, gefragt, konstruktiv kritisiert, analysiert und immer wieder motiviert; Du warst geduldiger Zuhörer, IT-Berater, Personal Trainer, Lektor, Expressbote, Küchenchef, Kinderanimateur und immer, wenn es darauf ankam, da, um mir den Rücken freizuhalten. Ohne Dich hätte ich weder den Entschluss zu einer Promotion gefasst noch die Zeit und Ausdauer gefunden, sie tatsächlich umzusetzen. Kurzum: ohne Dich gäbe es diese Arbeit nicht.

Claudia Warken

Laupheim, im Juli 2019