ITeG | Interdisciplinary Research on Information System Design | 3

Paul C. Johannes | Alexander Roßnagel

Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt

ITeG Research Center for Information System Design

kassel university press

ITeG – Interdisciplinary Research on Information System Design

Band 3 / Vol. 3

Herausgegeben von / Edited by
ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung
an der Universität Kassel

Universität Kassel
ITeG Wissenschaftliches Zentrum
für Informationstechnik-Gestaltung
Pfannkuchstraße 1
D-34121 Kassel

Paul C. Johannes und Alexander Roßnagel

Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt

kassel university press

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISBN 978-3-7376-0126-9 (print)
ISBN 978-3-7376-0127-6 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737601276
URN: http://nbn-resolving.de/urn:nbn:de:0002-401275

Printed in Germany

Abschlussbericht
Pro Privacy
Teilvorhaben Recht

Fachprogramm „IKT 2020 – Forschung für Innovationen“ des Bundesministeriums für Bildung und Forschung (BMBF)

Verbundprojekt: Technische und rechtliche Untersuchung von Privatheit unterstützenden Technologien – Pro Privacy

Teilvorhaben: Recht

Projektleiter: Prof. Dr. Alexander Roßnagel

Projektgruppe für verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

März 2016

Vorwort

Gegenstand dieses Buchs ist die rechtliche Möglichkeit für Bürger und Unternehmen, ihre Grundrechte in der Digitalen Welt selbst zu schützen. Solchen Grundsatzfragen von Freiheitsgewährleistung und Sicherheit widmet sich das „Forum Privatheit – Selbstbestimmtes Leben in einer digitalisierten Welt“. Diese interdisziplinäre Forschungsplattform wird von 2014 bis 2016 vom Bundesministerium für Bildung und Forschung unterstützt, um ein interdisziplinär fundiertes, zeitgemäßes Verständnis der Rolle von Privatheit zu erarbeiten. Hieran anknüpfend werden Konzepte zur (Neu-)Bestimmung und Gewährleistung informationeller Selbstbestimmung und des Privaten in der digitalen Welt erstellt. Zugleich versteht sich das Forum Privatheit als eine Plattform für den fachlichen Austausch und erarbeitet Orientierungswissen für den öffentlichen Diskurs.

Im Rahmen des Forums Privatheit untersuchte ein Explorationsprojekt die Frage, wie der Einzelne seine Grundrechte durch Selbstschutztechniken besser schützen kann. Das Projekt „Pro Privacy“ wurde von November 2014 bis zum April 2015 von Informatikern des Fraunhofer-Instituts für Sicherheit in der Informationstechnik (SIT) in Darmstadt und Juristen der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel durchgeführt.

Das Teilvorhaben Recht des Explorationsprojekts „Pro Privacy“, dessen Abschlussbericht hiermit vorgelegt wird, untersuchte konzeptionelle Mittel für die zukünftige Entwicklung neuer Technologien zum Selbstdatenschutz und ihre staatliche Förderung durch gesetzgeberische Maßnahmen. Hierfür wurde ein interdisziplinär angelegtes Arbeits- und Forschungsprogramm in Zusammenarbeit mit dem Fraunhofer SIT verfolgt, um die rechtlichen Grundlagen für eine gezielte Förderung des Selbstdatenschutzes zu erarbeiten.

Kassel, März 2016 *Alexander Roßnagel*

Übersicht

1 Ausgangslage und Zielsetzung

Im Juni 2013 begannen die britische Zeitung The Guardian und die amerikanische Zeitung The Washington Post, geheime Dokumente der amerikanischen National Security Agency (NSA) zu veröffentlichen. Die von *Edward Snowden* zur Verfügung gestellten Dokumente zeichnen das Bild eines weltweiten Netzes von Spionagesystemen, bei dem die amerikanische NSA, die britischen Government Communications Headquarters (GHCQ) und ihre Partnerdienste jede Form elektronischer Kommunikation überwachen.[1] Bekannt geworden ist auch, dass der Bundesnachrichtendienst (BND) Programme der NSA nutzt und Daten an diese weitergegeben hat.[2] Die Debatte über die NSA-Ausspähung wird auf politischer,[3] juristischer[4] und technischer[5] Ebene geführt. Der Sachverhalt steht dabei immer unter dem Vorbehalt, dass er aus Veröffentlichungen zusammengesetzt werden muss, deren Quellen Presseberichte und Angaben aus politischen Kreisen sind. Der Bundestag bemüht sich durch einen Untersuchungsausschuss um Aufklärung.[6] Er soll Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären.[7] Ziel der

---

1 *Greenwald* 2014; Zusammenfassungen zur NSA-Spähaffäre bei http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal; www.heise.de/thema/NSA.

2 *Leyendecker/Mascolo*, „Gedränge am Daten-Drehkreuz", SZ vom 1.6.2014, www.sueddeutsche.de/digital/geheimdienst-kooperation-gedraenge-am-daten-drehkreuz-1.2016514.

3 *Leupold,* MMR 2014, 145; *Schaar,* ZRP 2013, 214; *Schellenberg*, AnwBl. 2013, 631; *Voss*, ZD 2014, 218.

4 *Ewer/Thienel*, NJW 2014, 30; *Hoffmann-Riem,* JZ, 53; *ders.*, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014, MAT-A SV 2/1 zu Ausschuss-Drs. 54; *Hoffmann/Schulz/Borchers,* MMR 2014, 89; *Kipker/Voskamp*, RDV 2014, 84; *Papier*, Gutachterliche Stellungnahme Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des deutschen Bundestags 18. Wahlperiode, MAT-A SV 2/2 zu Ausschuss-Drs. 54; *Roos*, K&R 2013, 769; *Roßnagel/Jandt/Richter*, DuD 2014, 545; *Schmahl*, JZ 2014, 220; *Wolf*, JZ 2013, 1039.

5 *Hansen*, DuD 2014, 439; *Pohlmann*, DuD 2014, 47; *Ruhmann*, DuD 2014, 40; *Saeltzer*, DuD 2014, 333; *Waidner*, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014, MAT-A SV 1/2 zu Ausschuss-Drs. 53.

6 Das Gremium wurde auf Antrag aller Bundestagsfraktionen eingesetzt.

7 BT-Drs. 18/843; s. auch http://www.bundestag.de/bundestag/ausschuesse18/ua/.

umfassenden NSA-Überwachung ist die Kontrolle aller digitalen Kommunikationsinhalts- und -metadaten im gesamten Internet.[8] Ausgedrückt in Datenkategorien des deutschen Rechts werden sowohl Bestands- und Verkehrsdaten nach Telekommunikationsgesetz (TKG), Bestands- und Nutzungsdaten nach Telemediengesetz (TMG) als auch Inhaltsdaten nach Bundesdatenschutzgesetz (BDSG) anlasslos gesammelt und auf unbestimmte Zeit zentral von der NSA gespeichert.

Gerade in Deutschland trifft die Erkenntnis, dass auf internationaler Ebene massenhaft Daten ausgespäht werden, auf deutlichen Widerstand. Viele Menschen demonstrierten gegen diese Überwachung, nahezu alle Kommentare in Medien und Presse protestierten gegen diese flächendeckende und anlasslose Ausspähung. Sogar Innenminister Friedrich riet deutschen Unternehmen und Bürgern, ihre Internetkommunikation zu verschlüsseln.[9] Andere Regierungsmitglieder rechtfertigten dagegen nicht nur die Ausspähaktionen der NSA, sondern auch die nationalen Überwachungsmaßnahmen insbesondere des Verfassungsschutzes als notwendige Maßnahmen zum Schutz der Bevölkerung vor Terrorismus und organisierter Kriminalität.[10] Die Diskussionen um die Ausspähaktionen betrifft im Kern die Frage der Ausbalancierung der gesellschaftlichen Grundwerte der Sicherheit und Freiheit.[11]

Diesen Grundsatzfragen widmet sich das „Forum Privatheit – Selbstbestimmtes Leben in einer digitalisierten Welt".[12] Im Rahmen des Forums Privatheit wurde das Explorationsprojekt „Pro Privacy" gefördert, das die Frage untersuchte, wie der Einzelne seine Grundrechte durch Selbstschutztechniken besser schützen kann. In diesem Projekt

---

8 *Rosenbach/Stark* 2014, 124.

9 Spiegel-Online vom 16.7.2013, http://www.spiegel.de/politik/deutschland/friedrich-fordert-deutsche-zu-mehr-datenschutz-auf-a-911445.html

10 S. z.B. Kanzleramtsminister Pofalla, Youtube, 13.8.2013: NSA: Merkelsprecher Pofalla erklärt das illegale Abhören für legal, www.youtube.com/watch?v=H1cz6xLqkEc.

11 S. hierzu ausführlich *Roßnagel* 2003a, 17 ff.

12 www.forum-privacy.de.

wurden Anforderungen an die Gewährleistung des Schutzes der Privatheit in der digitalen Welt aus der technischen[13] und rechtlichen Perspektive erforscht. Hierfür wurden die Sicherheitsbedürfnisse der Bevölkerung und Wirtschaft vor dem Hintergrund der bekannt gewordenen Bedrohung der weltweiten Ausspähung konkretisiert. Vor diesem Hintergrund wurde das Verständnis von Privatheit in der digitalen Welt bestimmt. Dies erfolgt aus der verfassungsrechtlichen Perspektive, da die Grundrechte die Grundlage für den gesellschaftlichen Konsens über das Sicherheitsbedürfnis zum Schutz der Privatheit bieten.

Des Weiteren wurden konkrete technische und rechtliche Fragestellungen beantwortet. Untersucht wurde, warum existierende Technologien zur Förderung der Privatheit (zum Beispiel Privacy Enhancing Technologies, PETs) nur selten eingesetzt werden, obwohl sie teilweise schon dreißig Jahre in der Wissenschaft bekannt sind. Außerdem wurde untersucht, welche Kriterien Informationstechnik erfüllen müssen, um eine hohe Nutzerakzeptanz zu erfahren. Auch wurden Konzepte für Informationstechniken gesucht oder auch für neue Techniksysteme definiert, die gerade diese Kriterien erfüllen. Die Konzepte wurden technisch in Bezug auf ihre Umsetzbarkeit und Zielerreichung evaluiert. Sie wurden juristisch insbesondere in Bezug auf ihre Eignung zur Erfüllung verfassungsrechtlicher Vorgaben, die rechtlichen Voraussetzungen zu ihrer Umsetzung, insbesondere ihre Konformität zum Datenschutzrecht, die Notwendigkeit gesetzlicher Pflichten für Infrastrukturanbieter sowie haftungsrechtliche Konsequenzen untersucht und bewertet.

Die Grundrechte in der digitalen Welt sowie insbesondere die Vertraulichkeit von personenbezogenen Daten sind vielfältigen Risiken ausgesetzt. Um technische Konzepte für konkrete Anwendungsberei-

[13] S. hierzu den Abschlussbericht des Teilprojekts Technik *Hahn/Herfert/Lange* 2015.

che zu entwickeln, fokussiert die Untersuchung auf die Kommunikationsbereiche

- Kommunikationsinhalte ,
- Verbindungsdaten,
- Positionsbestimmung und
- Smart Home.

Dadurch konnte die rechtlich unterschiedlich zu bewertende Schutzintensität der in diesen Kommunikationsbereichen anfallenden Daten untersucht werden.

Aufgrund dieser Kriterien wurden existierende technische Konzepte zur Förderung der Privatheit in den vier Kommunikationsbereichen evaluiert. Die unterschiedliche Konzepte und Techniken zur Verbesserung der Verwirklichungsbedingungen der Grundrechte des Endnutzers in den vier Kommunikationsbereichen lassen sich jedoch nicht einheitlich bewerten. Abhängig vom Einsatzaufwand und der Stelle der Implementation im Kommunikationsnetz sind zum Beispiel unterschiedliche Grade der Stärkung von informationeller Selbstbestimmung feststellbar. So kann die Anonymität des Endnutzers in der Regel durch diesen selbst hergestellt werden, zumeist aber nur mit etwas Aufwand und unter Einbuße von Performanz oder Nutzungsmöglichkeiten. Mit einer entsprechenden Implementation der Konzepte und Techniken bereits auf Seiten der Telekommunikations- und Telemedienanbieter würden jedoch verfassungsrechtliche Vorgaben besser erfüllt und ein höherer Grad an Rechtsverträglichkeit erreicht. Entsprechendes gilt für die Einhaltung von geltendem Datenschutzrecht. Durch die Techniken können Anonymität und Pseudonymität der Endnutzer gegenüber den Diensteanbietern und Dritten hergestellt werden Festgestellt werden konnte auch, dass der Einsatz von Techniken zum Selbstdatenschutz für den Endnutzer in der Regel rechtlich zulässig ist und ihm durch deren Einsatz keine rechtlichen Nachteile erwachsen und erwachsen dürfen. Um Selbstdatenschutz und damit

Selbstbestimmung in allen vier Kommunikationsbereichen zu ermöglichen und zu verbreiten wurden in Pro Privacy Forschungsfragen dahin gehend formuliert, inwiefern Diensteanbieter verpflichtet werden können, solche Angebote in ihre Dienste einzubinden.

2 Rechtliche Grundlagen der Privatheit

Vor dem Problemhintergrund massenhafter gesellschaftlicher Ausspähung ist im Folgenden als erster Schritt das Verständnis von Privatheit in der digitalen Welt zu bestimmen. Dies hat aus verfassungsrechtlicher Perspektive zu erfolgen, da die Grundrechte die Grundlage für den gesellschaftlichen Konsens über das Sicherheitsbedürfnis zum Schutz der Privatheit bieten.

Zu beantworten ist auch die Frage, ob und in welchem Umfang ein verfassungsrechtlicher „Anspruch" auf Selbstdatenschutz auch gegenüber außerstaatlichen Stellen besteht.

2.1 Hoheitliche Handlungsverpflichtung

Angesichts der verschiedenen Überwachungsmaßnahmen fühlt sich ein großer Teil der Bevölkerung in seiner „Privatheit" betroffen. Dieser umgangssprachliche Begriff ist jedoch im Grundgesetz nicht zu finden.[14] Privatheit ist buchstäblich kein deutsches Grundrecht. Auch auf europäischer und internationaler Ebene gibt es kein ausdrücklich verbrieftes Recht zur Gewährleistung von Privatheit. So findet sich in den europäischen Rechtsgrundlagen zwar ein Recht auf Achtung des „Privatlebens" in Art. 8 Europäische Menschenrechtskonvention (EMRK) und Art. 7 Charta der Grundrechte der Europäischen Union (GRC) sowie ein grundrechtlich garantiertes Recht auf Schutz personenbezogener Daten in Art. 8 GRC und Art. 16 Vertrag über die Arbeitsweise der europäischen Union (AEUV), nicht aber ein Recht auf „Privatheit".

Im Grundgesetz ist an keiner Stelle ein Recht auf Privatheit, Privatsphäre oder Privatleben oder Schutz personenbezogener Daten verschriftlicht. Dennoch garantieren Einzelgrundrechte mit jeweils verschiedenen Schutzbereichen punktuell Privatheits- und Geheimnisgewährleistungen.[15] Sie beinhalten für bestimmte Situationen Un-

---

14 *Geminn/Roßnagel*, JZ 2015, 703; *Nebel*, ZD 2015, 517.

15 Bezüglich Selbstdatenschutz s. *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 9 ff.

verletzlichkeits-, Schutz- und Freiheitsversprechen und wahren damit die Selbstbestimmung des Einzelnen.[16] Zu diesen Grundrechten zählen

- das allgemeine Persönlichkeitsrecht,[17]
- das Recht auf Privatsphäre,[18]
- das Recht auf informationelle Selbstbestimmung,[19]
- das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (kurz Computergrundrecht),[20]
- das Fernmeldegeheimnis[21] sowie
- das Recht auf Unverletzlichkeit der Wohnung.[22]

Aber auch andere Grundrechte enthalten einen Abwehranspruch, der in bestimmten Situationen Privatheit gewährleistet. So gewährleistet zum Beispiel die Glaubens- und Gewissensfreiheit nach Art. 4 GG sowohl als negative Religionsfreiheit das Recht, keine Religion haben oder ausüben und sich nicht zu seiner Religion erklären zu müssen als auch das Recht, seine Religion für sich und abgeschottet von öffentlicher Anteilnahme ausüben zu können.[23]

Das, was allgemein unter „Privatheit" verstanden wird, schützt das Recht durch das Zusammenspiel verschiedenster Abwehrrechte. Als Begriff ist „Privatheit" deswegen für die juristische Auseinandersetzung konturenlos und wenig brauchbar. Schließlich geht es gerade darum zu bestimmen, was privat ist. Dies erfordert eine Abgrenzung. Aus Sicht des Einzelnen kann nur er bestimmen, was in Bezug auf ihn privat sein soll. Alles andere wäre Fremdbestimmung. Die vorgenann-

---

16 Zu Privatheit als Inhalt vieler grundrechtlicher Schutzfunktionen siehe z.B. *Albers*, DVBl. 2010, 1061; *Geminn/Roßnagel*, JZ 2015, 703; *Nebel*, ZD 2015, 517

17 Folgt aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, s. BVerfGE 35, 202.

18 Folgt aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, s. BVerfGE 27, 344.

19 Folgt aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, s. BVerfGE 65, 1.

20 Folgt aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, s. BVerfGE 120, 274.

21 Art. 10 GG.

22 Art. 13 GG.

23 *Morlok*, in: Dreier 2013, Art. 4 GG, Rn. 69.

ten Grundrechte entfalten in der Regel aber nur Wirkung dadurch, dass der Grundrechtsträger einen Lebensvorgang oder Lebensaspekt als privat und damit getrennt von der Öffentlichkeit definiert. [24]

Aus der Sicht des Individuums, also des einzelnen Grundrechtsträgers, ist es deswegen zielführender bezogen auf den Umgang mit seinen personenbezogenen Daten von informationeller Selbstbestimmung zu sprechen. Die vom Bundesverfassungsgericht im Volkszählungsurteil gewählte Terminologie hebt die Entwicklungsoffenheit des allgemeinen Persönlichkeitsrechts in Abgrenzung zum bis dahin üblichen Schutz der „Privatsphäre" hervor.[25] Die informationelle Selbstbestimmung betont die Gefährdung der Integrität des speziell durch umfassende Techniken der Datenspeicherung und Datenvernetzung aller Grundrechtsträgers. Das Recht auf informationelle Selbstbestimmung will Garantie der Entscheidungsfreiheit des Menschen sein: Denn „wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das mögliche Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[26] Die Entscheidungs- und Entfaltungsfreiheit kann auch bezüglich anderer Grundrechte nur unter dem Aspekt der Selbstbestimmung gewahrt werden.

Die Spähaktionen der NSA und anderer Nachrichtendienste greifen in die Grundrechte aller Internetnutzer ein.[27] Das Abhören von Internet-

---

24 S. hierzu näher *Geminn/Roßnagel*, JZ 2015, 707f.

25 *Di Fabio*, in: Maunz/Dürig, 72. Ergl., 2014, Art. 2 GG, Rn. 173; *Geminn/Roßnagel*, JZ 2015, 703 ff.; *Nebel*, ZD 2015, 517 ff.

26 BVerfGE 65, 1 (42f.).

27 S. z.B. *Roßnagel/Jandt/Richter*, DuD 2014, 546 f.; *Forum Privatheit*, Whitepaper Selbstdatenschutz, 2014.

telefonie mit HAMMERCHANT[28] und das Abfangen von E-Mails und SMS über TEMPORA, RAMPART-A[29] und DISHFIRE[30] greifen in das Fernmeldegeheimnis aus Art. 10 GG ein. Die Erhebung von Verkehrs-, Bestands- und Nutzungsdaten über PRISM[31] und das Erstellen von Profilen über XKEYSCORE[32] greifen in das allgemeine Persönlichkeitsrecht, speziell in das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG[33] ein. Manipulierte Verschlüsselungstechnik[34] und der Einbau von Hintertüren in Betriebssysteme von Smartphones[35] sind Eingriffe in das Grundrecht auf Vertraulichkeit und Integrität eigengenutzter Systeme nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.[36]

Diese Grundrechtseingriffe konnten nicht gerechtfertigt werden. Der NSA-Direktor begründete die Spähaktionen mit dem 11. September 2001 und den seitherigen islamistischen Terroranschlägen und Anschlagsversuchen.[37] Mithilfe der Überwachung seien in den letzten

---

28 HAMMERCHANT dient zur Überwachung von VoIP-Gesprächen, s. *Gallagher/ Greenwald*, „How the NSA Plans to Infect Millions of Computers with Malware", The Intercept vom 12.3.2014, https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/.

29 TEMPORA und RAMPART-A sammeln alle Daten, die über transatlantische Glasfaserkabel gesendet werden, s. *Rosenbach/Stark* 2014, 124 ff.

30 Mit DISHFIRE werden täglich Millionen von SMS abgegriffen und ausgewertet, s. *Ball*, „NSA collects millions of text messages daily in 'untargeted' global sweep", The Guardian, 16.1.2014, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

31 Über PRISM werden Google, Apple, Facebook, Microsoft und andere gezwungen, Nutzerdaten herauszugeben, *Greenwald* 2014, 160 ff.

32 Mit XKEYSCORE können aus den riesigen Datenbanken der NSA in einem Such- und Analyseverfahren Profile zu einzelnen Personen angelegt werden, *Greenwald* 2014, 221 ff.

33 Zum Grundrecht BVerfGE 65, 1.

34 *Gallagher/Greenwald*, „How the NSA Plans to Infect Millions of Computers with Malware", The Intercept vom 12.3.2014, https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/.

35 *Rosenbach/Stark* 2014, 183 ff.

36 Zum Grundrecht BVerfGE 120, 274.

37 *Rosenbach/Stark* 2014, 118.

Jahren 54 Anschläge verhindert worden.[38] Diese Behauptung dient der nachträglichen Rechtfertigung und ist nicht belegt. Selbst wenn jedoch diese Angaben stimmen sollten und die Maßnahmen, die Chancen erhöhen würden, solche Angriffe zu verhindern, stünden diese Chancen außer Verhältnis zum verfassungswidrigen Verlust an Selbstbestimmung und freier Entfaltung der Persönlichkeit, der allen Nutzern des Internets weltweit hierfür abverlangt wird.[39]

Aufgrund der allumfassenden Überwachung und Sammlung von Metadaten können äußert genaue Persönlichkeitsprofile erstellt werden. Das Bedrohungspotenzial ist enorm und wird in den folgenden Kapiteln unter den einzelnen Kommunikationsbereichen dargelegt.[40]

Beispielshaft sei hier auf Folgendes verwiesen: Zu den bei der E-Mail-Kommunikation anfallenden Verbindungsdaten gehören unter anderem die Adressen von Empfänger und Sender, der Betreff und die Sendezeit. Durch eine Analyse dieser Daten können soziale Gruppen erkannt und Beziehungsgraphen erstellt werden. Auch die Art der Beziehung zu den Kontakten kann anhand der Häufigkeit der Kommunikation abgeschätzt werden. Kann bei der Analyse ein längerer Zeitraum untersucht werden, können auch besondere Ereignisse im Leben des Nutzers, wie zum Beispiel der Wechsel zu einer anderen Firma, erkannt werden. Forscher des MIT haben mit Immersion[41] ein online verfügbares Tool veröffentlicht, mit dem jeder diese Analysen für seinen eigenen E-Mail-Account durchführen kann. Die Ergebnisse der Analysen ermöglichen eine genaue Beschreibung des sozialen Umfelds des Nutzers, auch ohne die Inhalte der E-Mails zu betrachten. In Tests wurden die Kontakte zum größten Teil in die richtigen Gruppen

---

38 *Fischer*, „NSA-Anhörung in US-Senat“, SPON vom 31.7.2013, http://www.spiegel.de/politik/ausland/us-senatoren-kritisieren-geheimdienst-nsa-und-keith-alexander-a-914205.html.

39 Für die Vorratsdatenspeicherung EuGH, Urteil vom 8.4.2014, Az. C-293/12 u. C-594/1 = DuD 2014, 488.

40 Ausführlich wird es auch in *Hahn/Herfert/Lange* 2015 beschrieben.

41 S. https://immersion.media.mit.edu/.

(Studium, Freunde, Jobs) eingeteilt und der von Immersion ermittelte Graph entsprach zu einem hohen Grad den tatsächlichen sozialen Verbindungen.

Bei der Mobilkommunikation gibt es zusätzliche Möglichkeiten, die Nutzer anhand der Verbindungsdaten zu analysieren. Da ein Mobiltelefon immer in eine Basisstation eingebucht sein muss, kann hierüber die ungefähre Position des Nutzers bestimmt werden, da die Basisstationen eindeutig identifizierbar sind und deren Position bekannt ist.[42] Anhand bestimmter Bewegungs-Muster kann auch direkt auf das Verhalten des Nutzers geschlossen werden. Google bietet zum Beispiel als Teil seines „Google Now"-Dienstes die Möglichkeit, über die Sensoren im Mobiltelefon automatisch zu erkennen, wann und wo der Nutzer sein Auto geparkt hat, um ihn später wieder zu dieser Stelle zurück zu führen.[43] Werden Daten dieser Art über einen längeren Zeitraum erfasst, können genaue Bewegungsprofile des Nutzers erstellt werden. Indem die so erstellten Bewegungsprofile vieler Nutzer miteinander verglichen werden, lassen sich auch bisher noch unbekannte Verbindungen zwischen Nutzern erkennen, zum Beispiel wenn diese sich über einen bestimmten Zeitraum auf den gleichen Wegen befinden. Dieses Verfahren wird von der NSA im Rahmen des CO-TRAVELER Programms[44] eingesetzt, wobei zusätzlich zur Bewegung noch weitere Auswahlkriterien zum Einsatz kommen. Der deutsche Politiker *Malte Spitz* hat 2011 die bei der Telekom von ihm gespeicherten Verbindungsdaten angefragt und öffentlich zur Verfügung gestellt. Indem die Daten mit anderen, ebenfalls frei verfügbaren Informationen verknüpft wurden, ergab sich ein sehr detailliertes Bild seines Lebens.[45]

---

42 Genauigkeit in Großstädten bis zu 200 Meter bei einzelner Messung.

43 S. https://support.google.com/websearch/answer/6015842?hl=en.

44 Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program.

45 *Biermann*, „Was Vorratsdaten über uns verraten", zeit online vom 24.2.2011, www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz.

Diese Beispiele verdeutlichen, dass die Grundrechtseingriffe durch die NSA-Spähprogramme unverhältnismäßig sind. Die genannten Grundrechte, die für ein selbstbestimmtes Leben in der digitalen Welt entscheidend sind, stehen allen Menschen zu; es sind Jedermanns-Rechte,[46] die weder territorial[47] noch auf eine bestimmte Nationalität des Betroffenen beschränkt sind. Aus deutscher Sicht kann daher dahinstehen, ob die Eingriffe nach geltendem Recht der USA legal sind.[48] Die Vorratsdatenspeicherung, also die Speicherung nur von Verkehrsdaten für einen bestimmten Zeitraum dezentral bei Diensteanbietern, wurde vom Bundesverfassungsgericht lediglich unter sehr engen Voraussetzungen als noch mit dem Grundgesetz vereinbar gehalten.[49] Der Europäische Gerichtshof hält die flächendeckende und anlasslose Vorratsdatenspeicherung mit der Europäischen Grundrechtecharta sogar für ganz und gar unvereinbar und erklärte die europäische Richtlinie dazu für nichtig.[50] Gegen die seit dem 18.12.2015 wieder in Deutschland eingeführte Vorratsdatenspeicherung bestehen erhebliche Bedenken, ob sie mit der Rechtsprechung des Europäischen Gerichtshofs vereinbar ist.[51] Die zentrale, anlasslose, dauerhafte und allumfassende Speicherung von Kommunikationsdaten durch die NSA und andere Geheimdienste ist nach diesen Kriterien ein sehr schwerwiegender, unverhältnismäßiger und nicht zu rechtfertigender Eingriff in die Grundrechte aller Internetnutzer.

---

46 S. *Kloepfer* 2010, § 49, Rn. 13.

47 S. auch Art. 33 Abs. 1 GG.

48 *Wolf*, JZ 2013, 1039 (1040) stellt Legalität nach US-Recht fest; zur Unvereinbarkeit mit internationalem Recht s. *Ewer/Thienel*, NJW 2014, 30 (31).

49 BVerfGE 125, 260; s. auch *Roßnagel*, NJW 2010, 1238.

50 EuGH, Urteil vom 8.4.2014, Az. C-293/12 u. C-594/1 = DuD 2014, 488.; s. auch *Roßnagel*, MMR 2014, 372.

51 Ausführlich *Roßnagel*, NJW 2016, 533.

2.2 Staatliche Schutzpflichten

Ausländische Staaten, wie die USA oder Großbritannien, sind nicht an das deutsche Grundgesetz gebunden.[52] Die Grundrechte binden aber die Bundesrepublik Deutschland und verpflichten sie – Exekutive, Legislative und Judikative – zum Handeln.[53]

Grundrechte sind in erster Linie Abwehrrechte des Bürgers gegen staatliche Eingriffe in seinen Freiheitsbereich und begründen Unterlassungs- und Beseitigungsansprüche. Diese ursprüngliche Funktion der Grundrechte steht auch heute noch im Vordergrund. Sie wird allerdings durch weitere Grundrechtsfunktionen und die Einwirkung der Grundrechte auf den gesellschaftlichen und privaten Bereich ergänzt. So gelten auch grundrechtliche Schutzpflichten.[54] Diese verpflichten den Staat, die in den Grundrechten gewährleisteten Rechtsgüter gegen Beeinträchtigungen oder Gefährdungen durch Dritte zu schützen.[55] Die Schutzpflichten gelten nicht nur dem Verhalten (anderer) privater Akteure. Sie können auch durch das Verhalten anderer Staaten ausgelöst werden.[56] Die Schutzpflichten können es gebieten, Gesetze so auszulegen und zu gestalten, dass die Gefahr von Grundrechtsverletzungen eingedämmt wird.[57] Adressat der Schutzpflicht ist nicht der störende Dritte, sondern der deutsche Staat, der sich schützend zwischen Angreifer und Angegriffenen stellen muss.[58] Da der Staat im Interesse der Friedenssicherung das Gewaltmonopol für sich in Anspruch nimmt, muss er den Bürger gegen Eingriffe, auch anderer Staaten, schützen.

---

52 BVerfGE 66, 39 (56 f.); s. *Kloepfer* 2010, § 50, Rn. 65 f.
53 Überblick bei *Klein*, JuS 2006, 960.
54 S. *Kloepfer* 2010, § 48, Rn. 55 f.
55 BVerfGE 39, 1 (41).
56 S. BVerfGE 14, 192 (199f.); *Kloepfer* 2010, § 48, Rn. 57; *Ewer/Thienel*, NJW 2014, 30 (34); *Hoffmann-Riem*, JZ 2014, 53 (56); *Roßnagel/Jandt/Richter*, DuD 2014, 546.
57 BVerfGE 49, 89 (1429); 88, 203 (251).
58 *Maurer* 2010, § 9, Rn. 25.

Das Bundesverfassungsgericht hat bisher konkret Schutzpflichten vor allem aus Art. 2 Abs. 2 GG angenommen, also Pflichten die letztlich auf den Erhalt der Gesundheit und des Lebens abzielen.[59] Grundrechtliche Schutzpflichten lassen sich, vor allem im Angesicht einer konkreten Bedrohung, aber auch aus anderen Grundrechten ableiten.[60] So gilt nach ausdrücklicher Bestätigung durch das Bundesverfassungsgericht das Fernmeldegeheimnis auch als objektiv-rechtliches Prinzip.[61] Daraus lässt sich eine Schutzpflicht ableiten,[62] die sich insbesondere auch gegen die Tätigkeit ausländischer Staaten und deren Nachrichtendienste richtet.[63] Aber auch das Recht auf informationelle Selbstbestimmung[64] und das Recht auf Integrität informationstechnischer Systeme schützen die freie Entfaltung der Persönlichkeit und damit sowohl das Individuum als auch die Gemeinschaft. Auch aus ihnen lassen sich Schutzpflichten ableiten.

Aus anlassloser, allumfassender Überwachung von Konsum-, Informations- und Kommunikationsverhalten im Internet sowie weiteren gespeicherten Daten und der Profilbildung daraus folgt zwangsweise, dass die freie Entfaltung der Persönlichkeit Einzelner gestört wird.[65] Der massenhafte Eingriff in Individualrechte stört mittelbar auch das Gemeinwesen. Die Totalüberwachung des Internet ist besonders gefährlich, da es in den westlichen Informationsstaaten der Gegenwart

---

59 S. BVerfGE 39, 1(42) zum Schwangerschaftsabbruch; BVerfGE 49, 78 (141 f.) zur Sicherung von Atomkraftwerken; BVerfGE 56, 54 ff. zu Fluglärm.

60 S. z.B. BVerfGE 75, 40 (63); 90 107 (115) zum Recht der Errichtung privater Schulen sowie BVerfGE 84, 133 (146f.) und 92, 140 (150) zur freien Berufswahl.

61 BVerfGE 67, 157 (185); 125, 260 (339).

62 BVerfGE 106, 28 (37).

63 Das BVerfG hat das Vorliegen einer Schutzpflicht angenommen, wenn die Maßnahmen einer fremden Hoheitsgewalt gegenüber Deutschen oder in Deutschland Wirkung entfalteten, s. BVerfGE 55, 349 (364 ff.); 77, 170 (215).

64 Ausführlich *Kipker/Voskamp*, RDV 2014, 84.

65 Schon nach BVerfGE 27, 1 (6) lässt sich die erzwungene Registrierung und Katalogisierung der gesamten Persönlichkeit nicht mit der Menschenwürde vereinbaren; nach BVerfGE 125, 260 (324) gehört zur verfassungsrechtlichen Identität der BRD, dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf.

ubiquitär und pervasiv ist.[66] Der Territorialstaat, der diese Schutzpflichten in weltweiten Netzen zu erfüllen versucht, wird jedoch leicht mit Ohnmachtserfahrungen konfrontiert,[67] da seine Gebietshoheit territorial beschränkt ist. Die Machtlosigkeit der Bundesrepublik Deutschland und der Europäischen Union gegenüber der Massenausspähung durch die Geheimdienste der USA nach den Enthüllungen durch *Snowden* haben dies verdeutlicht.

Das Bundesverfassungsgericht gewährt dem Gesetzgeber und der Exekutive einen weiten Einschätzungs- und Wertungsspielraum für die Frage, wie sie ihren Schutzpflichten nachkommen.[68] Es stellt nur dann die Verletzung einer Schutzpflicht fest, „wenn die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder erheblich dahinter zurückbleibt".[69] Nur wenn dieses Untermaß verletzt ist, entsteht dem einzelnen Bürger ein einklagbarer Schutzanspruch.[70] Selbst dann bleibt aber noch offen, welche positiven Schutzmaßnahmen zu treffen sind. Aus den genannten Grundrechten erwächst dem Staat eine verfassungsrechtliche Schutzpflicht gegen rechtswidrige Datenerhebung. Da die Schutzpflichten am Schutzgut orientiert sind, ist es ist unerheblich, von wem eine Beeinträchtigung ausgeht. Allerdings hat der Staat bei der Auswahl der zu treffenden Maßnahmen die Möglichkeit, die nach seiner Einschätzung geeigneten Maßnahmen – auch dem Angreifer entsprechend – auszuwählen. Aus einer Schutzpflicht entsteht in der Regel keine bestimmte verfassungsrechtliche Handlungsvorgabe.

---

66 *Roßnagel*, NJW 2010, 1242.
67 *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 18.
68 BVerfGE 77, 170 (214f.); 79, 174 (202); BVerfG, NVwZ 2011, 991 (993).
69 BVerfGE 92, 26, 46 mit Hinweis auf frühere Entscheidungen.
70 *Dreier*, in: ders. 2013, Vorb. Rn. 103.

Die grundrechtliche Schutzpflicht, die sich aus den genannten Grundrechten ergibt, wird bereits in zahlreichen Gesetzen ausgestaltet und erfüllt.[71] Zu denken ist insbesondere an das Bundesdatenschutzgesetz, das Strafgesetzbuch und die Buß- und Strafvorschriften in Telekommunikationsgesetz und Telemediengesetz. Dass diese Vorschriften jemals gegen einen Mitarbeiter der NSA vollzogen werden können, ist unwahrscheinlich.[72] Die Bundesregierung befindet sich wegen der NSA-Ausspähung im „Cyber-Dialog" mit den USA, Verhandlungen über ein No-Spy-Abkommen sind allerdings gescheitert.[73] Ein durchgreifender Erfolg bei der Eindämmung der konkreten geheimdienstlichen Massenausspähung durch die NSA konnte nicht erzielt werden.[74]

Zur Erfüllung der Schutzpflichten stehen Deutschland dennoch viele technische und gesetzgeberische Mittel zur Verfügung. Bestimmte technische Maßnahmen zur Verhinderung von Verletzungen der vorgenannten Grundrechte durch die Ausspähung im Internet müsste Deutschland zur Erfüllung seiner Schutzpflichten aber nur dann ergreifen, wenn sie auch Erfolg versprechen und, unter Wahrung ökonomischer und rechtlicher Verhältnismäßigkeit, realistisch umsetzbar sind.[75] Dabei genügt für den Erfolg auch schon eine Beschränkung oder Verringerung der Überwachung. Diskutiert wurde zum Beispiel die Sicherung durch ein Routing der Internetkommunikation innerhalb Deutschlands oder Europas, das auf Deutschland oder die Schengen-Staaten begrenzt ist.[76] Aber auch wenn der Staat nur wenig Handlungsspielraum sieht, sich selbst schützend vor die Grundrechte seiner Bürger zu stellen, ist er zumindest verpflichtet, ihnen die Möglichkei-

---

71 S. *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 25 ff..

72 *Schmahl*, JZ 2014, 220.

73 „Cyber Dialog statt No-Spy-Abkommen", N24.de vom 28.2.2014, www.n24.de/n24/Nachrichten/Politik/d/4355974/-cyber-dialog--statt-no-spy-abkommen. html.

74 *Schmahl,* JZ 2014, 220, stellt klar, dass dies auch am Fehlen effektiver zwischenstaatlicher Rechtschutzmöglichkeiten liegt; *Wolf*, JZ 2013, 1039, sieht einen besatzungsrechtlichen Nebel in den Rechtsbeziehungen zwischen USA und BRD.

75 *Kipker/Voskamp*, RDV 2014, 84 (85).

76 *Hansen*, DuD 2014, 439 (443); *Geminn*, MMR 2015, 98

ten und Rahmenbedingungen zu bieten, sich selbst zu schützen. Auch wenn er nicht seiner Erfüllungsverantwortung gerecht werden kann, bleibt noch immer seine Gewährleistungsverantwortung für den Schutz der Grundrechte.[77] Diese ist für den Datenschutz im Internet zumindest als eine Infrastrukturverantwortung zu verstehen.[78] Dies bedeutet, dass der Staat dem Bürger infrastrukturelle Voraussetzungen bieten muss, damit dieser überhaupt eigenverantwortlich handeln kann. Selbstbestimmung, auch im grundrechtlichen Sinne, setzt die Möglichkeit voraus, sich für Selbstschutzmaßnahmen entscheiden zu können.[79]

Am einfachsten wäre es, solche Mittel zu nutzen, die von den Grundrechtsträgern selbst eingesetzt werden können, ohne dass es weiterer staatlicher Leistung im konkreten Einzelfall bedarf. Die Aufgabe des Staates bestünde dann darin, über diese Mittel in genügender Weise aufzuklären und die gesetzlichen Rahmenbedingungen so auszugestalten, dass die Verbreitung dieser Techniken möglichst einfach und ungehindert erfolgen kann. Darüber hinaus wird der Staat aber auch gewährleisten müssen, dass die für die Selbstschutztechniken notwendige Infrastruktur entsteht.[80]

2.3 Schutz des Selbstschutzes durch Grundrechte

Der umgangssprachliche Begriff der Privatheit ist für den Rechtsschutz in der digitalen Welt untauglich. Vielmehr ist das meiste, was mit diesem Begriff verbunden wird, rechtlich durch unterschiedliche Grundrechte geschützt. Sie enthalten individuelle Freiheitsgarantien und korrespondierende subjektive (Schutz-)Rechte. Aus Grundrechten, wie dem Brief-, Post und Fernmeldegeheimnis (Art. 10 GG), dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) sowie dem Recht auf Gewährleistung

---

77 S. dazu *Hoffman-Riem*, AöR 1998, 532 (534).
78 *Roßnagel*, ZRP 1997, 28.
79 S. *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 20.
80 S. *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 79.

der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) erwächst dem Staat eine verfassungsrechtliche Schutzpflicht gegen rechtswidrige Datenerhebung. Diese Schutzpflichten greifen nicht nur bei Beeinträchtigungen durch Private, sondern auch bei Beeinträchtigungen durch ausländische Staaten. Da die Schutzpflichten schutzgutorientiert sind, ist es ist unerheblich, von wem eine Beeinträchtigung ausgeht. Allerdings hat der Staat bei der Auswahl der zu treffenden Maßnahmen einen weiten Einschätzungs-, Wertungs- und Gestaltungsspielraum. Aus einer Schutzpflicht entsteht in der Regel keine bestimmte verfassungsrechtliche Handlungsvorgabe. Das heißt jedoch nicht, dass der Staat keine Schutzmaßnahmen ergreifen muss. Sofern er sich nicht in der Lage sieht, gegen übermächtige Geheimdienste selbst wirksame Schutzmaßnahmen zu ergreifen, muss er zumindest seine Bürger in die Lage versetzen, sich selbst zu schützen. In Erfüllung dieser Gewährleistungsverantwortung ist es Aufgabe des Staates, über technische Mittel zur Abwehr von Grundrechtseingriffen in genügender Weise aufzuklären und die gesetzlichen Rahmenbedingungen so auszugestalten, dass die Verbreitung dieser Techniken möglichst einfach und ungehindert erfolgen kann. Außerdem muss er durch rechtliche Rahmenbedingungen sicherstellen, dass die für die Nutzung von Selbstschutztechniken erforderlichen Infrastrukturen errichtet werden.

3 Selbstdatenschutz

Unter Selbstdatenschutz ist in der digitalen Welt die Möglichkeit des Einzelnen zu verstehen, seine Grundrechte durch eigene technisch-organisatorische Maßnahmen selbst vor Verletzungen durch Dritte zu schützen. Zwar können Maßnahmen des Selbstdatenschutzes die Möglichkeit des Missbrauchs bereits erhobener Daten nicht verhindern. Vor allem im Bereich des Internet kann jedoch durch den Einsatz von den Datenschutz fördernden Techniken (Privacy Enhancing Technologies) der Missbrauch und die Zusammenführung unterschiedlicher Datenarten durch die Unterbrechung von Zuordnungsketten und die Verschleierung der eigenen Identität deutlich erschwert werden.[81]

Eine ausdrückliche oder gar in sich kohärente gesetzliche Ausgestaltung des Selbstdatenschutzes fand jedoch noch nicht statt. Dies wäre aber zur Durchsetzung des Selbstdatenschutzes als Bestandteil des staatlichen Schutzauftrags erforderlich.[82] Auch in der Datenschutzrichtlinie ist das Konzept nicht verankert worden.[83] Dagegen wird wenigstens der Kontrollansatz der Aufsichtsbehörden im Datenschutz zunehmend durch den Selbstdatenschutz der Bürgerinnen und Bürger ergänzt. Den Aufsichtsbehörden kommt dabei – inzwischen teilweise auf ausdrücklicher landesgesetzlicher Basis[84]– die Aufgabe zu, durch Informations- und Bildungsangebote die Betroffenen in die Lage zu versetzen, vorsichtig mit den eigenen Daten, respektvoll mit den Daten Dritter und selbstbewusst mit den gesetzlichen Datenschutzrechten umzugehen.[85] In vergleichbare Stoßrichtung zielt die Förderung der Stiftung Datenschutz, durch die eine tragfähige und zukunftsfähige Datenschutzkultur verankert werden soll.

---

81 *Schulz*, in: BeckOK Datenschutzrecht, § 3a BDSG, Rn. 50.1; *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 44 ff.

82 *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 88 ff.

83 *Schneider*, in: BeckOK Datenschutzrecht, EU-Datenschutzrichtlinie, Rn. 123.

84 § 24 Abs. 8 LDSG Rheinland Pfalz; § 43 Abs. 1 LDSG Schleswig Holstein.

85 *Brink*, in: BeckOK Datenschutzrecht, § 38 BDSG, Rn. 2.

Die Enthüllungen um die Spähprogramme der NSA führen vor Augen, wie weit die Überwachung des Internets zwischenzeitlich gediehen ist und wie intensiv die Spuren, die die Nutzer dort hinterlassen, ausgewertet werden. Das Internet von heute bietet eine Vielzahl von Diensten, und jeder Seitenaufruf, jeder Chat, jedes Foto, jede Suche, jeder Post und jede Nachricht hinterlassen eine Datenspur. Die Daten werden für Zwecke der Kundenbindung, der Online-Werbung oder der Marktforschung erfasst und ausgewertet und zu individuellen Nutzungs-, Kauf- oder Bewegungsprofilen verdichtet. Je mehr das Internet im Alltag genutzt wird, desto mehr Datenspuren liefern Hinweise auf Interessen, Vorlieben und Verhaltensweisen der Nutzerinnen und Nutzer. Selbst zu bestimmen, was man über sich preisgibt, ist dagegen das legitime Recht aller Nutzer des Internets. Die Globalität des Internet macht es häufig jedoch schwer, dies einzufordern. Man wird, gerade im elektronischen Rechts- und Geschäftsverkehr nicht immer und vollständig anonym bleiben können. Hier gleicht das Internet dem analogen Alltag: Auch hier müssen je nach Situation sich notwendige Preisgabe persönlicher Daten und berechtigtes Verschweigen abwechseln.[86]

Die Schutzwirkung von Maßnahmen des Selbstdatenschutzes kann zudem im Subordinationsverhältnis zwischen Staat und Bürger durch Gesetz oder hoheitliche Anordnungen durchbrochen werden, etwa bei Mitwirkungspflichten, wie zum Beispiel gemäß § 200 Abgabenordnung oder § 97 Insolvenzordnung oder der Sicherstellung und Beschlagnahme von E-Mails nach der Strafprozessordnung.[87]

Der Staat darf sich bei der Erfüllung seiner Schutzpflichten nicht darauf beschränken, dem Einzelnen den Selbstschutz seiner informationellen Selbstbestimmung zu überlassen. Selbstdatenschutz darf daher nicht isoliert gesehen werden. Soweit jedoch die Möglichkeiten der

---

86 *Wagner*, DuD 2013, 676.

87 *Schulz*, in: BeckOK Datenschutzrecht, § 3a BDSG, Rn. 50.2.

normativen Verhaltenssteuerung und des Systemdatenschutzes ausgeschöpft sind, kann auf die Möglichkeiten des Selbstdatenschutzes als ergänzende Maßnahmen nicht verzichtet werden.[88]

Im Folgenden werden Kriterien zur Förderung des Selbstdatenschutzes in den vier Kommunikationsbereichen Verbindungsdaten, Positionsbestimmung, Kommunikationsinhalte und Smart Home evaluiert.[89] Die unterschiedlichen Techniken und Konzepte zur Stärkung der Grundrechte des Endnutzers in den vier Kommunikationsbereichen lassen sich nicht einheitlich bewerten. Abhängig vom Einsatzaufwand und der Stelle der Implementation im Kommunikationsnetz sind zum Beispiel unterschiedliche Grade der Stärkung von Selbstdatenschutz feststellbar.[90]

Für die vier Kommunikationsbereiche Verbindungsdaten, Positionsbestimmung, Kommunikationsinhalte und Smart Home sind jeweils spezifische Kriterien für einen Optimierung des Selbstdatenschutzes erarbeitet worden.[91] Dazu wurden die technischen Gründe für die Nichtnutzung bisheriger Techniken zum Selbstdatenschutz analysiert und untersucht wie diese durch neue Gestaltungsansätze zukünftig vermieden werden können.

Allgemeine Kriterien für neue Technologien zum Selbstdatenschutz sind Angriffsschutz, Performanceerhalt, Nutzerfreundlichkeit, Verbreitung und Vertrauen. Die Ziele der Kriterien widersprechen sich teilweise. In der konkreten Ausgestaltung ist dann eine Abwägung zwischen ihrer Verwirklichung zu finden.[92]

---

88 *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 42.
89 Zur technischen Evaluation *Hahn/Herfert/Lange* 2015.
90 S. die Bewertung in *Hahn/Herfert/Lange* 2015, 35, 57, 69 und 89.
91 S. auch Konzepte für neue Technologien in *Hahn/Herfert/Lange* 2015, 37, 60, 70 und 89.
92 Zum Beispiel, ob mehr Gewicht auf Nutzerfreundlichkeit oder mehr Gewicht auf Angriffsschutz gelegt wird.

3.1 Kriterium Angriffsschutz

Neue Techniken zum Selbstdatenschutz sollen so gestaltet sein, dass sie Schutz davor bieten, dass andere mit den personenbezogenen Daten des Nutzers in einer Weise umgehen, die dieser ihnen nicht erlaubt hat. Sie müssen die Sicherheit der Betroffenen faktisch fördern. Dabei bieten sie grundsätzlich sowohl Schutz gegen unrechtmäßige als auch Schutz gegen rechtmäßige Datenverarbeitungen. Die Erfüllung des Kriteriums verlangt nicht, dass Angriffe unmöglich sind, sondern lediglich, dass die eingesetzten Techniken sie erschweren. Ein wesentliches Akzeptanzmerkmal für Techniken zum Selbstdatenschutz ist diese Werkzeugeignung, der ihren Einsatz für die Abwehr von Angriffen überhaupt geeignet erscheinen lässt.

3.2 Kriterium Performanzerhalt

Performanceeinbußen sind ein Grund für die mangelnde Nutzung von Techniken zum Selbstdatenschutz. Beispielsweise ist der Zugriff auf das Internet über Tor[93] deutlich langsamer als ein direkter Zugriff. Wird zusätzlich ein spezieller Browser verwendet, ergeben sich durch den Verzicht auf Techniken wie Javascript teilweise Darstellungsfehler auf Webseiten, manche Webseiten können ohne Javascript überhaupt nicht verwendet werden.[94]

Neue Techniken zum Selbstdatenschutz sollen so gestaltet sein, dass sie die Leistung der mit ihr verbunden oder genutzten Technik möglichst wenig einschränken. Beide müssen auch zusammen benutzbar sein. Idealerweise fördert die Technik zum Selbstdatenschutz die Leistung der mit ihr verbundenen Technikanwendungen sogar und verbessert damit die Performanz.

---

93 S. Kapitel 5.3.

94 *Hahn/Herfert/Lange* 2015, 59.

3.3 Kriterium Nutzerfreundlichkeit

Neue Techniken zum Selbstdatenschutz sollen nutzerfreundlich gestaltet sein. Ein maßgeblicher Grund für ihre mangelnde Verwendung, wie beispielswiese Verschlüsslung bei E-Mails, ist die fehlende Nutzerfreundlichkeit verfügbarer Programme. Sie sind in ihrer Handhabung zu kompliziert, fordern eine stetige Beschäftigung mit Sicherheitsabfragen und Schlüsselverwaltung oder überfordern das technische Verständnis der meisten Nutzer.[95] Bisherige Lösungen sind nicht nutzerfreundlich genug.

3.4 Kriterium Verbreitung

Ein wesentlicher praktischer Hinderungsgrund für den Einsatz von Techniken zum Selbstdatenschutz besteht auch darin, dass zwar viele unterschiedliche Lösungen existieren, diese aber nicht genügend verbreitet und kompatibel sind.

Zum einen besteht bei einer Vielzahl von Nutzern von Internet und Kommunikationstechniken keine oder wenig Kenntnis über die Gefährdungslage sowie keine oder wenig Kenntnis über die zur Verfügung stehenden Sicherungsmittel. Eine mangelnde Kenntnis über bestehende Lösungen führt also zu deren geringer Verbreitung.[96] Dem ist mit Aufklärung, Bildung und Schulung über Gefährdung und Selbstschutzmöglichkeiten entgegenzuwirken.[97]

Hinzu kommt, dass Kommunikation auf der Interaktion mehrerer beruht. Sobald einer der Akteure sich nicht an der Technikanwendung zum Selbstdatenschutz beteiligt, sind die Bemühungen der anderen Teilnehmer zum Selbstdatenschutz fruchtlos. Entweder die Kommunikation kann nicht stattfinden oder der Schutz wird in der Sphäre des Nicht-Teilnehmenden aufgehoben. Dies liegt auch daran, dass beste-

---

95 *Hahn/Herfert/Lange* 2015, 59.
96 *Hahn/Herfert/Lange* 2015, 36, 59, 70 und 90.
97 *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 86.

hende Technikanwendungen zum Selbstdatenschutz untereinander nicht kompatibel sind. Dies wird besonders deutlich am Beispiel der E-Mail-Verschlüsselung. Stellt der Empfänger keinen öffentlichen Schlüssel zur Verfügung, kann der Sender an diesen gerichtete Nachrichten nicht verschlüsseln. Auch wenn sich der Sender um Mittel des Selbstdatenschutzes bemüht hat, kann er sie bezüglich dieses einen Empfängers nicht einsetzen. Dies gilt auch, wenn Sender und Empfänger unterschiedliche Verschlüsselungsmethoden verwenden.[98] Ein einzelner Nutzer kann somit nicht wirksam verschlüsseln, wenn seine Kommunikationspartner nicht gleichziehen. Neue Techniken und bestehende Lösungen werden daher nur zögernd aufgenommen.[99] Selbstdatenschutz funktioniert als gesamtgesellschaftliches Instrument aber nur bei möglichster hoher Verbreitung.

Technikanwendungen zum Selbstdatenschutz sollen daher möglichst weit verbreitet werden können und möglichst untereinander kompatibel sein.

3.5 Kriterium Vertrauenswürdigkeit

Ein entscheidender Faktor bei der Auswahl bestehender Techniken zum Selbstdatenschutz ist, ob und inwieweit der Nutzer Technik und Diensteanbieter vertrauen kann. Dieser Bedarf ist technikübergreifend und kann an unterschiedlichen Stellen infrage gestellt werden.

Bisher sind zum Beispiel keine Sicherheitslücken der Verschlüsselungsfunktion in S/MIME bekannt, die Verschlüsselung kann daher als sicher gelten. Nach Bekanntwerden der NSA-Überwachungsaktivitäten ist das hierarchische Vertrauensmodell jedoch als potentielle Schwachstelle gewertet worden, weil von politischer Seite Einfluss auf Zertifizierungsbehörden oder die kommerziellen Implementierungen von S/MIME genommen werden kann.[100] Der Nutzer muss jedoch der

98 Zum Beispiel S/MIME und PGP, s. *Hahn/Herfert/Lange* 2015, 22 ff.
99 *Hahn/Herfert/Lange* 2015, 21.
100 *Hahn/Herfert/Lange* 2015, 22.

verwendeten Software vertrauen und sicher sein können, dass die Software keine Hintertüren enthält und ordnungsgemäß funktioniert.[101]

Nicht nur der Technik selbst sondern gegebenenfalls auch dem Diensteanbieter einer Selbstdatenschutzanwendung muss der Nutzer vertrauen können. Soweit E-Mail-Dienste-Anbieter serverseitigen für ihre Nutzer verschlüsseln, müssen diese darauf vertrauen, dass die Verschlüsselung ordnungsgemäß vorgenommen wird.[102] Das gilt sowohl in Bezug auf die korrekte Durchführung der Verschlüsselung als auch auf die sorgsame Verwaltung der geheimen Schlüssel.[103] Werden Anonymisierungsdienste beim Internetsurfen benutzt,[104] muss der Nutzer darauf vertrauen können, dass der Dienstanbieter seine IP-Adresse gegenüber Dritten wirksam verschleiert.[105]

Vertrauen stellt sich mithin als wesentliches Merkmal aller eingesetzten Selbstdatenschutztechniken dar. Vertrauen in Anwendungen und Diensteanbieter könnten zum Beispiel über unabhängige Auditierung[106] und Zertifizierung erzeugt werden.[107]

---

101 *Hahn/Herfert/Lange* 2015, 38, 94.
102 *Hahn/Herfert/Lange* 2015, 24, 51.
103 *Hahn/Herfert/Lange* 2015, 26, 39.
104 S. Kapitel 5.3.
105 *Hahn/Herfert/Lange* 2015, 51.
106 Bezüglich Software s. *Hahn/Herfert/Lange* 2015, 38.
107 *Roßnagel*, in: ders. 2003, Kapitel 3.4, Rn. 94 ff., 103.

4 Kommunikationsinhalte

Kommunikationsinhalte sind jene Inhalte, die bei schriftlicher oder mündlicher Kommunikation über die verschiedensten Kommunikationskanäle wie Telefonfestnetz, Mobilfunk oder Internet ausgetauscht werden. Dabei kommt eine Vielzahl an Kommunikationsformen zum Einsatz: Neben klassischen Kommunikationsformen wie Telefon und Brief wird die tägliche Kommunikation in zunehmendem Maß über SMS und Handygespräche sowie über internetbasierte Dienste wie E-Mail, Messagingdienste, Chat/Voice-Chat und soziale Netzwerke geführt. Gerade die neueren elektronischen Kommunikationsformen haben zu einer starken Steigerung an ausgetauschten Nachrichten und Gesprächen sowie zu einem geänderten Kommunikationsverhalten insgesamt geführt. Dieses verschiebt sich immer mehr in Richtung einer kontinuierlichen und von Multitasking geprägten Alltagskommunikation. Dementsprechend aussagekräftig sind die ausgetauschten Kommunikationsinhalte, anhand derer sich nicht nur das Leben einer Person detailliert nachvollziehen lässt. Diese geben auch Alltagsgewohnheiten, Einstellungen, Lebensumstände, Beziehungen bis hin zu den intimsten Details preis. Diese Zunahme an alltäglicher Kommunikation und Steigerung an Aussagekraft über einzelne Personen steht gerade vor dem Hintergrund massenhafter Überwachung in auffälligem Missverhältnis zu den zahlreichen Angriffsmöglichkeiten auf die Kommunikationsinhalte und führt zu einem Bedarf an Schutzmöglichkeiten, um die Vertraulichkeit der Kommunikation sicherzustellen.[108]

4.1 Schutz durch Verschlüsselung

Zentraler Baustein des Schutzes von Kommunikationsinhalten ist deren Verschlüsselung.[109] Dabei ist zwischen unterschiedlichen Formen

[108] S. *Hahn/Herfert/Lange* 2015, 7.
[109] S. *Hahn/Herfert/Lange* 2015, 7.

der Verschlüsselung zu unterschieden: Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung.

Transportverschlüsselung besteht in einer verschlüsselten Übermittlung von Kommunikationsinhalten auf verschiedenen Teilstrecken der Telekommunikation. An den Zwischenstationen werden die Inhalte entschlüsselt und für die nächste Teilstrecke neu verschlüsselt. Die Inhalte sind damit auf den Transportwegen verschlüsselt, liegen jedoch ungeschützt in allen Zwischenstationen vor.[110] Die hierzu notwendigen Schlüssel sind nur dem Telekommunikationsanbieter bekannt.

Ende-zu-Ende-Verschlüsselung besteht im Gegensatz zur Transportverschlüsselung in einer Verschlüsselung der übertragenen Inhalte über alle Zwischenstationen hinweg, so dass die Inhalte nur beim Absender und Empfänger entschlüsselt vorliegen. Die dazu notwendigen Schlüssel sind nur dem Absender und Empfänger bekannt.[111]

Beide Verfahren können kombiniert werden.

Verschlüsselung setzt dabei immer das Vorhandensein von geheimem Schlüsselmaterial beim Absender und Empfänger voraus. Dabei wird zwischen zwei unterschiedlichen Arten von Verschlüsselungsverfahren unterschieden, der symmetrischen Verschlüsselung und der asymmetrischen Verschlüsselung.

Bei der *symmetrischen* Verschlüsselung verfügen Absender und Empfänger über denselben geheimen Schlüssel, der nur ihnen bekannt ist. Nachrichten werden mit diesem Schlüssel verschlüsselt und wieder entschlüsselt.[112]

Dagegen verfügen bei der *asymmetrischen* Verschlüsselung Absender und Empfänger jeweils über ein Schlüsselpaar. Dieses besteht aus einem geheimen Schlüssel, der nur dem Besitzer selbst bekannt ist, und

---

110 S. *Hahn/Herfert/Lange* 2015, 8.
111 S. *Hahn/Herfert/Lange* 2015, 8f.
112 S. *Hahn/Herfert/Lange* 2015, 9f.

einem öffentlichen Schlüssel, der öffentlich bekannt und dem Besitzer zugeordnet ist. Nachrichten werden stets mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dem geheimen Schlüssel des Empfängers wieder entschlüsselt werden.[113]

Sowohl symmetrische wie asymmetrische Verschlüsselungsverfahren setzen voraus, dass Schlüssel zwischen Absender und Empfänger ausgetauscht werden müssen. Durch die Verwendung von öffentlichen Schlüsseln ist der Schlüsselaustausch bei asymmetrischen Verfahren einfacher, allerdings sind diese deutlich langsamer als vergleichbare Sicherheit bietende symmetrische Verfahren. In der Praxis werden daher die beiden Verfahren häufig miteinander kombiniert (hybride Verschlüsselung).[114]

Durch Verschlüsselung lassen sich unterschiedliche Gerade von Sicherheit realisieren.[115]

Ein *geringer Grad an Sicherheit* wird zum Beispiel erreicht, wenn elektronische Nachrichten durchgehend durch Transportverschlüsselung geschützt werden und die Transportverschlüsselung keine gravierenden Schwachstellen enthält. Damit sind die Kommunikationsinhalte durch einen grundlegenden Schutz vor großflächigem Abfangen oder Abhören der Kommunikation bei Sender, Empfänger oder einem der beteiligten Server, auf dem die Inhalte gespeichert sind, geschützt. So weist zum Beispiel der Server des eigenen E-Mail-Anbieters zumeist Schutzmaßnahmen für netzwerkbasierte oder physische Zugriffe von Unbefugten auf. Insbesondere sind die Inhalte auf den Servern vom Telekommunikationsdiensteanbieter verschlüsselt.[116]

Ein weitergehender Schutz, aber nur *mittlerer Grad an Sicherheit*, wird dadurch erreicht, wenn zusätzlich zur Transportverschlüsselung die

---

113 S. *Hahn/Herfert/Lange* 2015, 9.
114 S. *Hahn/Herfert/Lange* 2015, 9.
115 S. *Hahn/Herfert/Lange* 2015, 35 ff.
116 S. *Hahn/Herfert/Lange* 2015, 35.

Kommunikation Ende-zu-Ende verschlüsselt wird. Dabei werden alle auf einem Server abgelegten Nachrichten für einen Empfänger mit dessen öffentlichem Schlüssel verschlüsselt. Private Schlüssel liegen nur passwortgeschützt auf den Servern des eigenen Diensteanbieters. Schutz wird auch gegenüber Angriffen auf den Server des Dienste-Anbieters, oder gegenüber Angriffen von Administratoren mit Zugriff auf das eigene Postfach erreicht. Ferner wird Schutz der meisten Kommunikationsinhalte auch dann erreicht, wenn ein Angreifer die Transport-Verschlüsselung brechen kann. Kein Schutz wird vor gezielten Angriffen erreicht, bei denen der eigene Diensteanbieter selbst beteiligt ist. Kein Schutz besteht auf den Transportstrecken für unverschlüsselt eingehende und ausgehende Nachrichten.[117]

Ein sehr weitgehender Schutz der Kommunikationsinhalte und *hoher Grad an Sicherheit* wird erreicht, wenn elektronische Nachrichten nur Ende-zu-Ende-verschlüsselt gesendet und empfangen werden. Dabei liegt der private Schlüssel ausschließlich passwortgeschützt auf den eigenen Endgeräten, wie Desktop-PC, Laptop oder Smartphone.[118]

4.2 Kryptofreiheit

Der Einsatz von Kryptografie und dazugehörigen Produkten ist in Deutschland nicht eingeschränkt und nur in geringem Maß geregelt. Der Einsatz von Kryptografie wird für die Zwecke des sicheren elektronischen Rechtsverkehrs auf dem Gebiet der elektronischen Identifizierung, der elektronischen Signaturen und zukünftig auch anderer Vertrauensdienste reguliert.

In der sogenannten Kryptodebatte der 1990er Jahre wurde diskutiert, ob und in welchem Umfang der Einsatz kryptografischer Produkte gesetzlich beschränkt werden sollte.[119] Die leistungsfähige Verschlüsse-

---

117 S. *Hahn/Herfert/Lange* 2015, 36.

118 S. *Hahn/Herfert/Lange* 2015, 36.

119 Gemeinsame Presseerklärung des BMI und des BMWi vom 2.6.1999, Eckpunkte der deutschen Kryptopolitik, MMR 1999, Heft 7, XVII.

lung empfanden einige Politiker als eine Bedrohung der nationalen Sicherheit, da sie keinen Zugang zum Schlüssel und damit keine Möglichkeit hatten, die verschlüsselte Nachricht zu entschlüsseln. Der bloße Einsatz von Verschlüsselungsverfahren ist jedoch kein Indiz für kriminelle Handlungen,[120] sondern liegt im berechtigten und rechtmäßigen Interesse von Bürgern, Verwaltung und Wirtschaft.[121] Daraus folgt das sogenannte Krypto-Dilemma:[122] Einerseits sollen sichere Kryptoverfahren für rechtmäßige Nutzer zur Verfügung gestellt werden, andererseits sollen sich Straftäter nicht der Verfolgung und Verurteilung entziehen können, indem sie Kryptografie einsetzen. Diskutiert wurde in der Kryptodebatte, wie dem Staat eine Möglichkeit gegeben wird, trotz Verschlüsselung auf die so gesicherten Daten zuzugreifen.[123] Ansätze dazu sind unter anderem das Verbot und die Einschränkung des Einsatzes von Krypto-Verfahren und die Umgehung von Krypto-Verfahren durch den Einbau von Hintertüren oder die vorgeschriebene Schlüsselhinterlegung.[124] Solche Regelungen in Deutschland einzuführen und grundsätzlich die Kryptofreiheit zu beenden, hätte angesichts der leichten Verfügbarkeit von Kryptoprodukten über das Internet wohl auch kaum Wirkung.[125] Angesichts der NSA-Ausspähungen muss dagegen sogar das Ende der Kryptodebatte gefordert werden.[126] Wenn Kryptografie ein probates Mittel dafür ist, Grundrechtsverletzungen aller Internetnutzer zu verhindern, dann ist die allgemeine Verhinderung von Kryptografie zum Zwecke der Strafverfolgung unverhältnismäßig.

Im Folgenden wird gezeigt, dass sich die Kryptofreiheit im geltenden Technik- und Kommunikationsrecht widerspiegelt. Der Einsatz von

120 S. BGH CR 2008, 240.
121 *Brunst*, DuD 2012, 333 (334).
122 So *Brunst*, DuD 2012, 333 (334).
123 *Marauhn*, KritV 1999, 57.
124 S. *Brunst*, DuD 2012, 333 (334f.); s. auch *Gerhards* 2010.
125 *Brunst*, DuD 2012, 333 (334).
126 S. *Geminn*, DuD 2015, 546

Kryptografie wird für die Zwecke des sicheren elektronischen Rechtsverkehrs auf dem Gebiet der elektronischen Identifizierung, der elektronischen Signaturen und auch anderer Vertrauensdienste reguliert.

4.3 Verpflichtungen zur Verschlüsselung

Eine Verpflichtung zur Verschlüsselung kann sich für den Zugangsschutz, den Zugriffsschutz und den Transport- und Übertragungsschutz personenbezogener Daten aus Abs. 2 der Anlage zu § 9 BDSG ergeben. In dieser 2009 in das Bundesdatenschutzgesetz aufgenommenen Vorschrift wird Verschlüsselung ausdrücklich als Schutzmaßnahme genannt. [127] Die Verschlüsselung muss dem Stand der Technik entsprechen. Die Verschlüsselung kann auch durch eine andere Sicherungsmaßnahme ersetzt werden, wenn diese eine ausreichende Sicherheit verspricht.

Auch wenn die Maßnahme der Verschlüsselung nicht ausdrücklich genannt ist, kann sie sich als Verpflichtung dann ergeben, wenn die gesetzlich gebotene Geheimhaltung von Informationen bei der elektronischen Übertragung nicht auf andere Weise sicher gewährleisten lässt. Dies gilt für alle Berufsgeheimnisträger, die in § 203 StGB genannt sind und für die eine unbefugte Offenbarung der ihnen anvertrauten Informationen strafbar ist. Betroffenen von dieser Verschlüsselungspflicht können daher Ärzte, Apotheker, Berufspsychologen, Rechs- und Patentanwälte, Notare Wirtschaftsprüfer, Buchprüfer, Steuerberater, Steuerbevollmächtigte, Ehe-, Familien- Erziehungs- und Jugendberater, Mitglieder von Schwangerschaftsberatungsstellen, Sozialarbeiter und Sozialpädagogen und Angehörige eines Unternehmens der privaten Kranken-, Unfall-, oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle und viele weitere in § 203 StGB genannten Berufsgeheimnisträger.

---

[127] S. ausführlich z.B. *Ernestus*, in: Simitis 2014, § 9 BDSG, Rn. 164 ff.

Für Finanzbehörden legt die Abgabenordnung ausdrücklich eine Pflicht zu Verschlüsselung fest. Sie sind nach § 87a Abs. 1 Satz 3 AO verpflichtet, „die Daten, die dem Steuergeheimnis unterliegen" bei einer Übermittlung „mit einem geeigneten Verfahren zu verschlüsseln". Aber auch für andere elektronische Kommunikationen, die amtlich geheim zu haltende Informationen betreffen, kann eine Verschlüsselungspflicht gelten, auch wenn sie nicht ausdrücklich erwähnt ist. So hat der Bundestag schon mehrfach festgestellt, dass für Übermittlungen gemäß § 30 VwVfG die notwendigen Sicherheitsvorkehrungen getroffen werden müssen. Soweit erforderlich, sind die Daten, wenn sie über das Internet übermittelt werden, zu verschlüsseln. [128] Ähnlich hält die amtliche Begründung zum E-Government-Gesetz fest, dass eine Behörde bei „der Versendung von Daten, z.B. Sozialdaten, mit sehr hohem Schutzbedarf verpflichtet ist, weitere Sicherungsmaßnahmen, z.B. eine Ende-zu-Ende-Verschlüsselung, einzusetzen".[129]

Telemediendiensteanbieter haben nach § 13 Abs. 4 Nr. Nr. 3 TMG, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann".[130] Telekommunikationsdiensteanbieter müssen nach § 109 Abs. 1 TKG „erforderliche technische Vorkehrungen und sonstige Maßnahmen" zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. In beiden Fällen ist der Stand der Technik zu berücksichtigen. Auch wenn diese Regelungen Verschlüsselung nicht ausdrücklich erwähnen, können beide Verpflichtungen dazu führen, dass der Anbieter Verschlüsselung zum Schutz der Vertraulichkeit der in der Telekommunikation und den Telemedien übertragenen Daten einsetzen muss. [131]

---

128 BT-Drs. 14/9000, S. 28.
129 S. BT-Drs. 17/11473, S. 34.
130 S. z.B. *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 106 ff.
131 S. z.B. *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 110.

4.4 Im- und Exportregulierung

Eine Einfuhrbeschränkung bezüglich der Datenverschlüsselungsprodukte (Krypto-Produkte) besteht in Deutschland nicht. Zu kryptografischen Verfahren und Techniken existieren lediglich Ausfuhrbestimmungen.

Die Europäische Union kontrolliert den Export von zivilen Gütern, die auch zu militärischen Zwecken gebraucht werden können (sog. Dual-Use-Güter), gemäß Verordnung (EG) Nr. 428/2009.[132] Anlage I dieser Verordnung enthält eine Liste kontrollpflichtiger Güter, die auf Konsensentscheidungen im Zusammenhang mit internationalen Ausfuhrkontrollregimen beruht. Kontrollpflichtige Güter dürfen ohne eine entsprechende Ausfuhrgenehmigung die Zollgrenzen der Europäischen Union nicht verlassen. Die allgemeinen Ausfuhrgenehmigungen gemäß Anlage II erstrecken sich auf risikoarme Ausfuhren bestimmter Güter nach bestimmten Bestimmungszielen. Die Ausfuhrkontrollen für Güter und Technologien mit doppeltem Verwendungszweck sollen das Risiko einer Verbreitung und militärischen Nutzung begrenzen, ohne den legitimen Handel einzuschränken.

Die Europäische Kommission hat mit der Delegierten Verordnung (EU) Nr. 1382/2014 vom 22. Oktober 2014 den Anhang I der Verordnung (EG) Nr. 428/2009 des Rates über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck neu gefasst. Diese Delegierte Verordnung ist am 31. Dezember 2014 in Kraft getreten. In Anlage I wird Kryptotechnik bestimmt als Technik, Prinzipien, Mittel und Methoden zur Transformation von Daten, um ihren Informationsinhalt unkenntlich zu machen, ihre unbemerkte Änderung oder ihren unerlaubten Gebrauch zu verhindern. Krypto-

---

[132] Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (Dual-Use-Verordnung), EG ABl. Nr. L 134 Satz 1, ber. ABl. Nr. L 224 Satz 21, Celex-Nr. 3 2009 R 0428.

technik beschränke sich auf die Transformation von Informationen unter Benutzung eines oder mehrerer „geheimer Parameter“ (z.B. Schlüssel-Variable) oder des zugehörigen Schlüssel-Managements. Nach Kategorie 5 „Telekommunikation und Informationssicherheit“ sind spezielle Systeme für “Informationssicherheit”[133] und Software, die Kryptotechnik[134] enthalten und die keinen dezidierten kommerziellen Nutzen haben,[135] von der Ausfuhrkontrolle betroffen.

4.5 Regulierung für den elektronischen Rechtsverkehr

Der Einsatz von Kryptografie wird für die Zwecke des sicheren elektronischen Rechtsverkehrs auf dem Gebiet der elektronischen Identifizierung, der elektronischen Signaturen und auch anderer Vertrauensdienste reguliert.

4.5.1 eID-Funktion des Personalausweis

Seit Einführung des neuen Personalausweises und Novellierung des Personalausweisgesetzes (PAuswG)[136] verfügt der nun ausgegebene Personalausweis[137] über maschinenlesbare Chips[138] und Möglichkeiten zur elektronischen Identifizierung. Dazu werden die Speicher auf dem Personalausweis gemäß § 5 Abs. 5 PAuswG mit bestimmten, identifizierenden Daten des Ausweisinhabers sowie mit Sperrkennwort, Sperrmerkmale, Seriennummer und Prüfziffern gefüllt.[139]

Nach § 18 Abs. 2 PAuswG erfolgt der elektronische Identitätsnachweis durch Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises. Dabei sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung

133 S. 5A002 Anhang I Dual-Use-Verordnung.
134 S. 5D002 Anhang I Dual-Use-Verordnung.
135 S. Teil 2 Anmerkung 3 Anhang I Dual-Use-Verordnung.
136 Zur Einführung und Gesetzesgenese *Borges*, NJW 2010, 3334; *Polenz*, MMR 2010, 671.
137 Entsprechend auch neue Reisepässe und neue Aufenthaltstitel.
138 „Elektronische Speicher und Verarbeitungsmedium“ im Sinne von § 5 PAuswG.
139 S. zur Begriffsbestimmung jeweils § 2 PAuswG.

von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten. Erfolgt die Abfrage und Übertragung über das Internet, sind außerdem Verschlüsselungsverfahren anzuwenden. Der elektronische Identitätsnachweis beruht auf dem Konzept der Authentisierung durch Besitz und Wissen. Dieses besagt im Kern, dass die Identität des Handelnden dadurch nachgewiesen wird, dass dieser sich durch eine Information ausweist, die nur ihm bekannt ist (Wissen), und zusätzlich durch den Besitz an einer beweglichen Sache (Besitz), die ihm ausschließlich zugewiesen ist und über die nur er verfügen kann. Beim elektronischen Identitätsnachweis nach § 18 PAuswG wird dieses Konzept durch die Bindung des Schlüssels an den Personalausweis und dessen Ausgestaltung als Chipkarte und die Verwendung einer asymmetrischen Verschlüsselungstechnologie umgesetzt.[140] Die zur Authentisierung verwendete Information wird als geheimer Schlüssel ausgestaltet, die nach dem Stand der Technik eine besonders gute Grundlage für die Authentisierung in der elektronischen Kommunikation darstellt.[141] Der geheime Schlüssel wird auf dem Chip gespeichert. Dieser ist so ausgestaltet, dass er die Information nur nach Eingabe des richtigen Passworts, der sogenannten PIN, preisgibt. Ein Auslesen des Chips ohne Eingabe der PIN ist ausgeschlossen. Der Chip ist im Personalausweis integriert. Das Auslesen des auf dem Personalausweis integrierten Chips erfolgt durch ein separates Lesegerät. Die Ausschließlichkeit der Verwendung der Authentisierungsinformation wird durch Besitz am Ausweis und durch ausschließliche Kenntnis der PIN gesichert.[142]

Zwar nutzen der neue Personalausweis und das elektronische Identifizierungsverfahren Verschlüsselungstechnik. Diese ermöglichen aber keine Sicherung von Kommunikationsinhalten. Die verwendeten

---

140 *Möller*, in: Hornung/Möller 2011, § 18 PAuswG, Rn. 5.
141 *Borges* 2011, 8.
142 *Borges* 2011, 8.

Schlüssel sind auch nicht ohne Weiteres auslesbar, sodass die Informationen auf dem Ausweis nicht zur Verschlüsselung von Inhalten „zweckentfremdet" werden können. Zur Verschlüsslung von Inhalten könnten jedoch auf den neuen Personalausweis nachträglich aufgebrachte Schlüssel für qualifizierte elektronische Signaturen genutzt werden.[143] Gemäß § 22 PAuswG wird der Ausweis als sichere Signaturerstellungseinheit im Sinn des § 2 Nr. 10 Signaturgesetzes (SigG) ausgestaltet.

4.5.2 Elektronische Signaturen

Eine elektronische Signatur ist ein mathematischer Wert, der mit Hilfe eines geheimen Signaturschlüssels zu einem elektronischen Dokument berechnet worden ist. Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Prüfschlüssels die Authentizität und Integrität des elektronischen Dokuments zu prüfen.[144] Die elektronische Signatur bietet in der Regel keinen Schutz vor dem Zugriff Dritter während des elektronischen Transports, sondern lässt nur nachträglich erkennen, ob der Text seit seiner Signierung verändert wurde. Soll er auch gegen Kenntnisnahme Dritter geschützt werden, muss er zusätzlich – mit dem öffentlichen Schlüssel des Empfängers – verschlüsselt werden.

Zur Beschleunigung des Verfahrens der Signaturerstellung berechnet das Programm des Verwenders eine Kurzfassung des elektronischen Dokuments, die statt des gesamten Dokuments mit dem Signaturschlüssel verschlüsselt wird. Dazu nutzt es einen sogenannten Hashalgorithmus, das heißt ein Verfahren zur Berechnung eines „elektronischen Fingerabdrucks" von elektronischen Daten, der ein bestimmtes festes Format hat und diese Daten repräsentiert. Zur Prüfung der Integrität so signierter Daten errechnet das Prüfprogramm die Kurzfassung des elektronischen Dokuments, transformiert das Kryptogramm mit dem öffentlichen Schlüssel des Verwenders wieder zu der

---

143 Zur elektronischen Signatur sogleich im nächsten Abschnitt.

144 S. hierzu ausführlich *Roßnagel*, in: ders. 2013, Einleitung ins SigG, Rn. 7 ff.

ursprünglichen Kurzfassung zurück und vergleicht beide Kurzfassungen. Wurde das signierte elektronische Dokument verändert, unterscheidet sich die Kurzfassung des elektronischen Dokuments von der entschlüsselten Kurzfassung. Solange das Kryptogramm der Kurzfassung nicht gebrochen werden kann und die Kurzfassungen identisch sind, kann der Verwender sicher sein, dass das elektronische Dokument unverfälscht ist. Mit Hilfe der elektronischen Signatur kann daher die Integrität eines elektronischen Datensatzes nachgewiesen werden.[145]

Die Authentizität des Dokuments lässt sich mit Hilfe elektronischer Zertifikate nachweisen. Der Prüfschlüssel wird mit Hilfe der Bestätigung eines Dritten (zum Beispiel eines Zertifizierungsdiensteanbieters) einer Person zugeordnet. Dieses Zertifikat wird durch eine elektronische Signatur des Dritten gesichert und in dessen Verzeichnisdienst aufgenommen. Das Zertifikat wird einer Signatur immer beigefügt. So kann das Prüfprogramm bei der Prüfung einer Signatur das Zertifikat auslesen und mit dem Verzeichnisdienst des Zertifizierungsdiensteanbieters abgleichen. Wenn das dort hinterlegte Zertifikat noch gültig ist und den Schlüsselinhaber ausweist und die Prüfung mit dem Prüfschlüssel funktioniert hat, kann man ausreichend sicher sein, dass die dem Prüfschlüssel zugeordnete Person auch diejenige ist, die die Signatur erstellt hat.[146]

Elektronische Signaturen sind ein geeignetes Mittel für eine rechtssichere und beweiskräftige elektronische Kommunikation.[147] Sie ermöglichen es, elektronische Dokumente mittels kryptografischer Verfahren zu sichern, um so Authentizität und Integrität belegen zu können. Die eingesetzte Infrastruktur kann auch zur Sicherung der Kommunikationsinhalte genutzt werden.

---

145 S. hierzu *Roßnagel*, in: ders. 2013, Einleitung ins SigG, Rn. 13 ff

146 S. näher *Roßnagel*, in: ders. 2013, Einleitung ins SigG, Rn. 18 ff

147 *Fischer-Dieskau/Roßnagel/Steidle,* MMR 2004, 451.

Der Gesetzgeber hat bereits 1997 im ersten Signaturgesetz Rahmenbedingungen für das Angebot elektronischer Signaturen geschaffen. Nach Verabschiedung der Signaturrichtlinie der Europäischen Gemeinschaft im Dezember 1999[148] wurden die deutschen Rahmenbedingungen in Einklang mit der EG-Richtlinie überarbeitet und resultierten in der Neufassung des deutschen Signaturgesetzes vom Mai 2001[149] und der Signaturverordnung vom November 2001.[150] Bis auf wenige Änderungen bilden deren Fassungen heute noch die Basis für Erstellung von qualifizierten elektronischen Signaturen und qualifizierten elektronischen Zeitstempeln.[151]

Das Signaturgesetz enthält keine Regelungen zu den Rechtsfolgen der Verwendung elektronischer Signaturen. Es regelt nur die Anforderungen, auf die Verwendungsregelungen verweisen können.[152] In § 1 Abs. 2 SigG ist klargestellt, dass die Verwendung von elektronischen Signaturen freigestellt ist, soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind. Aufgrund der Vielfalt der Einsatzmöglichkeiten der elektronischen Signatur werden diese Regelungen im Recht des jeweiligen Anwendungsfelds getroffen. Das Signaturgesetz unterscheidet zwischen einfachen, fortgeschrittenen und qualifizierten elektronischen Signaturen.[153] Darüber hinaus können sich die Zertifizierungsdiensteanbieter[154] von der Bundesnetzagentur akkreditieren lassen, so dass noch eine vierte Klasse von elektronischen Signaturen besteht.[155]

---

148 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

149 Signaturgesetz vom 16.5.2001 (BGBl. I, 876).

150 Signaturverordnung vom 16.11.2001 (BGBl. I, 3074).

151 Ausführlich zur Genese *Roßnagel*, in: ders. 2013, Einleitung ins SigG, Rn. 35 ff.

152 Nach § 1 Abs. 1 SigG sollen lediglich die Rahmenbedingungen geschaffen werden.

153 Dies in nahezu wortgleicher Umsetzung der Signaturrichtlinie, s. Nachweise bei *Roßnagel*, in: ders. 2013, § 2 SigG, Rn. 11 ff.

154 Zertifizierungsdiensteanbieter sind nach § 2 Nr. 8 SigG natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen.

155 S. § 15 und 16 SigG.

Mit dem Zeitablauf kann die Sicherheitseignung kryptografischer Algorithmen verloren gehen. Gefahren für die Sicherheit der Algorithmen und zugehörigen Parameter entstehen aus den Fortschritten der Rechner- und Softwaretechnologie sowie der Mathematik und Kryptografie.[156] Diese Fortschritte werden von der Aufsichtsbehörde, der Bundesnetzagentur, beobachtet und hinsichtlich ihrer Auswirkungen auf die Sicherheit der eingesetzten Algorithmen und zugehörigen Parameter bewertet. Der zu diesem Zweck erstellte sogenannte Algorithmenkatalog wird von der Bundesnetzagentur gemäß Anlage 1 Abschnitt 1 Nr. 2 SigV jährlich oder – bei Bedarf – öfter aktualisiert und im Bundesanzeiger veröffentlicht.

Eine Eignung von Algorithmen und Parametern wird von der Bundesnetzagentur festgestellt, wenn für die nächsten sieben Jahre nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von qualifizierten elektronischen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann.[157] Nach der Überprüfung der Algorithmen und zugehörigen Parameter dürfen keinerlei vernünftige Zweifel verbleiben, dass nicht erkennbare Manipulationen ausgeschlossen sind. Ein auf Tatsachen beruhendes Besorgnispotenzial, dass solche Manipulationen möglich sein könnten, genügt, um die Eignung auszuschließen.

Aufgrund einer solchen Besorgnis wurde der Hashalgorithmus SHA-1 von der Bundesnetzagentur als nicht mehr geeignet für die Erzeugung von qualifizierten elektronischen Signaturen eingestuft. Bis 2015 war er nur noch für die Prüfung qualifizierter Zertifikate zu benutzen. Die Hashfunktion SHA-1 war nur bis Ende 2010 als zur Erzeugung qualifizierter Zertifikate geeignet eingestuft worden, sofern in die Erzeugung der Seriennummer Zufall mit mindestens 20 Bit Entropie einge-

---

156 *Roßnagel*, in: ders. 2013, § 11 SigV, Rn. 40.
157 *Roßnagel*, in: ders. 2013, § 11 SigV, Rn. 41.

flossen ist. Seitdem gilt dieses Hash-Verfahren nicht als geeignet, um in Verfahren eingesetzt zu werden, die qualifizierte elektronische Signaturen erzeugen.

Bezogen auf die Sicherung von Kommunikationsinhalten, hat die Regulierung der elektronischen Signatur derzeit noch zwei Bedeutungen: Zum einem stellt die über die qualifizierten und akkreditierten elektronischen Signaturen geschaffene Public Key Infrastructure eine Möglichkeit zur Verschlüsselung von Kommunikationsinhalten bereit. Zum anderen wird über den Algorithmenkatalog der Bundesnetzagentur ein hoher Sicherheitsstandard hinsichtlich der Qualität der Verschlüsselung gewährleistet. Außerdem bietet der Algorithmenkatalog, über die Verwendung bei elektronischen Signaturen hinaus, verbindliche Hinweise für den Rechtsverkehr zur Sicherheit von Verschlüsselungs- und Hashverfahren.

4.5.3 eIDAS-Verordnung

Der Rechtsrahmen für elektronische Signaturen befindet sich in einer Umbildungsphase. Am 18. September 2014 trat die VO (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-VO) in Kraft.[158] Sie soll das Vertrauen in den elektronischen Rechtsverkehr in der Europäischen Union stärken. Zu diesem Zweck regelt sie die Sicherungsmittel und Sicherungsdienste, die Manipulations-, Rechts- und Beweissicherheit unionsweit gewährleisten sollen. Sie gilt nicht nur für elektronische Signaturen, sondern auch für Verfahren, die von elektronischen Signaturen abgeleitet sind wie elektronische Zeitstempel und elektronische Siegel. Es sind aber auch Verfahren gemeint, die meist elektronische Signaturen verwenden, wie die Langzeitaufbewahrung von Dokumenten, die bestätigte elektronische Zustellung oder die Website-Authentifizierung. Der

158 *Roßnagel*, NJW 2014, 3686.

Entwurf beschränkt sich aber nicht auf die Koordination der Anforderungen an diese „Vertrauensdienste“, sondern regelt auch punktuell die Rechtsfolgen ihres Einsatzes. Sie gilt außerdem für elektronische Identifizierungsmittel.

Die Verordnung wurde am 28. August 2014 im Amtsblatt[159] verkündet und trat am 18. September 2014 in Kraft.[160] Während sie seitdem für die Ermächtigungen der Kommission gültig ist, gelten die materiellen Regelungen erst ab dem 1. Juli 2016. Gemäß Art. 50 Abs. 1 eIDAS-VO wird die Signaturrichtlinie (1999/93/EG) auch zum 1. Juli 2016 aufgehoben. Bis zum Inkrafttreten aller Teile sollen europäische Techniknormen entwickelt sein, die das Sicherheitsniveau von Sicherheitsdiensten, Sicherheitsprodukten und Sicherheitssystemen festlegen.[161] Die Kommission wurde in der Verordnung dazu ermächtigt, zu diesem Zwecke durch den Erlass von Durchführungsrechtsakten auf diese Normen zu verweisen.[162]

Die eIDAS-VO soll der grenzüberschreitenden Koordinierung des elektronischen Rechtsverkehrs unter unionsweiter gegenseitiger Anerkennung und Akzeptierung der elektronischen Identifikations- und Vertrauensdienste dienen.[163]

Der Vorschlag bildet die letzte der zwölf Schlüsselaktionen, die in der „Binnenmarktakte für neues Wachstum 2012“[164] vorgesehen waren, und zielt auf die gegenseitige Anerkennung der nationalen eID-Systeme zwischen den einzelnen Mitgliedstaaten. Zudem soll die Verordnung einen Binnenmarkt für die grenzüberschreitende Verwendung elektronischer Signaturen und Vertrauensdienste schaffen, indem sie darauf hinführt, dass die Dienste künftig unter einheitlichen

159 EU ABl. 2014 L 257, 73.
160 S. Art. 52 Abs. 1 eIDAS-VO.
161 Beauftragt ist die Europäische Agentur für Netz- und Informationssicherheit (ENISA), s. auch *Hühnlein*, DuD 2014, 267.
162 *Roßnagel*, NJW 2014, 3686 (3687).
163 SWD(2012) 136, 2.
164 IP/11/469.

Standards grenzübergreifend sicher und funktional genutzt werden können und ihnen die gleiche Rechtswirkung zukommt wie den papiergestützten Verfahren.

Da diese Identifizierungs- und Vertrauensdienste den gesamten elektronischen Rechtsverkehr sichern sollen, regelt die Verordnung eine alle Bereiche der Informationsgesellschaft durchdringende Querschnittsmaterie. Sie wird damit zentraler Bausteine zur Verwirklichung von zum Beispiel eGovernment, eHealth, eJustice und eBusiness in den Mitgliedstaaten gestalten und Vorgaben für die weitere Entwicklung dieser Bereiche enthalten.[165]

Durch die Wahl des Rechtssetzungsmittels Verordnung, wird eine Vollharmonisierung des Unionsrechts erreicht. Das Rechtsinstrument der Verordnung wirkt in allen Mitgliedstaaten der Europäischen Union unmittelbar. Diese direkte Anwendbarkeit nach Art. 288 Abs. 2 AEUV gewährleistet eine unionsweite Rechtsvereinheitlichung. Im Gegensatz zu einer Richtlinie muss eine Verordnung nicht erst durch nationale Rechtsakte umgesetzt werden. Die Verordnung erlangt unmittelbare Geltung und in ihrem Anwendungsbereich. Anwendungsvorrang gegenüber allen wörtlich und sinngemäß widersprechenden Regelungen des deutschen Rechts und des Rechts anderer Mitgliedsstaaten erhalten. Dabei ist jedoch die Begrenzung des Anwendungsbereichs zu beachten.[166] Nach Art. 2 eIDAS-VO findet die Verordnung keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalen Rechtsvorschriften verwendet werden. Die Verordnung soll auch nicht nationales Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder anderen rechtlichen oder verfahrensmäßigen Verpflichtungen, für die nach nationalem

---

165 *Roßnagel*, NJW 2014, 3686; *Byszio/Houdeau/Meister/Wolfenstetter*, DuD 2013, 169; *Hühnlein*, DuD 2014, 267.

166 Dazu und zur Möglichkeit weiterer deutscher Regelungen ausführlich *Roßnagel*, MMR 2015, 359.

Recht oder Unionsrecht Formvorschriften zu erfüllen sind, verdrängen.

Inhaltlich fasst der Entwurf zwei verschiedene Regelungsgegenstände zusammen: die gegenseitige Anerkennung staatlicher Identifikationssysteme und die Anforderungen an „Vertrauensdienste“, die überwiegend von privaten Unternehmen erbracht werden.

4.5.4 Anerkennung staatlicher Identifikationssysteme

In der eIDAS-VO wird kein eigenes Identifikationssystem, sondern lediglich die gegenseitige Anerkennung bestehender oder zukünftiger elektronischer Identifikationssysteme geregelt. Art. 6 eIDAS-VO fordert von jedem Mitgliedstaat, der für nationale Online-Dienste die Verwendung eines elektronischen Identifizierungssystems verlangt, hierfür auch alle Identifizierungssysteme aus anderen Mitgliedstaaten anzuerkennen, die bei der Kommission notifiziert und nach Art. 9 Abs. 2 eIDAS-VO in einer Liste veröffentlicht worden sind.[167] Außerdem müssen sie dem Sicherheitsniveau „substanziell“ oder „hoch“ entsprechen, wenn der anerkennende Mitgliedstaat dieses Niveau für seine Anwendung fordert. Diese Sicherheitsniveaus werden in Art. 8 Abs. 2 eIDAS-VO abstrakt definiert. Für das deutsche Recht zum Personalausweis und das System der elektronischen Identifizierung, bedeutet die eIDAS-VO daher keine grundsätzliche Veränderung.

4.5.5 Vertrauensdienste

Unter dem neuen Begriff „Vertrauensdienst“ ist nach Art. 3 Nr. 16 eIDAS-VO jeder elektronische Dienst erfasst, der die Erstellung, Überprüfung, Validierung, Handhabung und Bewahrung elektronischer Signaturen, elektronischer Siegel, elektronischer Zeitstempel, elektronischer Dokumente, elektronischer Einschreiben, der Website-Authentifizierung und elektronischer Zertifikate einschließlich der Zertifikate für elektronische Signaturen und elektronische Siegel beinhaltet.

---

167 *Roßnagel*, NJW 2014 , 3686 (3687).

Die Verordnung unterscheidet zwischen „Vertrauensdiensten“ und „qualifizierten Vertrauensdiensten“.[168] Diese Dienste sollen von Vertrauensdiensteanbietern angeboten werden, also in der Regel privatwirtschaftlichen Unternehmen. Dies ist die Rolle der nach geltendem Recht als Zertifizierungsdiensteanbieter bezeichneten Unternehmen.

Für einfache Vertrauensdienste gelten nur wenige allgemeine und spezielle Vorschriften.[169] Dazu gehört vor allem die Verpflichtung nach Art. 18 Abs. 1 eIDAS-VO, die Dienste durch „geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken“ zu schützen, die den Stand der Technik berücksichtigen. Sicherheitsverletzungen müssen den zuständigen Aufsichtsstellen gemeldet werden. Für einen „qualifizierten Vertrauensdienst“ gelten zusätzlich zu den Anforderungen für einfache Vertrauensdienste weitere spezifische Anforderungen.[170]

Die Überprüfung dieser Anforderungen ist Aufgabe der nationalen Aufsichtsstellen nach Art. 16 eIDAS-VO. In Abkehr von der sehr zurückhaltenden Aufsichtskonzeption der Signaturrichtlinie verschärft der Entwurf die Aufsicht über qualifizierte, aber auch einfache Vertrauensdienste erheblich.

Qualifizierte Vertrauensdiensteanbieter müssen zur Erfüllung ihrer allgemeinen und speziellen Aufgaben, geeignete technische Maßnahmen zur Beherrschung der Sicherheitsrisiken[171] und vertrauenswürdige Produkte und Systeme verwenden, die die technische Sicherheit und Zuverlässigkeit ihrer Produkte sicherstellen.[172] Auch müssen zum Beispiel die qualifizierten Vertrauensdienste Signatur, Siegel, Zeitstempel und Einschreiben auf eine Weise mit den behandelten Daten

---

168 Diese sind nach Art. 2 Nr. 17 eIDAS-VO solche Vertrauensdienste, die die einschlägigen Anforderungen der Verordnung erfüllen.

169 S. Art. 13, 15, 18 eIDAS-VO.

170 *Roßnagel*, NJW 2014 , 3686 (3689).

171 S. Art. 19 Abs. 1 Satz 1 eIDAS-VO.

172 S. Art. 24 Abs. 1 e) und f) eIDAS-VO.

verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.[173] Da diese Dienste mit Hilfe von Verschlüsselungsverfahren arbeiten, erfordert dies eine Bewertung der Sicherheit dieser Verfahren. Geprüft werden muss, ob diese noch sicher genug sind, um zu gewährleisten, dass die nachträgliche Veränderung von Daten erkannt werden kann. Dies macht ein Bewertungsverfahren vergleichbar zu dem von der Bundesnetzagentur nach Anlage 1 Abschnitt 1 Nr. 2 SigV jährlich erstellten Algorithmenkatalog notwendig. Ein solches ist in der eIDAS-VO nicht ausdrücklich vorgesehen, wird aber zum einem über den Weg der technischen Normung etabliert und stellt sich zum anderem als Aufgabe der Aufsichtsstelle nach Art. 17 eIDAS-VO dar. Die Aufsichtstätigkeit ist ohne eine solche Bewertung schlicht nicht möglich.

Zu den in Art. 43 und 44 eIDAS-VO geregelten Dienste für die Zustellung elektronischer Einschreiben ist noch festzustellen, dass diese konzeptionell der De-Mail gleicht.[174] Diese Dienste sollen angebotenen werden, um die Übermittlung von Daten mit elektronischen Mitteln nachweisen zu können und die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung zu schützen. Sie gelten nach Art. 44 eIDAS-VO als qualifiziert, wenn sie von einem qualifizierten Vertrauensdiensteanbieter erbracht werden, der die eindeutige Identifizierung des Absenders und des Empfängers sicherstellt, das Absenden und Empfangen der Daten durch eine fortgeschrittene Signatur oder ein fortgeschrittenes Siegel so sichert, dass jede Möglichkeit einer unbemerkten Veränderung der Daten ausgeschlossen ist. Darüber hinaus sind das Datum und die Zeit des Absendens und Empfangens durch einen qualifizierten Zeitstempel zu sichern.[175] Eine Ende-zu-Ende Verschlüsselung ist nicht zwingend vorgesehen. Diese oder die Möglichkeit zu dieser könnte aber als zusätzli-

---

173 S. Art. 26 d), 36 d), 42 Abs. 1 a) und 44 Abs.1 d) eIDAS-VO.
174 S. *Hahn/Herfert/Lange* 2015, 20.
175 *Roßnagel*, NJW 2014 , 3686 (3690).

che Funktion vom jeweiligen Vertrauensdiensteanbieter angeboten werden.

Demnach werden auch unter der Geltung der eIDAS-VO Verschlüsselungstechniken nicht zum Schutz von Kommunikationsinhalten etabliert. Die aufkommenden Dienste elektronischer Signaturen und Siegel können zukünftig, abhängig von den Ergebnissen der technischen Normung und der konkreten technischen Ausgestaltung, aber dazu genutzt werden.

4.6 Kommunikationsarten

Kommunikationsarten bei denen Kommunikationsinhalte entstehen die geschützt werden sollen, können zunächst nach der Art der verwendeten Technik voneinander abgegrenzt werden:[176]

Die *Telefonkommunikation* beschreibt gesprochene Kommunikation über Telefon oder Mobiltelefon. Diese kann über Festnetz, Mobilfunk oder VoIP (Voice-Over-IP) übermittelt werden.

Die *SMS-Kommunikation* ermöglicht das versenden kurzer Textnachrichten über das Mobilfunknetz.[177]

Über *Messagingdienste*, wie WhatsApp, Telegram, Viber, Google Hangouts und Skype, können über die Diensteanbieter und das Internet sowohl Text als auch Sprachnachrichten verschickt werden.[178]

Vergleichbares erlauben *Chats und Voice-Chats*, wie Internet Relay Chat und Instant Messaging.[179]

In *sozialen Netzwerken* geben Nutzer freiwillig persönliche Informationen preis und übermitteln Nachrichten an andere.[180]

---

176 S. *Hahn/Herfert/Lange* 2015, 10 ff.
177 S. *Hahn/Herfert/Lange* 2015, 12.
178 S. *Hahn/Herfert/Lange* 2015, 13.
179 S. *Hahn/Herfert/Lange* 2015, 13f.
180 S. *Hahn/Herfert/Lange* 2015, 14.

Bei der *Internetkommunikation (Surfen)* werden abgerufene Webseiten zwischen Server und Nutzer übertragen. Dabei werden die Protokolle HTTP für Klartext-Übertragung, oder HTTPS für verschlüsselte Übertragung verwendet.[181]

4.7 E-Mail-Dienste

Ein besonderer Schwerpunkt für Kommunikationsverschlüsslung ist unter den verschiedenen Kommunikationsformen die E-Mail-Kommunikation. Der Verbreitungsgrad von E-Mail und die Universalität der Einsatzszenarien und möglichen Kommunikationsinhalte, machen diese Kommunikationsform besonders relevant.[182]

Bei der E-Mail-Kommunikation können Textnachrichten, aber auch digitale Inhalte aller anderen Art ausgetauscht werden.[183] Dabei wird die E-Mail vom Gerät – PC oder mobiles Gerät – des Absenders zunächst zum E-Mail-Server des Absenders gesandt. Von dort wird sie zum E-Mail-Server des Empfängers weitergeleitet und dort vom Empfänger heruntergeladen. Um E-Mail-Kommunikationsinhalte vor unbefugtem Zugriff zu schützen, muss eine E-Mail daher sowohl auf dem Transportweg sowie auf den Mailservern von Absender und Empfänger sicher vor dem Zugriff Unbefugter sein.

E-Mail-Dienste sind Telekommunikationsdienste im Regelungsbereich des Telekommunikationsgesetzes. Es handelt sich bei E-Mail um Telekommunikation im Sinn der Begriffsbestimmung von § 3 Nr. 22 TKG, also der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Mithin gilt für E-Mail-Anbieter in Deutschland das Telekommunikationsgesetz. Dies gilt nicht nur für die datenschutzrechtliche spezielle Erlaubnisnorm nach § 107 TKG, die Nachrichtenübermittlungssysteme mit Zwi-

181 S. *Hahn/Herfert/Lange* 2015, 15f.
182 S entsprechend *Hahn/Herfert/Lange* 2015, 16 ff.
183 S. *Hahn/Herfert/Lange* 2015, 16f.

schenspeicherung,[184] sondern auch für andere, allgemeinere Regelungen, wie etwa das Fernmeldegeheimnis nach § 88 TKG.[185] Es gelten aber auch die Erlaubnistatbestände für Ermittlungsbehörden und Nachrichtendienste.

Gleichzeitig handelt es sich bei den Diensten um Telemediendienste im Sinne des Telemediengesetzes. Es herrscht eine Doppelregulierung nach Telekommunikationsgesetz und Telemediengesetz, soweit es sich um einen „reinen" E-Mail-Dienste handelt, der lediglich die Übertragung von Nachrichten ermöglicht, die der Nutzer selbst auf seinem Computer verfasst hat.[186] E-Mail-Dienste, die über die Übertragungsfunktion hinaus ein im Internet verfügbares Angebot machen, sind auch als Telemedien einzustufen.[187]

Die im Zug der Diensterbringung vorgenommen Verschlüsselung der Kommunikationsinhalte sind weder speziell im Telekommunikationsgesetz noch im Telemediengesetz geregelt, so dass die jeweils allgemeinen Bestimmungen gelten und auf die Inhaltsverschlüsselung anzuwenden sind. Sowohl nach Telekommunikationsgesetz als auch nach Telemediengesetz ist es den E-Mail-Diensten nicht verboten, Inhaltsverschlüsselung anzuwenden. Auch dem Nutzer steht es frei, seine Nachrichten zu verschlüsseln.

4.8 Rechtstaatlicher Zugriff auf E-Mail-Inhalte

Der staatliche Zugriff auf Kommunikationsinhalte, wie zum Beispiel des E-Mail-Verkehrs, ist danach zu differenzieren, ob die jeweilige Ermittlungsmaßnahme dem Durchsuchungs- und Beschlagnahmerecht der §§ 94 ff. und 102 ff. StPO zuzurechnen ist oder sich als Maßnahme der Telekommunikationsüberwachung nach den §§ 100a ff.

184 S. *Klesczewski*, in: Säcker 2013, § 107 TKG, Rn. 3.
185 Zur Ausdifferenzierung des Schutzbereichs in Bezug auf E-Mail Dienste BVerfGE 115, 166; s. auch *Eckhardt*, in: Spindler/Schuster 2015, § 88 TKG, Rn. 12.
186 *Holznagel/Schuhmacher*, in: Geppert/Schütz 2013, Einl. C., Rn. 24.
187 BT-Drs. 16/3078, 13.

StPO darstellt.[188] Möglich ist es jedenfalls, dass verschlüsselte E-Mail-Nachrichten aufgrund einer der Vorschriften beim Sender, beim Empfänger oder bei einem zwischengeschalteten E-Mail-Dienst sichergestellt oder beschlagnahmt werden oder dort im Wege der Telekommunikationsüberwachung in den Besitz der Ermittlungsbehörden kommen. Beschuldigte sind grundsätzlich nicht verpflichtet, sich zur Beschuldigung zu äußern, und sind nach § 136 Abs. 1 StPO auch dementsprechend zu belehren. Niemand ist verpflichtet sich selbst zu belasten. Dieses Prinzip (nemo-tenetur) ist ein Kernstück des Rechts auf ein faires Verfahren und ein übergeordneter verfassungsrechtlicher Grundsatz. Beschuldigte zur Herausgabe von verwendeten Schlüsseln oder Passwörtern zu verpflichten, würde gegen dieses Prinzip verstoßen und wäre daher verfassungswidrig.[189] Dritte (nicht beschuldigte) Personen sind dagegen nach geltender Rechtlage als Zeugen verpflichtet, Passwörter zu nennen und Daten in ihrem Gewahrsam herauszugeben.[190] Dazu zählen auch E-Mail-Dienste-Anbieter. Die Herausgabe von Passwörtern und Schlüsseln kann ihnen gegenüber nach § 95 StPO angeordnet werden.[191] Darüber hinaus sind Telekommunikationsdiensteanbieter zur Zusammenarbeit mit staatlichen Sicherheitsbehörden verpflichtet und können sogar im Rahmen einer institutionalisierten Telekommunikationsüberwachung zur Vorhaltung und Herausgabe von Schlüsseln verpflichtet werden. In Fällen angeordneter Telekommunikationsüberwachung nach der Strafprozessordnung, dem Gesetz zu Art. 10 GG, dem Zollfahndungsdienstgesetz, dem Bundeskriminalamtsgesetz oder nach Landesrecht sind die Diensteanbieter nach § 8 Abs. 3 Satz 1 Telekommunikationsüberwachungsverordnung (TKÜV) verpflichtet, Schlüssel und Passwörter bei netzseitig verschlüsselter Telekommunikation ebenfalls zu speichern und den

188 S. *Graf*: in: BeckOK StPO 2015, § 100a StPO, Rn. 27f., zur Bewertung der einzelnen Phasen der E-Mail-Versendung.

189 Ausführlich dazu *Gerhards* 2010, 294 ff.

190 *Gerhards* 2010, 301f.

191 *Wicker*, MMR 2013, 765.

Sicherheitsbehörden bereitzustellen.[192] Dies umfasst die Verschlüsselung, die durch den Diensteanbieter selbst vorgenommen wird. Betroffen sind damit alle E-Mail-Dienste, die für ihre Nutzer die Schlüssel generieren, verwalten und Nachrichten automatisiert verschlüsseln.

4.9 Rechtsfortbildung

Aus der geschilderten Risikolage und dem Angebot und der Verbreitung von Techniken zur Sicherung von Kommunikationsinhalten stellen sich für die Rechtsfortbildung unterschiedliche Fragen und Aufgaben. Diese Fragen müssen im Rahmen weiterer Untersuchungen vertieft erörtert werden. In diesen könnte auch der gesetzliche Anpassungsbedarf detailliert werden. Vorgestellt werden hier sich stellende Rechtsfragen als Forschungsfragen.

4.9.1 Verschlüsselter E-Mail-Verkehr mit Behörden

Seit dem 1. Januar 2015 ist gemäß § 2 E-Government-Gesetz (eGovG) jede Behörde die Bundesrecht ausführt, verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente, zu eröffnen. Zur Eröffnung eines elektronischen Zugangs für De-Mail sind die Behörden des Bundes erst ein Jahr, nachdem das geplante zentrale „De-Mail-Gateway“[193] seinen Betrieb aufgenommen hat, verpflichtet.[194] Auch außerhalb dieser Verpflichtung nutzen viele Behörden der Länder und des Bundes bereits E-Mail zur Kommunikation mit dem Bürger. Um verschlüsselt kommunizieren zu können, müssen beide Kommunikationspartner an dem Verschlüsselungsverfahren teilnehmen.[195] Auch der an Selbstdatenschutz interessierte und informierte Bürger kann nicht sicher mit der Behörde elektronisch kommunizieren, wenn diese ihm dazu keine Möglichkeit zur Verfügung stellt.

---

192 *Gerhards* 2010, 408.

193 S. BT-Drs. 17/11473, 34.

194 Art. 31 IV Gesetz zur Förderung der elektronischen Verwaltung, s. *Roßnagel*, NJW 2013, 2710 ff.

195 S. *Hahn/Herfert/Lange* 2015, 9.

Deswegen sollten Behörden grundsätzlich verpflichtet sein, sich an Verschlüsselungsverfahren zu beteiligen, um sowohl verschlüsselte Nachrichten empfangen als auch versenden zu können.[196] Hierzu ist die Behörde bei der Übermittlung personenbezogener Daten gemäß Abs. 2 der Anlage zu § 9 Abs. BDSG ohnehin verpflichtet.[197] Auch § 87a Abs. 1 Satz 3 AO verpflichtet die Finanzbehörden ausdrücklich, „die Daten mit einem geeigneten Verfahren zu verschlüsseln", wenn sie Daten übermitteln, die dem Steuergeheimnis unterliegen. Darüber hinaus könnte in § 30 VwVfG und § 35 SGB I und anderen Regelungen zur Geheimhaltung ebenfalls ausdrücklich festgelegt werden, dass die Wahrung des Verwaltungsgeheimnisses bei der elektronischen Übermittlung eine Verschlüsselung der Nachricht voraussetzt.[198] Nur wenige zusätzliche Worte in diesen Regelungen hätten Millionen Kosten erspart, die immer noch aufgebracht werden müssen, weil immer wieder neu darüber diskutiert werden muss, ob für diese oder jene Anwendung eine Verschlüsselung erforderlich ist oder ob auf sie verzichtet werden kann.

Diese gesetzliche Regelung müsste mit entsprechenden Verwaltungsanweisungen verbunden werden, die einheitlich für alle Behörden festlegen, welche Verschlüsselungsstandards zu verwenden sind und wie die Verfahren in der Behörde organisatorisch zu implementieren sind. Festzulegen wäre auch wie die Behörden bei einer verbreiteten Verwendung von verschlüsselter Kommunikation die elektronischen Akten und deren Aufbewahrung und Langzeitarchivierung technisch und organisatorisch auszugestalten haben.

4.9.2 Verpflichtende Verschlüsselungsangebote

Ein funktionierender Selbstdatenschutz von Kommunikationsinhalten setzt voraus, dass sich möglichst viele Kommunikationsteilnehmer an

---

196 Zu dieser Forderung *Nedden* 2001, 67 ff.; *Roßnagel*, DÖV 2001, 230; *Hansen*, DuD 2014, 439 (441).

197 S. Kapitel 4.3.

198 S. hierzu *Roßnagel*, NJW 2003, 475.

Verschlüsselungsverfahren beteiligen. Zu untersuchen ist deswegen, ob die die Kommunikation ermöglichenden Diensteanbieter verpflichtet werden sollen, Verschlüsselungstechniken anzuwenden und ihren Nutzern anzubieten.[199] So wird die Transportverschlüsselung bereits von vielen Anbietern werbewirksam durchgesetzt.[200] Fraglich ist, ob alle Anbieter dazu verpflichtet werden können.

In Folge der NSA-Ausspähungen ist eine Zunahme an verfügbaren Lösungen der Verschlüsselung zu beobachten. Dies betrifft Verschlüsselungsapplikationen für Messagingdienste oder Chat und zeigt sich am deutlichsten im Bereich der E-Mail-Kommunikation. So garantieren zahlreiche E-Mail-Provider mittlerweile eine konsequente Transportverschlüsselung zu anderen Providern und den Endgeräten des Kunden. Die dabei verwendeten Verschlüsselungsmechanismen entsprechen jedoch nicht immer dem aktuellen Stand der Forschung. Obwohl Lösungen zur Ende-zu-Ende-Verschlüsselung einen über Transportverschlüsselung hinausgehenden Schutz bieten, werden diese kaum genutzt.[201]

Deswegen ist zu untersuchen, ob Telekommunikationsdiensteanbieter verpflichtet werden können, über die Transportverschlüsselung hinaus Methoden der Inhaltsverschlüsselung anzubieten, Schlüssel zu genieren, zu verwalten und dienstanbieterübergreifend auszutauschen. Die technische Ausgestaltung solcher Angebote ist anspruchsvoll, wird von einigen Anbietern aber bereits erbracht und beworben.[202]

Für Telemedien und Telekommunikation besteht bereits eine Verpflichtung der Anbieter nach § 13 Abs. 4 Nr. Nr. 3 TMG und § 109 Abs. 1 TKG die Vertraulichkeit der übertragenen Daten sicherzustellen. Dies kann auch eine Verschlüsselung der Telemedien und Tele-

199 Zu dieser Forderung ZD-Aktuell 2014, 04209.
200 S. zu „E-Mail-made in Germany“ *Hahn/Herfert/Lange* 2015, 20.
201 S. zu „E-Mail-made in Germany“ *Hahn/Herfert/Lange* 2015, 40f.
202 S. *Hahn/Herfert/Lange* 2015, 23.

kommunikation voraussetzen.[203] Diese Regelungen sind sowohl mit Primär und Sekundärrecht der Europäischen Union als auch mit der grundrechtlich verbrieften Eigentumsgarantie und Berufsausübungsfreiheit der Anbieter vereinbar. Das verpflichtende Angebot für eine Ende-zu-Ende-Verschlüsselung setzt jedoch zusätzlich zu der bisher betriebenen Leitungsverschlüsselung weitere belastende Maßnahmen der Telekommunikations- und Telemedienanbieter voraus. Zwar könnten entsprechende Verpflichtungen in § 13 TMG und § 109 TKG aufgenommen werden. Doch setzt dies unionsrechtlich und verfassungsrechtlich den Nachweis voraus, dass die bisher angebotenen und praktizierten Formen der Verschlüsslung unzureichend sind, um einen ausreichenden Schutz des Fernmeldegeheimnisses und der personenbezogene Daten zu gewährleisten. Nur dann kann die Verpflichtung als erforderlich und damit verhältnismäßig gelten.

4.9.3 Verschlüsselung in elektronischen Einschreibediensten

Mit De-Mail steht in Deutschland ein hoheitlich kontrollierter elektronischer Einschreibedienst zur Verfügung. Der Dienst sieht eine Transportverschlüsselung jedoch keine standardmäßige Ende-zu-Ende-Verschlüsselung vor. Zu untersuchen ist, ob eine dienstseitig angebotene Ende-zu-Ende-Verschlüsselung technisch und rechtlich eingeführt werden kann. Ebenso wenig fordert dies die eIDAS-VO hinsichtlich der technischen und rechtlichen Ausgestaltung der elektronischen Zustelldienste. Auch in diesem Fall setzt eine rechtliche Verpflichtung zur standardmäßigen Ende-zu-Ende-Verschlüsselung unionsrechtlich und verfassungsrechtlich den Nachweis voraus, dass die bisher angebotenen und praktizierten Formen der Verschlüsslung unzureichend sind, um einen ausreichenden Schutz des Fernmeldegeheimnisses und der personenbezogene Daten zu gewährleisten.

Nach § 7 Abs. 1 De-Mail-Gesetz hat der akkreditierte De-Mail-Diensteanbieter eine Ende-zu-Ende-Verschlüsselung zumindest insoweit zu

[203] S. Kapitel 4.3.

unterstützen, dass er einen Verzeichnisdienst führt, in dem Nutzer auch ihre öffentlichen Schlüssel hinterlegen können. Eine entsprechende Regelung sieht die eIDAS-VO zu elektronischen Zustelldiensten jedoch nicht vor. Eine solche Regelung sollte jedoch ergänzt werden. Sie erscheint verhältnismäßig, weil sie das Sicherheitsniveau der Zustelldienste deutlich erhöht, ohne vom Anbieter einen unvertretbaren Aufwand zu verlangen.

4.9.4 Verschlüsselung durch eID-Mittel

Der neue Personalausweis setzt zwar zur elektronischen Identifizierung Verschlüsselungstechnik ein, bietet aber von sich aus keine Möglichkeit zur Verschlüsselung von Inhaltsdaten. Zu untersuchen wäre, inwieweit mit der Infrastruktur und Technik hinter dem neuen Personalausweis, auch eine Public Key-Infrastruktur zur Verschlüsselung von Inhaltsdaten angeboten werden könnte. Als zusätzliche Leistung der deutschen Infrastruktur des deutschen Personalausweises dürfte dies mit Art. 6 eIDAS-Verordnung vereinbar sein, wenn dieses Angebot nicht auch von anderen nach Art. 9 eIDAS-VO notifizierten Identifizierungssystemen als Voraussetzung für eine Anerkennung in Deutschland gefordert würde. Auch wäre zu prüfen, ob und inwieweit sich das eID-Mittel und dahinterliegende Infrastrukturen zu nutzerfreundlichen Lösungen und Angeboten für Schlüsselverwaltung und Schlüsselverteilung ausbauen lassen.[204]

[204] S. *Hahn/Herfert/Lange* 2015, 39.

5 Verbindungsdaten

Verbindungsdaten sind die bei Kommunikationsvorgängen anfallenden Metadaten. Sie beinhalten unter anderem, wer wann wie mit wem kommuniziert hat. Diese Kommunikations-Metadaten sind Daten, die Informationen über andere Daten enthalten.[205] Für den Schutz der Grundrechte in der elektronischen Kommunikation sind Verbindungsdaten besonders wichtig. Indem diese Daten in großem Umfang gesammelt und analysiert werden, zum Beispiel im Rahmen der Vorratsdatenspeicherung oder durch die NSA, lassen sich Profile der einzelnen Kommunikationspartner erstellen, und Beziehungen zwischen den Kommunikationspartnern erkennen.[206] Die Analyse von Metadaten ist hinsichtlich der technischen Performanz vielversprechend, da die anfallenden Daten durch den Wegfall der Kommunikationsinhalte deutlich geringer sind.[207]

5.1 Begriffsbestimmung Verbindungsdaten

Der Begriff Verbindungsdaten wird nicht legaldefiniert, weder im Telekommunikationsrecht noch im Telemedienrecht und auch nicht im Datenschutzrecht. In § 2 Nr. 4 Telekommunikations-Datenschutzverordnung (TDSV), die am 25. Juni 2004 außer Kraft trat, wurden Verbindungsdaten noch als personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden, definiert. Der Begriff Verbindungsdaten wird außerdem noch in § 45g Abs. 1 Nr. 4 TKG und § 45i Abs. 1 Satz 2 TKG verwendet und bezieht sich dort auf zur Tarifierung und Preisermittlung notwendiger Weise zu erhebenden Daten. Dabei kann es sich um Metadaten zu Kommunikations-

205 S. *Hahn/Herfert/Lange* 2015, 42.
206 S. hierzu z. B. *Roßnagel/Moser-Knierim/Schweda* 2013, 127 ff.
207 S. *Hahn/Herfert/Lange* 2015, 42.

partner, Zeit, Dauer, Entfernung und Volumen von erbrachten Telekommunikationsdiensten handeln.[208]

5.1.1 Definition Verkehrsdaten

Im Telekommunikationsgesetz ist jedoch der Begriff Verkehrsdaten definiert. Der Begriff Verkehrsdaten geht auf die Definition in Art. 2 lit. b) der Datenschutzrichtlinie[209] zurück.[210] Er folgt dabei dem Begriff Verbindungsdaten aus § 2 Nr. 4 TDSV.

Nach § 3 Nr. 30 TKG sind Verkehrsdaten, Daten die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Das sind alle Daten, die bei der einzelnen Inanspruchnahme eines Telekommunikationsdienstes entstehen, zum Beispiel Beginn, Dauer und Ende einer Verbindung, Rufnummer des Anrufers sowie des Angerufenen, Standorte von Anrufer und Angerufenem, soweit beide Mobilfunkgeräte benutzen, und Datenmenge einer Nachricht.[211] Außerdem sind Verkehrsdaten die Leitwege, das verwendete Protokoll, Format der Nachricht, das Netz, von dem die Nachricht ausgeht und an das gesendet wird, die in Anspruch genommene Telekommunikationsdienstleistung, die Endpunkte von festgeschalteten Verbindungen sowie deren Zeitpunkt und Dauer und sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung erforderlichen Verbindungsdaten.[212] Es handelt es sich dabei um Daten, die beim Telekommunikationsvorgang selbst anfallen, denn im Unterschied zu Bestandsdaten beruhen Verkehrsdaten regelmäßig nicht auf willentlichen Angaben des Teilnehmers, sondern fallen automatisch bei der Erbringung von Telekommunikationsdiens-

---

208 S. *Ditscheid/Rudloff,* in: Geppert/Schütz 2013, § 45g TKG, Rn. 3 ff.

209 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

210 Dabei dem Begriff Verbindungsdaten aus § 2 Nr. 4 TDSV folgend, so *Säcker*, in: ders. 2013, § 3 TKG, Rn. 89.

211 *Graf*, in: Graf, BeckOK StPO 2015, § 3 TKG, Rn. 20.

212 *Ricke,* in: Spindler/Schuster 2015, § 3 TKG, Rn. 49.

ten an. Die Verkehrsdaten sind somit umfangreicher und wesentlich sensitiver als die Bestandsdaten nach § 3 Nr. 3.[213] Zu den Verkehrsdaten gehören insbesondere gemäß § 96 Abs. 1 TKG die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit, der vom Nutzer in Anspruch genommenen Telekommunikationsdienst sowie die Endpunkte von festgeschalteten Verbindungen. Hierunter fallen insbesondere IP-Adressen.

5.1.2 Definition Nutzungsdaten

Im Telemediengesetz haben die Metadaten zur Erbringung der Telemedien einen eigenen begriff erhalten, nämlich Nutzungsdaten. Nach § 15 Abs. 1 TMG sind Nutzungsdaten all die Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Nutzungsdaten sind insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien.[214]

5.1.3 Eigene Begriffsbestimmung Verbindungsdaten

In der juristischen Literatur und Rechtsprechung werden die Begriffe Verbindungsdaten und Verkehrsdaten aufgrund der Gesetzesentwicklung zuweilen synonym verwendet.[215] Teilweise gelten auch die Nutzungsdaten als Verbindungdaten. Im Folgenden wird der Begriff Verbindungsdaten jedoch allgemeiner verwendet und meint mehr als Verkehrsdaten. Er meint alle Verkehrsdaten im Sinn des Telekommunikationsgesetzes, alle Nutzungsdaten im Sinn des Telemediengesetzes, aber auch alle Arten von Metadaten die bei telemedialen und teledienstlichen Vorgängen anfallen können und die dazu dienen können, den oder die Nutzer zu identifizieren.

---

213 *Ricke,* in: Spindler/Schuster 2015, § 3 TKG, Rn. 49.
214 S. näher *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 42 ff.
215 Begründung von BVerfGE 125, 260.

5.2 Gefährdungslage

Bei allen modernen Kommunikationstechniken fallen Verbindungsdaten in verschiedenen Formen an. Im Rahmen des Pro Privacy-Projekts wurden die bei E-Mail, Messagingdienst, Telefonkommunikation und bei der Nutzung des Web anfallenden Verbindungsdaten betrachtet.[216]

Bei der *E-Mail-Kommunikation* lassen sich Informationen aus dem E-Mail-Header als Metadaten nutzen. Das sind Name, E-Mail und IP-Adresse von Sender und Empfänger, Betreff, Datum, Uhrzeit, Zeitzone und Eindeutige ID der Nachricht. Eine Analyse eines kompletten E-Mail-Verkehrs einer Person über einem längeren Zeitraum lässt den Beobachter leicht soziale Beziehungen und Änderungen im Leben des Betroffenen erkennen, wie zum Beispiel Umzüge, neue Jobs oder Abschluss des Studiums. Auch die Intensität der Beziehung zu einzelnen Kontakten kann anhand der Häufigkeit der Kommunikation abgeschätzt werden. Die Analyse ist ohne jeglichen Zugriff auf die Inhalte der E-Mails möglich.[217]

Bei *Messagingdiensten*[218] werden neben den eigentlichen Inhalten noch zusätzliche Informationen zwischen den Nutzern übertragen. Die anfallenden Metadaten sind vom verwendeten Protokoll abhängig, beinhalten aber bei den nicht auf sichere Kommunikation spezialisierten Diensten normalerweise mindestens Sender, Empfänger und Datum sowie die Uhrzeit der Nachricht. Damit sind die gleichen Analysen möglich wie bei den E-Mail-Verbindungsdaten.[219]

Bei der *Telefonkommunikation* sind die anfallenden Metadaten die Telefonnummern der beiden Kommunikationspartner, der Zeitpunkt, die Dauer und die Häufigkeit der Kommunikation. Auch hier lassen sich Beziehungsgraphen erstellen. Im Mobilfunk kommen hinzu die ein-

---

216 S. *Hahn/Herfert/Lange* 2015, 42.
217 S. *Hahn/Herfert/Lange* 2015, 44.
218 S. Kapitel 4.6.
219 S. *Hahn/Herfert/Lange* 2015, 45.

deutige Kennung des Telefons (IMEI), die eindeutige Kennung der SIM-Karte (IMSI) und die Kennung der Funkzelle, in der sich der Nutzer aktuell aufhält. Bewegt sich der Nutzer während er telefoniert, lässt sich anhand der vom ihm durchquerten Funkzellen ein Bewegungsprofil erstellen. Bei Voice-Over-IP können, abhängig vom verwendeten Protokoll, Metadaten anfallen, wie Betreff, Name und SIP-Adresse oder Telefonnummer von Sender und Empfänger und Eindeutige ID der Unterhaltung (Call-ID).[220]

Bei der *Web-Kommunikation* werden Webseiten mittels Browsern aufgerufen.[221] Dabei werden die auf Servern im Internet abgelegten Informationen über HTTP (unverschlüsselt) oder HTTPS (verschlüsselt) vom Nutzer abgerufen und im Browser des Nutzers dargestellt. Neben dem Inhalt der Seite werden auch hier zusätzliche Metainformationen übertragen, wie die Adresse des Servers und der abgerufenen Webseite, das Datum und Uhrzeit des Webseitenaufrufs, die vom Benutzer eingegeben Daten wie Login und Passwörter, die IP-Adresse des Nutzers[222] und damit indirekt auch die Position des Nutzers, Angaben über die verwendete Software (Browser, Betriebssystem) und über die Hardware (Bildschirmauflösung) sowie Cookies und zwischengespeicherte Daten. Wird der Standard HTTP verwendet, bei dem alle Daten im Klartext übertragen werden, sind all diese Informationen für Angreifer mit Zugriff auf die Verbindung sichtbar. Bei der Verwendung von HTTPS werden einige dieser Daten verschlüsselt übertragen und sind daher für Außenstehende nicht ohne weiteres zugreifbar.[223]

Da alle diese Daten unter anderem beinhalten können, wer wann mit wem kommuniziert hat, und sie leicht im großen Umfang gesammelt und analysiert werden können, lassen sich Profile auch über einzelne

220 S. *Hahn/Herfert/Lange* 2015, 47f.
221 S. *Hahn/Herfert/Lange* 2015, 49.
222 Damit indirekt auch die ungefähre Position des Nutzers.
223 Felder wie Quell- und Zieladresse bleiben allerdings auslesbar.

Nutzer erstellen und Beziehungen zwischen den Nutzern erkennen. Werden diese Daten gesammelt, verraten sie Details über alle betroffenen Personen. Sie lassen sich einfach strukturieren, verarbeiten und miteinander verknüpfen. Der technologische Fortschritt hat die Speicherung und die erforderliche Rechenleistung möglich gemacht. Dadurch sind neue Wege entstanden, große Mengen dieser Daten zu rastern und Strukturen zu erkennen.

So lassen bei der Web-Kommunikation anhand der gesammelten Daten die Interessen und das Verhalten der Nutzer analysieren, und es können Profile erstellt werden, deren Detailgrad mit der Menge an gesammelten Informationen ansteigt. Diese Techniken werden allerdings nicht nur von Geheimdiensten oder anderen Angreifern verwendet, sondern auch von normalen Webseiten-Betreibern. Deren Ziel ist es, Nutzer wiederzuerkennen und ihnen, etwa in einem Online-Shop, passende Kaufempfehlungen anzuzeigen.[224]

5.3 Schutzmöglichkeiten

Für den Schutz der Verbindungsdaten gibt es unterschiedliche Möglichkeiten.[225] Zunächst kann der Nutzer versuchen, dass entstehen von Verbindungsdaten zu vermeiden.[226] Vermeidungsstrategien sind abhängig von der Kommunikationsart. Sie haben – je nach Kommunikationsart unterschiedliche – Aussichten auf Erfolg.

Eine anonyme Nutzung des Web kann durch die Verwendung von Anonymisierungsdiensten wie TOR oder JonDonym erreicht werden. Dabei werden alle Daten auf dem Computer des Nutzers mehrfach verschlüsselt und über mehrere Knoten zum eigentlichen Ziel geleitet. Durch die verwendeten Verschlüsselungsverfahren kennt keiner der beteiligten Partner sowohl die Quelle als auch das Ziel der Kommuni-

224 S. *Hahn/Herfert/Lange* 2015, 50.
225 S. *Hahn/Johannes/Lange*, DuD 2015, 71 (72f.).
226 Dazu und den technischen Möglichkeiten *Hahn/Herfert/Lange* 2015, 45, 46 und 48.

kation. Eine Re-Identifizierung ist damit sehr schwierig, wenn auch nicht ganz unmöglich.[227]

Bei der E-Mail-Kommunikation gibt es keine direkte Möglichkeit, alle Verbindungsdaten zu verschleiern. Selbst bei der Verwendung von Ende-zu-Ende-Verschlüsselung, z.B. mittels OpenPGP, fallen immer noch Verbindungsdaten an, die sich aufgrund des Aufbaus des E-Mail-Protokolls auch nicht vermeiden lassen. Hierzu gehören unter anderem die Adressen von Sender und Empfänger.

Für die bei der Mobilkommunikation anfallenden Verbindungsdaten gibt es nur sehr wenige Möglichkeiten zur Anonymisierung. Anonyme SIM-Karten und die Verwendung von Internet-basierten Kommunikationsdiensten verringern die anfallenden Verbindungsdaten, eine komplette Vermeidung ist hier allerdings nicht möglich.

Ein Schutz von Verbindungsdaten auf persönlicher Ebene durch Verwendung von Anonymisierungsdiensten ist also nicht immer möglich. Den Nutzern stehen nicht für alle Kommunikationsarten Möglichkeiten zur Verschleierung oder Vermeidung der Metadaten zur Verfügung, womit eine durchgängige Wahrung der Anonymität nicht gewährleistet werden kann.[228]

Der Umgang mit Verbindungsdaten ist daher im Kontext einer möglichen Anonymisierung durch den Nutzer zu betrachten. Herausgestellt werden müssen die Möglichkeiten und das Recht auf Anonymisierung im Rahmen der Internetkommunikation.

Im Pro Privacy-Teilvorhaben Technik wurde durch das Fraunhofer-Institut SIT die Anonymisierungsmethoden zu den verschiedenen Kommunikationsformen dargestellt und die verfügbaren Techniken zum Schutz der Verbindungsdaten bewertet. Als besonderer Schwerpunkt wurde dabei die Web-Kommunikation gesehen.[229] Der Verbrei-

---

[227] Siehe dazu auch unten Kapitel 5.9.
[228] S. *Hahn/Herfert/Lange* 2015, 48.
[229] S. *Hahn/Herfert/Lange* 2015, 49.

tungsgrad der Web-Nutzung und die Universalität der Einsatzszenarien und möglichen Verbindungsdaten machen diese Kommunikationsform besonders relevant.

5.4 Anonymität, Anonymisierung und Pseudonymisierung

Innerhalb von Kommunikationsbeziehungen im Web bedeutet Anonymität, dass eine Person (namentlich) nicht identifiziert werden kann. Außerdem muss die Person im öffentlichen Raum frei von Überwachung und Kontrolle ihrer Identität handeln können.[230] Das Bundesverfassungsgericht hat außerdem im Zusammenhang mit dem Volkszählungsurteil und dem Grundrecht auf informationelle Selbstbestimmung den Begriff der „faktischen Anonymität" geprägt. Diese liegt vor, wenn die Identität einer Person verschleiert wird, so dass nach der Lebenserfahrung eine Zuordnung des Namens zu der Person nicht zu erwarten ist.[231] Im Web geht es häufig darum, ob eine dritte Person die Identität der an der Kommunikationsbeziehung beteiligten Personen aufdecken kann. Insoweit ist von Bedeutung, dass eine Dreiecksbeziehung besteht. Zu unterscheiden ist zwischen den beiden an der Kommunikationsbeziehung unmittelbar beteiligten Personen, also Sender und Empfänger der Daten, die über das Web vermittelt werden, sowie der Beziehung dieser Beteiligten zu einer dritten Person oder technischen Instanz, die in der Lage ist, die Identitäten von Sender und Empfänger, zum Beispiel durch die IP-Adresse, aufzudecken.[232]

Der Begriff der Anonymität ist außerdem von dem der Pseudonymität abzugrenzen. Bei einem Pseudonym wird der tatsächliche Name einer Person durch einen anderen Namen oder durch eine Kennzeichnung ersetzt. Dadurch wird die Identität der Person ebenfalls verschleiert. Im Internet stellt der Username ein Pseudonym dar. Allerdings kann

---

230 *Scheder-Bieschin* 2014, 22.
231 BVerfG, NJW 1984, 419 (423).
232 *Brunst* 2009, 8f.

dadurch, dass die personenbezogenen Daten einer Person im Internet gespeichert werden, das Pseudonym grundsätzlich dem tatsächlichen Namen zugeordnet werden.[233] Im Datenschutzrecht existiert auch eine Legaldefinition des Begriffs der Pseudonymisierung. Gemäß § 3 Abs. 6a BDSG ist Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Damit soll also die Zuordnung des für den Namen eingesetzten anderen Namens oder Kennzeichens zu den tatsächlichen persönlichen Daten des Betroffenen verhindert, zumindest aber erschwert werden. Allerdings ist eine scharfe Abgrenzung zwischen den Begriffen der Anonymisierung und der Pseudonymisierung schwierig, da in beiden Fällen Datenbestände um Identifikationsmerkmale bereinigt werden.[234]

Auch ist der Vorgang der Anonymisierung begrifflich von der Anonymität abzugrenzen. Nach der Legaldefinition in § 3 Abs. 6 BDSG ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

5.5 Identifizierungspflichten

Dort wo Identifizierungspflichten bestehen, kann es keine Anonymität der Betroffenen geben. Im deutschen Recht gibt es jedoch keine allgemeine Verpflichtung des Einzelnen, seine soziale Kommunikation

---

233 *Scheder-Bieschin* 2014, 23.

234 *Roßnagel/Scholz*, MMR 2000, 721 ff.; *Buchner*, in: Taeger/Gabel 2013, § 3 BDSG, Rn. 47; *Härting*, NJW 2013, 2065.

mit anderen Personen unter dem eigenen Namen auszuüben. Dem Einzelnen ist es gestattet, ohne staatlichen Identifizierungszwang mit anderen Menschen sozial zu interagieren.[235] Nur vereinzelt lassen Identifizierungspflichten ausmachen, die gegen ein Recht auf Anonymität stünden:

Eine Pflicht zur Identifizierung gegenüber Behörden ergibt sich unter anderem aus § 1 Abs. 1 PAuswG. Weitere Identifizierungspflichten können etwa im Strafprozess über § 243 Abs. 2 StPO (Vernehmung des Angeklagten über seine persönlichen Verhältnisse) oder § 68 Abs. 1 StPO (Befragung des Zeugen über Vornamen, Nachnamen, Geburtsnamen, Alter, Beruf und Wohnort) auftreten.

Die Identifizierungspflichten betreffen nur den Bereich des öffentlichen Rechts. Beim Umgang zwischen Privatpersonen ist regelmäßig keine Identifizierungspflicht gegeben. Allerdings können sich auch Privatpersonen aufgrund der im Zivilrecht geltenden Privatautonomie gegenseitig zur Angabe von persönlichen Verhältnissen verpflichten.[236]

5.6 Verbindungsdaten und Grundrechte

Der Umgang mit Verbindungsdaten steht im Spannungsverhältnis zwischen Datenschutz und Transparenz. So sollen einerseits Transaktionen, die über das Web stattfinden, nachvollziehbar sein. Der elektronische Handel und Rechtsverkehr benötigt diese Informationen, um funktionieren zu können. Andererseits ist zu fragen, ob und wie ein Recht auf Anonymität als Bestandteil des Grundrechts auf informationelle Selbstbestimmung und anderer – die Privatheit schützender – Grundrechte zu gewährleisten ist.

Dieses Spannungsfeld wird deutlich durch die Entscheidung des Europäischen Gerichtshofs, in der die Richtlinie zur Vorratsdatenspei-

---

235 *Bizer*, in: Bäumler/Mutius 2003, 81.

236 *Brunst* 2009, 196 f.

cherung[237] für ungültig erklärt wurde und damit strengere Maßstäbe für den Datenschutz in Europa gesetzt wurden.[238] Die Vorratsdatenspeicherung, also die Speicherung nur von Verkehrsdaten für einen bestimmten Zeitraum dezentral bei Diensteanbietern, wurde vom Bundesverfassungsgericht lediglich unter sehr engen Voraussetzungen als noch mit dem Grundgesetz vereinbar gehalten.[239] Der Europäische Gerichtshof hält die flächendeckende und anlasslose Vorratsdatenspeicherung mit der Europäischen Grundrechtecharta sogar für ganz und gar unvereinbar und erklärte die europäische Richtlinie für nichtig.[240] Andererseits hat der Bundesgerichtshof die siebentägige Speicherung von dynamischen IP-Adressen als eine Art interner Vorratsdatenspeicherung durch Internet-Access-Provider für zulässig erklärt.[241] Das Urteil des Europäischen Gerichtshofs sahen die Richter des Bundesgerichtshofs nicht als Hinderungsgrund, da es bei der Vorratsdatenspeicherung um die Speicherung von Daten für die Zwecke der Strafverfolgungsbehörden und nicht für die privaten Zwecke der Provider gehe.[242]

5.7 Recht auf Anonymität

Während das Recht auf Anonymität in der Zeit vor der elektronischen Datenverarbeitung kein relevantes Thema der Rechtsordnung und der Rechtswissenschaft war, spielt dieses mit der Zunahmen der Verarbeitung personenbezogene Daten und der Nutzung des Internet eine

---

237 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105, 54).

238 EuGH, Urteil vom 8. April 2014, Az. C-293/12 u.C-594/1 = DuD 2014, 488; s. auch *Roßnagel*, MMR 2014, 372.

239 BVerfGE 125, 260; s. auch *Roßnagel*, NJW 2010, 1238.

240 EuGH, Urteil vom 8. April 2014, Az. C-293/12 u.C-594/1 = DuD 2014, 488; s. auch *Roßnagel*, MMR 2014, 372.

241 BGH, NJW 2014, 2500.

242 S. hierzu kritisch *Roßnagel*, DVBl. 2015, 1211.

immer bedeutsamere Rolle. Nur wenige einfachgesetzliche Vorschriften enthalten ausdrücklich ein Recht auf Anonymität.[243] In den überwiegenden Fällen wird ein solches aus den Grundrechten des Betroffenen abgeleitet.

5.7.1 Anonymität im einfachen Recht

Beispiele für die wenigen einfachgesetzlichen Regelungen sind Folgende: In § 18 Abs. 2 Flugunfalluntersuchungsgesetz, das bei der Untersuchung von Unfällen und Störungen beim Betrieb ziviler Luftfahrzeuge Anwendung findet und dem Bereich der Gefahrenabwehr zuzuordnen ist, muss der Bericht über einen Flugunfall unter Wahrung der Anonymität der an dem Unfall oder an der Störung beteiligten Personen erfolgen.

§ 13 Abs. 6 Satz 1 TMG enthält die Pflicht des Diensteanbieters von elektronischen Informations- und Kommunikationsdiensten, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Ist für einen elektronischen Dienst die Identität des Nutzers nicht relevant, so kann und muss im Interesse der Selbstbestimmung hierauf verzichtet werden können. Damit hat der Nutzer zugleich ein Recht auf anonymes oder pseudonymes Handeln.[244] Problemträchtig ist, dass sich aus dem Inhalt der Vorschrift nicht ableiten lässt, unter welchen Voraussetzungen ein Recht auf Anonymität besteht und wann eine Ausnahme hiervon eingreift. Zumutbar ist ein relativer Begriff, der vor allem von Variablen wie Möglichkeiten der bereits im Unternehmen vorhandenen technischen Systeme, Unternehmensgröße und zur Verfügung stehendes Kapital des durchschnittlichen Anbieters abhängig ist.[245]

---

243 S. dazu auch *Brunst*, 2009, 196.

244 *Roßnagel/Scholz*, MMR 2000, 721 ff.; *Weichert*, in: Killian/Heussen 2008, Teil 13, Verfassungsrechtliche Grundlagen, Rn. 42.

245 *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 130.

5.7.2 Anonymität als Grundrecht

Ein Recht auf Anonymität als Baustein eines Konzepts der Privatheit lässt sich jedoch aus dem Verfassungsrecht ableiten. Das Recht auf Anonymität ist eine (implizite) Regel des Datenschutzrechts und lässt sich – unter anderem als Element des allgemeinen Persönlichkeitsrechts – grundrechtsdogmatisch herleiten.[246] Es folgt aus Art. 2 Abs.1 GG in Verbindung mit Art. 1 Abs. 1 GG sowie Art. 10 GG.[247]

Das Recht auf Anonymität korrespondiert mit der informationellen Selbstbestimmung, wonach jeder selbst entscheidet, wer erfahren soll, welches Handeln von ihm stammt.[248] Das Grundgesetz enthält keine explizite Verankerung eines Rechts auf Anonymität im Internet, aber ein solches ergibt sich aus dessen Wertentscheidungen. Vor allem das aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG hergeleitete Recht auf informationelle Selbstbestimmung beschränkt die Erhebung und Verwendung der den Nutzer identifizierenden Daten. Dadurch kann es „nicht nur zur rechtlich gesicherten Aufrechterhaltung von Anonymität ... , sondern mit dem Gebot der Datensparsamkeit zu historischer Anonymität führen".[249]

Der Inhalt und Schutzbereich des Rechts auf informationelle Selbstbestimmung bezieht sich auf „die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen",[250] und „bewirkt den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten".[251] Hintergrund dieser Ausprägung des allgemeinen Persönlichkeitsrechts ist, dass in der Ära der elektronischen

---

246 *Von Mutius*, in: Bäumler/Mutius 2003, 12 ff.

247 *Heckmann*, NJW 2012, 2631 (2632) leitet es darüber hinaus aus Art. 5 Abs.1 GG und Art. 13 GG her.

248 Zur Möglichkeit der anonymen Internetnutzung BGHZ 181, 328.

249 *Scheder-Bieschin* 2014, 46

250 BVerfGE 65, 1 (43).

251 BVerfGE 65, 1.

Datenverarbeitung keine Daten mehr als *belanglos* bezeichnet werden können. Aufgrund dessen, dass eine sekundenschnelle Erfassung und Weiterleitung von Informationen über sachliche und persönliche Verhältnisse einer Person möglich und demzufolge mittels Kombination von Daten unabhängig vom Willen des Betroffenen ein nahezu vollständiges Persönlichkeitsbild konstruierbar ist, ist es irrelevant, ob es sich um Informationen persönlichen oder privaten Charakters handelt. Vielmehr sind alle personenbezogenen Daten geschützt.[252]

Eine schrankenlose Gewährleistung dieses Rechts auf informationelle Selbstbestimmung ist jedoch nicht anerkannt. Vielmehr sind unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes Einschränkungen im überwiegenden Allgemeininteresse möglich. Daher kann in das Grundrecht aufgrund eines Gesetzes, das den Eingriff eindeutig und spezifisch festlegt, dem überwiegenden Allgemeininteresse dient und verhältnismäßig ist, eingegriffen werden. Der Grundsatz der Verhältnismäßigkeit besagt, dass ein Grundrechtseingriff nur dann verhältnismäßig ist, wenn er einen legitimen Zweck verfolgt und der Eingriff zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen ist.[253]

Auch spielt das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG eine Rolle für das Recht auf Anonymität. Im Hinblick auf den Datenschutz ist dessen relevanter Schutzgegenstand in der Vertraulichkeit der elektronisch vermittelten Kommunikation zu sehen. Der Schutzbereich des Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis vor einer Kenntnisnahme durch die öffentliche Gewalt. Unter Telekommunikation ist die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs zu verstehen.[254] Aus dieser Norm resultiert für den Bürger ein Schutzanspruch, der vor Gefährdungen aufgrund der Verwen-

252 *Wüllrich* 2006, 111 f.
253 BVerfGE 17, 306 (313); BVerfGE 96, 10 (23f.).
254 BVerfGE 125, 260 (309).

dung personenbezogener Daten bewahrt, die sich aus der unberechtigten Kenntnisnahme oder Einwirkung Dritter auf Kommunikationsvorgänge bei der Inanspruchnahme von Kommunikationsleistungen ergeben. Der Vertraulichkeitsschutz bietet dem jeweiligen Nutzer zudem das Recht der Verschlüsselung und Entschlüsselung eigener Nachrichten unabhängig von Telekommunikationsdiensten und staatlichen Regularien.[255] Somit ist auch Anonymität eine Modalität der Kommunikation im Sinne des Art. 10 Abs. 1 GG.[256]

Der Schutzbereich des Art. 10 Abs. 1 GG umfasst aber nicht nur die Inhalte der Kommunikation, sondern auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. Dazu gehören vor allem die Verbindungsdaten, also Angaben darüber, „wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist".[257] Dabei geht es auch um die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen.[258] Der Schutzbereich des Art. 10 Abs. 1 GG erstreckt sich mithin nicht lediglich auf die „Botschaft" selbst, sondern auf jegliche externen Umstände, die die Gefährdung der Vertraulichkeit der Telekommunikation heraufbeschwören können (Fernmeldeumstände). Hiervon erfasst sind daher auch Informationen in Bezug auf Ort, Zeit und Art und Weise des Fernmeldeverkehrs. Vor allem tangiert sind sämtliche Verbindungsdaten, die Informationen über die an der Kommunikation Beteiligten und die Umstände jener liefern.[259]

In den Schutzbereich des Art. 10 Abs. 1 GG wird eingegriffen, „wenn staatliche Stellen sich ohne Zustimmung der Beteiligten Kenntnis von

---

255 *Weidner-Braun* 2012, 84.
256 *Brunst* 2014, 280.
257 BVerfGE 125, 260 (309) mit weiteren Nennungen.
258 BVerfGE 125, 260 (309f.).
259 *Durner*, ZUM 2010, 833 (841f.).

dem Inhalt oder den Umständen eines geschützten Übermittlungsvorgangs verschaffen oder die so gewonnenen Informationen nutzen." Ein Eingriff in den grundrechtlich geschützten Bereich des Fernmeldegeheimnisses liegt demnach vor, wenn die öffentliche Gewalt von Kommunikationsdaten Kenntnis nimmt, sie aufzeichnet und verwertet oder sonstwie verwendet. Die Erfassung von Telekommunikationsdaten, ihre Speicherung, ihr Abgleich mit anderen Daten, ihre Auswertung, ihre Selektierung zur weiteren Verwendung oder ihre Übermittlung an Dritte stellen jeweils eigene Eingriffe in das Telekommunikationsgeheimnis des Betroffenen dar.[260]

Einschränkungen des Fernmeldegeheimnisses dürfen gemäß Art. 10 Abs. 2 Satz 1 GG nur aufgrund eines Gesetzes angeordnet werden. Konkretisiert wird Art. 10 GG unter anderem durch die einfachgesetzliche Regelung des § 88 TKG. Gemäß § 88 Abs. 1 und 2 TKG ist jeder Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet, das den Inhalt der Telekommunikation und ihre näheren Umstände inklusive der Umstände erfolgloser Verbindungsversuche erfasst.

Das Recht auf Anonymität kann sich daneben auch aus dem Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme („Computergrundrecht") erschließen, das ebenfalls aus dem allgemeinen Persönlichkeitsrecht abgeleitet wird und auf Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG basiert. Der Begriff des informationstechnischen Systems erfasst „alle Systeme, die alleine oder im Verbund personenbezogene Daten des Betroffenen enthalten und deren Einsicht durch Dritte dazu führen würde, dass ein ‚Einblick in wesentliche Teile der Lebensgestaltung einer Person' oder sogar ein Persönlichkeitsbild gewonnen werden könnte".[261] Die Vertraulichkeit stellt darauf ab, dass allein Berechtigte befugt sind, auf das System insgesamt und die darauf erzeugten, verarbeiteten und gespeicherten

[260] BVerfGE 125, 260 (309).
[261] BVerfGE 125, 260.

Daten zuzugreifen. Die Integrität ist bei einer Beeinträchtigung des Systems selbst oder seiner Daten verletzt. Das Recht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme tritt neben das auf informationelle Selbstbestimmung und auf Fernmeldegeheimnis, sofern jene keinen oder keinen ausreichenden Schutz sicherstellen. Seine Gewährleistung ist nicht schrankenlos; auf richterliche Anordnung hin können Eingriffe zu präventiven Zwecken oder zur Strafverfolgung in Betracht kommen. Die verfassungsrechtlichen Anforderungen daran, den Kernbereich privater Lebensgestaltung zu schützen, können einzelfallabhängig nach Art der Informationserhebung und der hierdurch erfassten Informationen variieren. Relevanz erfährt dieses Recht vor allem in den Fällen der „Onlinedurchsuchung“ gemäß § 20k Abs. 7 BKAG. Der verdeckte Eingriff in informationstechnische Systeme bezweckt die Bekämpfung der Internetnutzung für terroristische Ziele.

5.8 Anonymität bei der Web-Nutzung

Es gibt verschiedene Möglichkeiten, um den Zugriff auf die anfallenden Verbindungsdaten zu erschweren und die Menge an anfallenden Daten zu verringern. Dazu zählen der Betrieb des Browsers im privaten Modus, die Verwendung von Web-Proxies, die Nutzung von Mix-Netzwerken, das Onion-Routing und die Nutzung von Diensten wie ip2, TOR oder JonDo.[262]

Die zur Verfügung stehenden Techniken gewährleisten die Anonymität des Nutzers unterschiedlich. Eine absolute Anonymität kann keine der zur Verfügung stehenden Techniken bieten.[263] Durch sie lassen sich unterschiedliche Grade von Sicherheit und unterschiedliche Schutzniveaus realisieren. Ein steigender Grad an Schutz ist dabei meistens gleichbedeutend mit einem höheren Einrichtungsaufwand oder dem Verzicht auf bekannte Technologien.

---

262 S. *Hahn/Herfert/Lange* 2015, 50 ff.
263 S. *Hahn/Herfert/Lange* 2015, 57.

So bietet der Privacy-Modus der verschiedenen Browser, Web-Proxies und Virtual Private Networks (VPN) nur *geringe Sicherheit*. Auch wenn ein Anonymisierungs-Dienst zusammen mit den normalen Anwendungen des Nutzers verwendet wird, gibt es verschiedene Möglichkeiten den Nutzer zu identifizieren.[264]

Mittlere Sicherheit bieten die Nutzung von Bundles, also die Verwendung von eingeschränktem Browser und Anonymisierungsdiensten. Die verfügbaren Anonymisierungsbundles beinhalten neben dem eigentlichen Dienst einen speziell angepassten Browser, der bewusst auf Features verzichtet, um die Anonymität des Nutzers zu schützen.[265]

Hohe Sicherheit bieten Lösungen, bei denen das komplette Betriebssystem darauf abgestimmt ist, die Anonymität des Nutzers zu schützen. Damit soll ausgeschlossen werden, dass durch Fehlkonfigurationen Informationen über die Identität des Nutzers nach außen dringen können. Diese Lösungen sind verhältnismäßig schwierig einzurichten und unterscheiden sich in ihrer Nutzung stark von dem, was die meisten Nutzer aus ihrem Alltag gewöhnt sind.[266]

Unabhängig vom Grad der konkreten Sicherheit, bieten Anonymisierungsdienste die Möglichkeit, eine Anonymisierung oder Pseudonymisierung ihrer Nutzer herzustellen, indem sie den Ursprung oder das Ziel einer Kommunikationsverbindung vor Dritten verbergen. Damit helfen sie der Durchsetzung des verfassungsrechtlich geschützten Rechts auf Anonymität.

5.9 Funktionsweise der Anonymisierung im Web

Die Identifizierung von Nutzern im Web ist auf verschiedene Weisen möglich. Abgesehen davon, dass Web-Nutzer freiwillig persönliche Informationen an die Betreiber von Websites weitergeben, gibt es

---

264 S. *Hahn/Herfert/Lange* 2015, 57f.
265 S. *Hahn/Herfert/Lange* 2015, 58f.
266 S. *Hahn/Herfert/Lange* 2015, 58f.

Identifizierungsmöglichkeiten ohne Wissen der Betroffenen, wenn einen Web-Dienst nutzen und innerhalb dessen eine bestimmte URL aufrufen. Unter URL (Uniform Resource Locator) ist allgemein die Adresse eines Dokuments im HTML-Format im Web zu verstehen, das sich aus der Domäne und der Angabe des Ortes des Dokuments auf dem Server zusammensetzt, mittels dessen sich über ein Domain Name System (DNS) die dazugehörige IP-Adresse des aufzusuchenden Servers ergibt.

Mit der Versendung von Daten über das Web wird zugleich die IP-Adresse des Nutzers übermittelt. Unter einer IP-Adresse ist eine Adresse in Computernetzwerken zu verstehen, die auf dem Internetprotokoll (IP) basiert und aus einer bestimmten Abfolge von Zeichen oder Bits besteht sowie dazu verwendet wird, Daten von ihrem Absender zum vorgesehenen Empfänger zu transportieren. Dazu werden den jeweiligen Geräten eine Netzwerkkennung und eine Hostkennung zugewiesen, damit sie im Netz erreichbar sind. Die IP-Adresse wird zumindest für die Dauer der Web-Sitzung eingerichtet. Damit kann die IP-Adresse eindeutig einem bestimmten Rechner zugewiesen werden.[267] Eine weitere Identifizierung und Überwachung von Web-Nutzern ist über die elektronische Werbung möglich, insbesondere durch Cookies und sog. AdWare und SpyWare. Dabei werden zum Beispiel über eine Web-Seite Werbebanner eingeblendet. Durch das Anklicken dieser Banner werden bestimmte Daten heruntergeladen und es kann ein Informationsprofil über das Nutzungsverhalten des jeweiligen Nutzers erstellt werden.[268]

Daraus ergibt sich, dass Web-Nutzer ein Interesse daran haben können, Identifikationsmerkmale zu verbergen. Anonymisierungsdienste, wie etwa JonDonym (früher: AN.ON-Projekt) oder VPN-Provider, bezwecken die Verbergen des Nutzers gegenüber Kommunikationspart-

[267] *Brunst* 2009, 77.
[268] *Brunst* 2009, 79.

nern, wie zum Beispiel Telemedienanbietern, mit der Folge, dass dieser nicht auf die Identität des Nutzers, mittels der IP-Adresse, rückschließen kann.[269] Zu den Kommunikationsakteuren zählen involvierte Anwender, Access- sowie Host- und Content-Provider.[270]

Zudem ist eine Verschlüsselung des Datenverkehrs zwischen Nutzer und Anonymisierungsdienst in Abhängigkeit des verwendeten Protokolls möglich, so dass es weder dem Access-Provider noch einem externen Beobachter (z.B. Nachrichtendienste, öffentliche WLAN-Hotspots) möglich ist zu erkennen, um welche Inhalte es zwischen Nutzer und Anonymisierungsdienst – und damit im Endeffekt auch zwischen Nutzer und Kommunikationsakteur – geht. Anonymisiert wird indes allein der Kommunikationsvorgang, nicht zugleich der Kommunikationsinhalt.[271]

Der Einsatz von datenschutzfördernden Identitätsmanagementsystemen dient dem Einzelnen als Schutz vor ausufernder Überwachung sowie Bewahrung vor Identitätsdiebstahl und Profilbildung.[272] Mittels Anonymisierungsdiensten ist den Nutzern somit das Surfen im Web möglich, ohne hierbei verräterische Datenspuren zurückzulassen.

Die Anonymisierungsdienste basieren auf dem Konzept, schon auf technischer Ebene mittels Verwendung optionaler oder standardisiert auswählbarer hintereinandergeschalteter Server zu verhindern, die IP-Adressen den jeweiligen Nutzern zuordnen zu können. Dies ist in Bezug auf JonDonym durch „Mix-Kaskaden“ der Fall. Diese Vorgehensweise können auch VPN-Provider verwenden, indem die Daten zunächst über einen verschlüsselten VPN-Tunnel zu dem ersten VPN-Server geleitet werden und anschließend in eine (optionale) Kaskade zwecks Einbindung weiterer Server mittels Software (Proxifier, ProxyCap, MyEnTunnel) überführt oder übermittelt werden. Eine benutzer-

269 *Brunst* 2009, 130f.
270 *Brunst* 2009, 47.
271 *Brunst* 2009, 130f.
272 *Heckmann*, in: ders. 2014, Kap. 9, Rn. 269 ff.

freundliche Ausgestaltung zur Kaskadierung über mehrere involvierte VPN-Server stellt beispielsweise die von Perfect-Privacy.com angebotene Client-Software „Multi-Hop OpenVPN Manager“ dar.

Folglich leitet der Anonymisierungsdienst die Informationen Dritter „im eigenen Namen“, also mit seiner IP-Adresse, weiter, so dass für den Empfänger ausschließlich die IP-Adresse des Anonymisierungsdienstes, aber nicht die des ursprünglichen Senders erkennbar ist. Erfolgt keine Protokollierung der Umschreibung, ist eine Zurückverfolgung der Verbindung bis zum eigentlichen Absender nicht mehr möglich. Dies entspricht dem Geschäftsmodell eines Anonymisierungsdienstes. Festzuhalten bleibt aber, dass der Anonymisierungsdienstleister selbst erkennen könnte, welcher Nutzer gerade ihr System nutzt und auch welche Web-Seiten oder Dienste er in Anspruch nimmt.

Der Zugang zum Anonymisierungsdienst wird im einfachsten Fall über ein Web-Interface angeboten, dessen Zugangsseite wie ein selbstständiger Browser fungiert und dessen Bedienung auch so möglich ist. Der Nutzer fügt die gewünschte Internetadresse in ein Formular, das heißt, in die modifizierte Adresszeile des Webbrowsers ein und erhält sofort die erwarteten Daten. Die kontrollierte Headerinformation des Datenpakets weist die gesperrte Seite nicht aus; diese ist vielmehr im Dateninhalt verpackt und mithin für das Kontrollsystem verborgen.[273]

Eine Unterscheidung ist unter anderem denkbar in dezentral und zentral arbeitende Anonymisierungsdienste. Kennzeichen eines dezentral arbeitenden Anonymisierungsdienstes wie etwa TOR ist die Beteiligung vieler Nutzer an der Herstellung von Anonymität. Dies sorgt einerseits für eine geringe Kontrollierbarkeit, aber andererseits für eine größere Gefahr der Verwundbarkeit, falls kompromittierende Systeme eingeschleust werden. Zentrale Anonymisierungsdienste wie zum Beispiel JonDonym oder VPN-Provider wollen diesen Nachteil

[273] *Sieber* 1999, 87f.

mittels einer zentralen Struktur der anonymisierenden Server beseitigen.[274]

Eine Untersuchung der Verbraucherschutzstelle Niedersachsen[275] hat 2011 eine hohe Heterogenität des Markts der Anonymisierungsdienste belegt. Die Studie hat auch ergeben, dass Anonymisierungsdienste IP-Adressen ihrer Nutzer unterschiedlich behandelten und speicherten. Einige speicherten gar nicht, wie die deutsch-rumänische Cyberghost VPN152, die österreichische Hideway VPN153, die deutsche KeyVPN sowie den Anonymisierungsdienst TuVPN aus Singapur. Die amerikanische Hotspot VPN dagegen speicherte IP-Adressen ebenso wie Verbindungszeiten und Benutzername für eine Woche, der chinesische Anbieter Mad VPN speicherte Zeit, Original- und zugewiesene IP-Adresse und Benutzername sogar zwei Jahre. Der zyprische Anbieter VPN Accounts speicherte Verbindungszeiten, Original- und zugewiesene IP-Adressen und Datenvolumen einen Monat lang, der deutsche VPN-Anbieter Tiggers Welt speicherte Verbindungsdaten inklusive IP-Adressen für einen Monat und Datenvolumina summenmäßig jeden Tag. Beim amerikanischen AlwaysVPN fand eine Speicherung der Verbindungsdaten inklusive Zeit und eingehende sowie ausgehende IPAdresse für zwei Wochen statt. Der Anonymisierungsdienst 12VPN aus Hong Kong speicherte alle Verbindungsdaten (eingehende und ausgehende IP-Adresse, Zeiten sowie das übertragene Datenvolumen) drei Monate lang auf Vorrat. Die kanadische VPN Privacy führte eine fünfttägige Speicherung der Verbindungszeiten und IP-Adressen durch. Gleiches galt für den rumänischen Anbieter HideIP VPN. Der amerikanische VPN-Anbieter Solvpn speicherte sämtliche Verbindungsdaten wie Verbindungszeit, Benutzername und IP-Adressen für ein Jahr auf Vorrat.

---

274 *Brunst* 2009, 144.

275 *Verbraucherschutzstelle e.V. Niedersachsen*, Internet-Anonymisierungsdienste, http://verbraucherschutzstelle.de/anonym_surfen.htm.

Aufgrund dieser hohen Heterogenität im Umgang mit den Verbindungsdaten, stellt sich die Frage, welche gesetzlichen Regelungen für Anonymisierungsdienstleister gelten, die deutschem Recht unterliegen.[276]

5.10 Rechtliche Bewertung von Anonymisierungsdiensten

Anonymisierungsdienste dienen dazu, eine Anonymisierung ihrer Nutzer herzustellen, indem sie den Ursprung oder das Ziel einer Kommunikationsverbindung vor Dritten verbergen.[277] Nach deutschem Recht ist die Nutzung von Anonymisierungsdiensten für den Nutzer uneingeschränkt gestattet.[278] Weder das Telekommunikationsgesetz noch das Telemediengesetz und auch nicht das Strafgesetzbuch halten davon ab, die eigene IP-Adresse gegenüber Dritten zu verschleiern. Es gibt keine generelle Verpflichtung, in der sozialen Kommunikation unter dem eigenen Namen zu erscheinen oder sich zu identifizieren. Der Einzelne kann grundsätzlich ohne staatlichen Identifizierungszwang mit anderen Personen oder Telekommunikationsanbietern in Kontakt treten und mit ihnen interagieren. Dieser Grundsatz wird allerdings durch spezifische Verpflichtungen, sich gegenüber anderen identifizieren zu müssen, und durch staatliche Befugnisse, Einzelne identifizieren zu können, begrenzt.[279] Die wichtigste Identifizierungspflicht gegenüber Behörden ergibt sich aus § 1 Abs. 1 PAuswG.[280]

Im Folgenden soll zunächst die Möglichkeit der Diensterbringung durch einen deutschen Anbieter bewertet werden. Anhand der ihm obliegenden Rechte und Pflichten kann die Effektivität der Anonymisierungsleistung rechtlich abstrakt, also über den Einzelfall hinaus,

---

276 Die Frage der Anwendbarkeit deutschen Rechts auf einen ausländischen Anbieter wird nicht behandelt.

277 *Federrath/Golembiewski*, DuD 2004, 486.

278 *Redeker*, in: Hoeren/Sieber/Holznagel 2015, Teil 12, Rn. 473b.

279 Zu denken ist an (privat-)vertragliche Pflichten zur Identifikation und gesetzliche Identifizierungspflichten; s. detailliert dazu *Bizer*, in: Bäumler/Mutius 2003, 78 (81).

280 S. näher Kapitel 5.5.

bewertet werden. Zu klären ist deswegen vor allem die rechtliche Einordnung von Anonymisierungsdiensten. Uneinigkeit besteht in der Frage, ob in Anonymisierungsdiensten Telekommunikations- oder Telemediendienste zu sehen sind. Zur Abgrenzung ist es relevant, welche Funktion einem Anonymisierungsdienst zukommt.[281]

5.10.1 Abgrenzung Telemedien und Telekommunikation

Die Vorschriften des Telemediengesetzes gelten für den elektronischen Geschäftsverkehr. Es findet Anwendung für elektronische Dienstleistungen, soweit sie nicht Telekommunikationsdienste gemäß § 3 Nr. 24 TKG, telekommunikationsgestützte Dienste gemäß § 3 Nr. 25 TKG oder Rundfunk gemäß § 2 des Rundfunkstaatsvertrags sind. Telekommunikationsdienste sind gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Zu den Telekommunikationsdiensten gehören insbesondere die Angebote von Access-Providern, die lediglich den Zugang zum Internet ermöglichen. Dabei geht es um die technische Transportleistung des Sendens, Übermittelns und Empfangens von Daten.[282] Es bestehen unterschiedliche Rechtsmeinungen darüber, ob Anonymisierungsdienste dem Telemedienrecht oder dem Telekommunikationsrecht unterfallen.

Nach einer Auffassung fallen Anonymisierungsdienste unter das Telemediengesetz.[283] Begründet wird diese Auffassung damit, dass sie für eine Veränderung von Webseiten sorgten, als würden automatisch „Worte in eine andere Sprache übersetzt".[284] Aufgrund dessen unterfielen Anonymisierungsdienste nicht dem Regelungsbereich des Telekommunikationsgesetzes, da sie keine Telekommunikationsdienste

---

281 *Brunst*, 2009, 384; zum Meinungsstreit siehe *Heckmann* in: ders. 2014, Kapitel 9, Rn. 274.

282 *Hoeren*, NJW 2007, 801 (802).

283 *Gitter/Schnabel*, MMR 2007, 411 (415); *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 96.

284 *Klink/Straub*, DuD 2008, 123 mit weiteren Nachweisen.

darstellten. Die Unterscheidung zwischen der Zuordnung als Telekommunikationsdienst oder Telemediendienst habe auch für die derzeitige Regelung der Vorratsdatenspeicherung nach §§ 113a ff. TKG Relevanz.[285]

Nach anderer Auffassung seien Anonymisierungsdienste Telekommunikationsdienste.[286] Da Anonymisierungsdienste durch Umleitung von Nachrichten über verschiedene Intermediäre für eine Verschleierung der Beziehung zwischen Quelle und Ziel der Kommunikation sorgten, entspreche diese Einordnung der zugrunde liegenden Technik. Die Adressierungsdaten würden abgewandelt und ihre Inhalte verschlüsselt, was zur Folge habe, dass jeder Intermediär lediglich das notwendige Minimum an Informationen zur Weiterleitung erlange.[287] Der von der Gegenauffassung angenommene automatische Übersetzungsdienst sei vor dem Hintergrund der Funktionsweise einer Mix-Kaskade abzulehnen. Diese würde nach dem Grundsatz verschiedener, vom Absender ineinander verpackter und von außen nicht unterscheidbarer Briefumschläge arbeiten, die für die Intermediäre unter Beachtung ihrer Reihenfolge bestimmt seien. Jeder Intermediär mache dann nur den an ihn adressierten Umschlag auf und gebe den wiederum darin verpackten Umschlag weiter. Hierbei bleibe indes der ursprüngliche Inhalt unangetastet und es finde demnach eben keine Übersetzung in eine andere „Sprache“ statt. Das Einbringen zufälligen „Füllmaterials“ erfolge nur zur Verschleierung der Größe des Inhalts und dazu, „die bei einem Intermediär ein- und ausgehenden Briefe nicht verkettbar zu machen“.[288]

Nach einer dritten Auffassung komme es für die rechtliche Einordnung auf den Schwerpunkt der erbrachten Leistungsteile an.[289] Dabei

---

285 *Heckmann*, in: ders. 2014, Kapitel 9 Rn. 274.
286 *Raabe*, DuD 2003, 134 (135).
287 *Klink/Straub*, DuD 2008, 123.
288 *Klink/Straub*, DuD 2008, 123.
289 *Rau/Behrens*, K&R 2009, 766 (768).

sei davon auszugehen, dass es sich bei Anonymisierungsdiensten um eine hybride Leistungserbringung handelt, da der Inhalt der Daten zunächst verschlüsselt und dann mittels eines Transportprotokolls übertragen werde. Doch lasse sich nicht ohne weiteres und eindeutig feststellen, wann die unterschiedlichen Leistungsteile eines Anonymisierungsdienstes überwiegen. Auch bestehe die Gefahr einer Umgehung der Zuordnung durch Modifizierung der einzelnen Dienste. Des Weiteren wollte der Gesetzgeber durch die gesetzliche Unterscheidung der Telekommunikationsdienste von den Telemediendiensten die verschiedenen Leistungen gerade voneinander trennen. Eine einheitliche Einordnung von Anonymisierungsdiensten nach dem Schwerpunkt der Leistungserbringung würde dem Sinn und Zweck von Telekommunikationsgesetz und Telemediengesetz widersprechen.

Andere Stimmen lassen schließlich Anonymisierungsdienste sowohl dem Telemedienrecht als auch dem Telekommunikationsrecht unterfallen.[290] Ein Anonymisierungsdienst könne als Ganzes auch eine Doppelnatur aufweisen und mithin gleichzeitig Telekommunikationsdienst und Telemedium sein; es bedürfe dann nach einer funktionalen Betrachtungsweise einer Zerlegung in seine Bestandteile und der Anwendung des jeweils einschlägigen Gesetzes auf den in Rede stehenden Bestandteil.[291] Diese Meinung ist vorzugswürdig, da sie eine einzelfallabhängige und damit im Einzelfall gerechte Lösung erlaubt, die sowohl dem Regelungsziel des Telemediengesetzes als auch den Zielen des Telekommunikationsgesetzes dient.

---

290 *Raabe*, CR 2003, 268 (269 ff.).

291 So heißt es auch in der Begründung der Bundesregierung für den „Gesetzesentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“, BR-Drs. 275/07, 167: „Auch Anonymisierungsdienste weisen allerdings eine solche Doppelnatur auf, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste sind daher sowohl Telemedien als auch – im Hinblick auf ihre Transportfunktion – Telekommunikationsdienste für die Öffentlichkeit.“

Zur rechtlichen Einordnung muss folglich die technische Funktionsweise der Anonymisierungsdienste berücksichtigt werden. Dabei verhält es sich so, dass Anonymisierungsdienste sowohl Transportleistungen erbringen als auch die Leistung von Telemedien durch inhaltsrelevante Kommunikation zur Verfügung stellen können. Abzustellen ist deswegen auf die jeweils betrachtete Funktionalität.[292]

Hiernach erbringen Anonymisierungsdienste, die lediglich über ein Web-Interface/Proxy arbeiten, die Anonymisierungsleistung als Telemediendienst. Das Gleiche gilt, wenn sie kompromittierende Elemente aus den Kommunikationsinhalten entfernen oder die Sendungen verschlüsseln. Nur soweit sie Signaltransport übernehmen, sind sie als Telekommunikationsdienst einzuordnen. Insbesondere für die Verwendung von MIX-Kaskaden kommt es entscheidend darauf an, ob die Anonymisierungsdienste für die Übertragung der Nachrichten zwischen den Mixen Telekommunikationsdienste nutzen oder selbst solche für den unmittelbaren Signaltransport zur Verfügung stellen. Soweit diese Dienste nach ihrer technischen Ausgestaltung dem Telekommunikationsgesetz unterfallen, also geschäftsmäßig Anschlusskennungen vergeben oder Telekommunikationsanschlüsse bereitstellen, trifft sie nach § 111 TKG eine Pflicht zur Erhebung und Speicherung bestimmter Bestandsdaten, wie Rufnummer, Name und Anschrift.[293] Die Daten müssen erhoben werden, um sie im Einzelfall an staatliche Ermittlungsbehörden weitergeben zu können

Es sind daher zumeist sowohl Telekommunikationsgesetz als auch Telemediengesetz auf Anonymisierungsdienste anwendbar. Beide Gesetze schließen sich nicht gegenseitig aus, sondern sind im Sinn einer gegenseitigen Ergänzung konzipiert.[294]

---

[292] *Raabe*, DuD 2003, 134 (135f.).

[293] Die Vorschrift ist als Einschränkung des Rechts auf informationelle Selbstbestimmung, wobei nicht in Art. 10 GG eingegriffen würde, noch für verfassungsmäßig befunden worden, s. BVerfGE 130, 151.

[294] *Brunst* 2009, 386

Auch wenn aus der anonymen Nutzung des Web resultiert, dass die Verfasser von illegalen und unerwünschten Inhalten kaum zu ermitteln sind und mithin die Verfolgung von straf- und zivilrechtlichen Haftungsregeln nur unter schwierigsten Umständen möglich ist, sind Anonymisierungsdienste nicht explizit verboten. Ein etwaiges Verbot würde auch wegen des Eingriffs in die Berufs- und Gewerbefreiheit eine gesetzliche Ermächtigungsgrundlage erfordern.[295]

5.10.2 Rechtliche Vorgaben für Anonymisierungsdienste

Rechtliche Vorgaben für Anonymisierungsdienste ergeben sich also je nach den Leistungsteilen sowohl aus dem Telemediengesetz als auch aus dem Telekommunikationsgesetz.

Der Diensteanbieter von Telemedien hat gemäß § 13 Abs. 6 Satz 1 TMG die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Hierin ist indirekt eine Ermunterung des Nutzers zum Selbstdatenschutz zu sehen. Diese Bestimmung ist gerade für Anonymisierungsdienste relevant. Als einfachgesetzliche Normierung des Rechts auf Anonymität bezweckt diese Norm die Umsetzung des Gebots der Vermeidung und Minimierung von personenbezogenen Daten gemäß § 3a BDSG. Zugleich dient sie dem Schutz der Meinungsfreiheit nach Art. 5 Abs. 1 Satz 1 GG.[296]

Als weiteren Beitrag zur Wahrung der Anonymität des Nutzers gegenüber dem Anbieter fordert § 13 Abs. 4 TMG diverse technische und organisatorische Vorgaben. Aus dem Umstand, dass die anonyme Nutzung technisch ermöglicht wird, resultiert nicht, dass nicht im Innenverhältnis der Diensteanbieter eine Abfrage der Nutzerdaten vor-

---

[295] *Brunst* 2009, 414; zur Beschlagnahmefähigkeit von Datenträgern s. auch *Ritzert*, in: BeckOK StPO 2015, § 94 StPO, Rn. 1.

[296] *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 120 ff.; *Müller-Broich* 2012, § 13 TMG, Rn. 10.

nehmen kann. Auch ist keine absolute Verpflichtung zur Eingehung eines anonymen Vertragsverhältnisses gegeben.

Im Einzelnen muss hinsichtlich der Erhebung und Speicherung von Daten unterschieden werden zwischen Bestandsdaten und Nutzungsdaten. Dabei sind für den Umgang mit Bestandsdaten § 14 TMG und für den Umgang mit Nutzungsdaten § 15 TMG als relevante Erlaubnisvorschriften maßgeblich. Nach § 14 Abs. 1 TMG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Auskunft über Bestandsdaten darf der Diensteanbieter gemäß § 14 Abs. 2 TMG auf Anordnung der zuständigen Stellen im Einzelfall nur erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr sowie zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden und Nachrichtendienste des Bundes und der Länder erforderlich ist. Diese Pflicht zur Offenbarung trifft auch Anonymisierungsdienstleister. Übermittelt werden können aber nur Daten, die auch vorliegen. Eine Pflicht zur vorsorglichen Erhebung durch den Dienstleister besteht nicht.

Soweit Leistungsanteile von Anonymisierungsdiensten dem Telekommunikationsrecht unterfallen ist ihr Umgang mit personenbezogenen Daten ähnlich umfangreich geregelt. Ansatzpunkte, um ohne Speicherung eine anonyme Nutzung zu ermöglichen, bieten §§ 96 Abs. 3 Satz 2, 98 Abs. 1 Satz 1 und 99 Abs. 2 Satz 1 TKG. Die §§ 91 ff. TKG vermitteln für Verkehrsdaten[297] und Bestandsdaten sektorspezifischen Datenschutz gemäß § 1 Abs. 3 BDSG, so dass die Vorschriften des allgemeinen Datenschutzes nach dem Bundesdatenschutzgesetz lediglich subsidiär anwendbar sind.

[297] S. Kapitel 5.1.1.

Bestandsdaten sind gemäß § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikation erhoben werden. Nach § 95 Abs. 1 Satz 1 TKG darf der Diensteanbieter diese Daten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 TKG genannten Zwecke erforderlich ist. Im Gegensatz zu den Verkehrsdaten beziehen sich die Bestandsdaten nicht auf einen konkreten Kommunikationsvorgang, sondern auf die vertraglichen Rahmenbedingungen im Hinblick auf die Nutzung des Dienstes.

Aus Sicht der Diensteanbieter, die die Kontaktdaten ihrer Nutzer wie etwa Name und Anschrift registrieren, ist die Zuordnungsinformation über verwendete IP-Adressen ein personenbezogenes Datum und auch ein Verkehrsdatum. Grundsätzlich ergibt sich aus § 97 Abs. 1 Satz 1 TKG für sie keine Ermächtigung zur Speicherung dieser Daten, weil die Anbieter kostenpflichtiger Anonymisierungsdienste jene lediglich gegen eine Pauschalleistung offerieren. Hierbei geht es ihnen um die Minimierung der Datenspeicherung und die Erhöhung der Anonymität. Bei Pauschaltarifen ist eine Verkehrsdatenspeicherung einzig dann gestattet, wenn innerhalb dieser Tarife auch Dienstleistungen erbracht werden, die nicht bereits mit der Pauschale abgegolten sind.

Nur gemäß § 100 Abs. 1 TKG darf der Diensteanbieter, soweit erforderlich, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. Gemäß § 100 Abs. 3 TKG ist ferner eine Verwendung zur internen Missbrauchskontrolle erlaubt. Nach der Rechtsprechung gilt die anlasslose, jedoch auf sieben Tage begrenzte Speicherung der jeweils genutzten IP-Adressen als noch verhältnismäßig, wenn sie technisch für die Zwecke des § 100 Abs. 1 TKG erforderlich sind.[298]

[298] S. z.B. BGH, NJW 2014, 2500; OLG Frankfurt am Main, BeckRS 2013, 16296.

Registrierungsfreie (durch Werbung finanzierte) Anonymisierungsdienste müssen die ihrem Nutzer von seinem Access-Provider zugeordnete IP-Adresse gleichfalls zwecks korrekter Zuordnung seines Datenverkehrs speichern, und zwar mindestens für die Verbindungsdauer. Da sie hieraus aber nicht auf den Inhaber der IP-Adresse rückschließen können und es sich demnach nicht um personenbezogene Daten handelt, gelten für solche Anonymisierungsdienste nicht die strengen Vorschriften für Verkehrsdaten. Denn diese finden nach § 91 Abs. 1 Satz 1 TKG nur Anwendung, wenn es um personenbezogene Daten geht. Diesen Anonymisierungsdiensten ist daher die Speicherung jeglicher Verbindungsinformationen, vor allem auch IP-Adressen der Nutzer und Informationen im Hinblick auf deren interne Zuordnung, gestattet.[299]

Für Anonymisierungsdienste besteht keine Pflicht, die Adressdaten ihrer Nutzer nach § 111 TKG zu erheben, da diese Norm nur statische IP-Adressen erfasst und „die an die Nutzer von ihrem jeweiligen Accessprovider dynamisch verteilten IP-Adressen keine von anderen vergebenen Rufnummern im Sinne von § 111 Abs. 1 Satz 1 Alt. 2 TKG“ darstellen.[300] Im Übrigen besteht auch aufgrund mangels Rechtsgrundlage keine Pflicht zur Speicherung von Verkehrsdaten auf Zuruf.[301] Es existiert daher kein Anspruch eines Auskunftsgläubigers aus § 101 Abs. 1 und Abs. 2 Nr. 3 UrhG auf eine die Auskunft erst ermöglichende Speicherung,[302] selbst nicht aufgrund analoger Anwendung.[303]

---

299 *Scheder-Bieschin* 2014, 327.

300 *Scheder-Bieschin* 2014, 334.

301 OLG Hamm, MMR 2011, 193; OLG Frankfurt am Main, MMR 2010, 62; LG Hamburg, MMR 2011,
475; OLG Düsseldorf, MMR 2011, 546.

302 OLG Düsseldorf, MMR 2011, 546 (547); OLG Hamm, MMR 2011, 193 (194); OLG Frankfurt am Main,
MMR 2010, 62 (63).

303 OLG Frankfurt am Main, MMR 2010, 62 (63).

Eine gesetzliche Befugnisnorm für die Verwendung von Verkehrsdaten bietet § 96 Abs. 1 Satz 2 TKG in Bezug auf die dort erwähnten Zwecke. Gemäß § 96 Abs. 2 TKG ist die Erhebung und Verwendung von Verkehrsdaten allein in diesen Fällen zulässig. Ansonsten hat der Diensteanbieter laut § 96 Abs. 1 Satz 3 TKG Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen. Als Zweck im Sinn des § 96 Abs. 1 Satz 2 TKG kann nicht nur einer der in Satz 1 genannten Zwecke, sondern auch ein durch andere gesetzliche Vorschriften begründeter Zweck in Betracht kommen. Ein Anspruch auf weitere Speicherung von Verkehrsdaten gemäß § 101 Abs. 2 in Verbindung mit Abs. 9 UrhG ist jedoch nur in den Fällen denkbar, denen das Nichtlöschen oder weitere Vorhalten von Daten hinsichtlich abgeschlossener und gerichtlich überprüfter Rechtsverletzungen zugrunde liegt, aber nicht zur Verfolgung künftiger Rechtsverletzungen.[304]

Anonymisierungsserver sind regelmäßig gemäß § 110 TKG in Verbindung mit den Vorschriften der Telekommunikations-Überwachungsverordnung zur Vorhaltung von Überwachungseinrichtungen verpflichtet.[305] Allerdings fallen solche Anonymisierungsdienste, die den Zugang zu Diensten bereitstellen, die nur öffentlich zugängliche Webseiten ausliefern, gemäß § 3 Abs. 2 Satz 1 Nr. 4 TKÜV prinzipiell aus dem Kreis der nach § 110 TKG Verpflichteten ausgenommen. Sie unterliegen daher keinen Verpflichtungen aus der Telekommunikations-Überwachungsverordnung, sofern gewährleistet ist, dass über den Anonymisierungsdienst einzig der Abruf von öffentlich zugänglichen Angeboten möglich ist. Unabhängig davon sind sie jedoch verpflichtet, auf Anordnungen nach §§ 100a und 100b StPO hin, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.[306]

304 LG Hamburg, MMR 2011, 475 (476).
305 *Brunst* 2009, 389.
306 *Brunst* 2009, 387 f.

5.10.3 Technische Einschränkungen der Anonymisierungsdienste

Um den Missbrauch bei der Nutzung von Anonymisierungsdiensten einzuschränken, könnten technische Beschränkungen in die Produkte selbst eingebaut werden, etwa Nichtauflösung von Domainnamen zu IP-Adressen (DNS-Sperren), IP-Adressbereich-Sperrungen, Portsperren, Drosselung bestimmter Protokolle und ähnliche Maßnahmen, die die Möglichkeiten eines Missbrauchs zu verhindern versuchen oder ihn anderweitig unattraktiv erscheinen lassen. Allerdings lassen sich nicht alle denkbaren technischen Einschränkungen praktisch sinnvoll umsetzen. Sie können von technisch versierten Nutzern zumindest zum Teil wieder wirkungslos gemacht werden.[186] Zudem würden diese Beschränkungen dem Nutzerinteresse entgegenstehen, anonym und unzensiert auf Informationen zugreifen zu können, sodass die Anwender einen solchen Dienst meiden würden, um sich anderer zu bedienen.

5.10.4 Anonymisierungsdienste und Auskunftspflichten

Soweit Anonymisierungsdienste Telemediendiensten sind, darf deren Anbieter auf Anordnung von Sicherheitsbehörden diesen nach §§ 14 Abs. 2 und 15 Abs. 5 Satz 4 TMG Auskunft über Bestandsdaten und Nutzungsdaten erteilen.[307] Soweit Nutzungsdaten vom Telekommunikationsgeheimnis des Art. 10 GG geschützt werden, dürfen sie nur übermittelt werden, wenn spezielle, das Telekommunikationsgeheimnis einschränkende Rechtsvorschriften dies erlauben. Solche bestehen für Diensteanbieter, die ausschließlich Telemedien anbieten, nicht.[308]

Soweit Anonymisierungsdienste als Telekommunikationsdienste anzusehen sind, darf deren Anbieter auf Anordnung von Sicherheitsbehörden dies nach §§ 112 und 113 TKG in automatisierten oder manuel-

---

307 *Dix*, in: Roßnagel 2013, § 14 TMG, Rn. 47 ff; *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 91 ff.

308 *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 92.

len Verfahren Auskunft über Bestandsdaten geben.[309] Strafverfolgungsbehörden können die Herausgabe bestimmter Bestandsdaten nach § 100j StPO verlangen. Bestimmte Verkehrsdaten, die aus geschäftlichen Gründen nach §§ 96 und 97 TKG noch gespeichert sind, können sie nach § 100g Abs. 1 StPO herausverlangen. Verzichtet der Anonymisierungsdienst auf die Erhebung von Daten, um Rechnungen zu erstellen oder um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, können mithin keine Maßnahmen zur Herausgabe von Verkehrsdaten nach § 100g Abs. 1 StPO ergriffen werden. Erfolgt die Erhebung von Verkehrsdaten allerdings nicht beim Telekommunikationsanbieter, sondern etwa beim Teilnehmer, ist diese gemäß § 100g Abs. 3 StPO nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften zulässig.

Die nach §§ 113b TKG auf Vorrat gespeicherte Verkehrsdaten können sie jedoch nur herausfordern, wenn die spezifischen Voraussetzungen des § 100g Abs. 2 StPO erfüllt sind.[310] Dazu müssen bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine besonders schwere Straftat begangen oder zu begehen versucht hat. Die besonders schweren Straftaten sind in § 100g Abs.2 Satz 2 StPO abschließend aufgelistet. Zweitens muss die Tat auch im Einzelfall besonders schwer wiegen. Drittens darf die Erhebung nur insoweit erfolgen, als die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Schließlich muss die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Nach § 101a StPO setzt eine Maßnahme nach § 100g StPO eine gerichtliche Entscheidung voraus.

Inhaltsdaten können vom Telekommunikationsdiensteanbieter für Zweck der Strafverfolgung nur aufgrund von Anordnungen nach §§

---

309 In Betracht kann auch eine Beschlagnahme von Datenträgern mit Bestandsdaten gemäß §§ 94 ff. StPO kommen.

310 S. näher *Roßnagel* NJW 2016, 533 (536).

100a und 100b StPO herausverlangt werden. Die Erhebung solcher Daten, die Inhalt der Kommunikation sind, findet mittels Ausleitung während des Übertragungsvorgangs statt. Nicht beim Diensteanbieter gespeicherte Daten können einzig auf diesem Weg erhoben werden. Aufgrund der Heimlichkeit dieser Maßnahmen ist hierin ein besonders schwerer Grundrechtseingriff zu sehen. Ihre Anordnung ist nur unter den Voraussetzungen des § 100a Abs. 1 und nur durch einen Richter möglich. Soweit tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Überwachungsmaßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, die Maßnahme gemäß § 100a Abs. 4 Satz 1 StPO unzulässig. Für die Überwachung der Inhalte der Telekommunikation für die präventive Arbeit des Bundeskriminalamts ist § 20l BKAG das Pendant zu § 100a StPO und §§ 1 und 3 G-10 bieten die entsprechende Ermächtigung für die Geheimdienste.

Die Grenze zwischen Verkehrs- und Inhaltsdaten kann fließend sein. Je nach Umstand können Inhalts- zu Verkehrsdaten werden und umgekehrt. In der Praxis werden Verkehrsdatenabfragen nach § 100g StPO zumeist innerhalb von zwei Wochen nach Ermittlungsbeginn erwirkt, und zwar als Vorstufe der Überwachung der Kommunikationsinhalte gemäß § 100a StPO. Hierdurch sollen erste Erkenntnisse über das Kommunikationsverhalten der Tatbeteiligten gewonnen werden. Die Anzahl der Verkehrsdatenabfragen übersteigt daher die der Inhaltsüberwachung deutlich.

5.10.5 Anonymisierungsdienste und Speicherpflichten

Für Telekommunikationsdiensteanbieter besteht seit dem 18. Dezember 2015 eine gesetzliche Pflicht zur Vorratsspeicherung von Verkehrsdaten. Mit ihr werden Daten auch erfasst, obwohl sie für die Erbringung eines Dienstes überhaupt nicht erforderlich sind. Der Europäische Gerichtshof hat am 8. April 2014 die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt, da durch sie ein Verstoß

gegen die Grundrechte auf Achtung des Privatlebens gemäß Art. 7 CrCh und auf Schutz personenbezogener Daten gemäß Art. 8 CrCh vorliegt. Außerdem steht durch diese Entscheidung fest, dass eine vorratsbedingte Datenspeicherung lediglich auf das absolut Notwendige begrenzt werden darf, folglich die Speicherung aller involvierten Verkehrsdaten, das heißt verdachtsunabhängig und anlasslos von allen Nutzern für einen längerfristigen Zeitraum, wie sie bisher geregelt war, auf europäischer Ebene nicht eingeführt werden darf.[311]

Trotz dieser Entscheidung verabschiedete der deutsche Gesetzgeber[312] das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ vom 10. Dezember 2015.[313] Das Artikelgesetz führt unter anderem im Telekommunikationsgesetz die Pflicht zur Speicherung von Verkehrsdaten auf Vorrat ein und ändert in der Strafprozessordnung die Regelungen zum Zugriff der Strafverfolgungsorgane auf die auf Vorrat gespeicherten Daten. Es stellt außerdem fest, dass diese Regelungen das Fernmeldegeheimnis in Art. 10 GG einschränken.

Die Pflichten zur Vorratsdatenspeicherung sind in den §§ 113a bis 113g TKG neu geregelt. Nach § 113a Abs. 1 TKG treffen die Pflichten zur Vorratsdatenspeicherung die Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer im Sinn von § 3 Nr. 6 lit. a TKG. „Erbringer“ überlassen den Kunden regelmäßig einen eigenen, in der Regel auf unbestimmte Dauer angelegten Telekommunikationsanschluss zur selbstständigen Verwendung. Anonymisierungsdienstleister können hierunter fallen, sofern sie auch Telekommunikationsanschlüsse zur selbstständigen Verwendung zur Verfügung stellen.[314]

Verpflichtet ist nur der Erbringer, der die zu speichernden Daten selbst erzeugt oder verarbeitet. Wer dies nicht tut, ist nach § 113a Abs.

311 S. hierzu näher *Roßnagel*, MMR 2014, 372 (375).
312 Zur Entstehung *Roßnagel* NJW 2016, 533 (534).
313 BGBl. I 2015, 2218.
314 S. Kapitel 5.10.1.

1 Satz 2 TKG verpflichtet, die Speicherung bei einem anderen sicherzustellen und der Bundesnetzagentur mitzuteilen, wer die Daten speichert.

Der Verpflichtete hat nach § 113b TKG alle in der Vorschrift präzise bestimmten Verkehrsdaten öffentlich zugänglicher Internetzugangsdienste[315] ohne Anlass für zehn Wochen zu speichern. § 113b Abs. 5 TKG verbietet ausdrücklich, den Inhalt der Kommunikation, Daten über aufgerufene Internetseiten (URL) und Daten aus E-Mail-Diensten zu speichern. Nach § 113b Abs. 8 TKG hat der Verpflichtete die Vorratsdaten „unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen … irreversibel zu löschen" und das Löschen gemäß § 113e Abs.1 TKG zu protokollieren.[316]

Die auf Vorrat gespeicherten Daten dürfen nach § 113c Abs. 1 TKG nur für drei Zwecke verwendet werden: Der Verpflichtete darf sie an eine Strafverfolgungsbehörde übermitteln, soweit diese sie unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine Erhebung der Vorratsdaten zur Verfolgung besonders schwerer Straftaten erlaubt.[317] Er darf sie auch an eine Gefahrenabwehrbehörde der Länder übermitteln, soweit diese sie unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine Erhebung der Vorratsdaten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt.[318] Drittens darf er selbst die Vorratsdaten für eine Bestandsdatenauskunft zu dynamischen IP-Adressen nach § 113 Abs. 1 Satz 3 TKG verwenden. Für andere Zwecke schließt § 113c Abs. 1 TKG eine Verwendung ausdrücklich aus.[319]

---

315 Gespeichert werden müssen Daten auch bei Telefon-, SMS-, MMS und ähnlichen Dienste.

316 Das Löschen hat nach dem Stand der Technik zu erfolgen.

317 Dies ist in § 100g Abs. 2 StPO geregelt.

318 *Roßnagel* NJW 2016, 533 (535).

319 *Roßnagel* NJW 2016, 533 (535).

5.11 Rechtsfortbildung

Anonymisierungsdienste verdienen angesichts der unbeschränkten Datenerfassung und Datenauswertung durch große Internetdiensteanbieter Unterstützung. Diese lassen die geltenden Rechtsregelungen jedoch vermissen. Daher wird ein deutlicher gesetzlicher Anpassungsbedarf bezügliches des Selbstdatenschutzes von Verbindungsdaten gesehen. Dieser besteht vor allem darin, die Vertrauenswürdigkeit von Anonymisierungsdiensten zu gewährleisten, ihre dafür erforderlichen Funktionen zu ermöglichen und für ihr Angebot ausreichende Rechtssicherheit zu gewährleisten.

5.11.1 Erleichterung der Diensterbringung

Die Erbringung von Anonymisierungsdiensten in Deutschland ist nach dem geltenden Rechtsrahmen dann äußerst eingeschränkt, wenn sie unter das Telekommunikationsgesetz fallen. Daher sollten sie weitgehend so organisiert werden, dass sie vom Telemediengesetz erfasst werden.

Für die Anwendung des Telekommunikationsgesetzes sollte unterschieden werden zwischen Anonymisierungsdiensten, die eine absolute Anonymität gewährleisten sollen, also Anonymität auch gegenüber dem Diensteanbieter bewirken, und Diensten, die die Identität des Nutzers gegenüber Dritten verbergen sollen. Beides wird durch die Verpflichtungen zur Identifizierung und Vorratsdatenspeicherung im Telekommunikationsrecht eingeschränkt. Identifizierungspflichten im Telekommunikationsgesetz sollten abgebaut werden, um die Erbringung von Anonymisierungsdiensten zu erleichtern. Nach geltendem Rechte ist eine anonyme Nutzung von Telekommunikationsdiensten eigentlich nicht möglich, da der Diensteanbieter stets die Identität des Kunden feststellen muss. Auch die Zielsetzung der wieder eingeführten Vorratsdatenspeicherung lässt sich nur dadurch erreichen, dass die Kommunikationsteilnehmer identifiziert sind. Hier ist zu untersuchen, ob das Angebot von Diensten, die die Verbindungsdaten der Nutzer

gegenüber Dritten verschleiern, aber bei berechtigten Interesse von Sicherheitsbehörden noch re-identifizieren können, gesetzlich klarer gefasst werden sollten.

Eine Ausweitung der Verbreitung von Techniken, bei denen eine sinnvolle Auswertung der Metadaten nicht mehr möglich ist, kann erreicht werden, indem die identifizierten Gründe für ihre mangelnde Nutzung behoben oder abgemildert werden. Durch die Einbindung großer Netzbetreiber oder Institutionen wie Universitäten und Forschungseinrichtungen könnte die Geschwindigkeit der Anonymisierungsnetzwerke deutlich erhöht werden.[320] Diese werden sich aber an dem Erbringen solcher Dienste nur beteiligen können, wenn der rechtliche Rahmen klar abgesteckt ist und Haftungsfragen geklärt sind.

5.11.2 Regulierung von Anonymisierungsdiensten

Damit Anonymisierungsdienste rechtsverträglich gestaltet und rechtmäßig erbracht werden, könnte eine Regulierung analog der Vertrauensdienste nach der eIDAS-Verordnung etabliert werden.[321] Die eIDAS-Verordnung erlaubt den Mitgliedstaaten Vertrauensdienste selbst zu regulieren und zu etablieren, die nicht in der Verordnung genannt sind. Ein Vertrauensdienst der die effektive Anonymisierung oder Pseudonymisierung gegenüber Dritten ermöglicht, aber im Falle des rechtswidrigen Missbrauchs die Strafverfolgung ermöglicht, könnte eine Vertrauenslücke schließen und zur Stärkung der Medienkompetenz von Bürgern beitragen.[322] Insbesondere hinsichtlich dieses Ausgleichs widerstreitender Interessen muss der gesetzliche Anpassungsbedarf in weiteren Forschungsprojekten noch detailliert werden.

320 S. *Hahn/Herfert/Lange* 2015, 60.
321 S. dazu Kapitel 4.4.3.
322 S. *Hahn/Herfert/Lange* 2015, 60f.

6 Positionsdaten

Bei der Positionsbestimmung wird der Aufenthaltsort des Nutzers festgestellt – meist, um an diesen Ort angepasste Dienstleistungen erbringen zu können. Die Genauigkeit hängt dabei von der verwendeten Technik ab, wobei die Bestimmung bis auf wenige Meter präzis möglich ist. Es hat sich allerdings gezeigt, dass die NSA weltweit massenhaft Positionsdaten von Smartphones sammelt und zu Bewegungsprofilen und Sozialprofilen auswertet.[323]

Die Positionsbestimmung kann über Navigationssatelliten erfolgen. Dabei werden global Satelliten in der Erdumlaufbahn verwendet, die kontinuierlich speziell codierte Signale aussenden. Aufgrund der unterschiedlichen Entfernung des Nutzers zu einzelnen Satelliten ergeben sich unterschiedliche Laufzeiten der Signale, die ausgewertet werden können, um die Position des Nutzers zu bestimmen.[324]

Die Positionsbestimmung kann auch über die Internetnutzung erfolgen. Dazu wird die vom Provider zugewiesene IP-Adresse ausgewertet. Ist die IP eines Nutzers bekannt, kann seine Position bestimmt werden. Die Genauigkeit der Positionsbestimmung beschränkt sich dabei meist auf die Stadt oder Region des Nutzers. Diese Information wird teilweise dazu verwendet, um dem Nutzer ortsbezogene Werbung anzuzeigen oder die auf einer Webseite verwendete Sprache automatisch umzuschalten.[325]

In der Gefahrenabwehr und der Strafverfolgung existieren zum Teil institutionalisierte Systeme zur Ortsbestimmung von Verdächtigen im Ermittlungsverfahren. So ist das Patras-System ein vom Deutschen Zoll betriebenes Ortungssystem, mit dem verdächtige Personen, Fahr-

---

323 Die dabei gesammelten Daten werden in einer speziellen Datenbank (FASCIA) gespeichert und umfassen unter anderem die eindeutige Kennung des Smartphones und die Kennung der Funkzelle.

324 S. *Hahn/Herfert/Lange* 2015, 63.

325 S. *Hahn/Herfert/Lange* 2015, 64.

zeuge und Waren verfolgt werden können. Zur Überwachung werden entweder Mobilfunkgeräte oder spezielle GPS-Tracker verwendet, die zum Beispiel an den zu überwachenden Fahrzeugen befestigt werden.[326] Diese Möglichkeiten der Standortüberwachungen wurden nicht betrachtet. Vielmehr erfolgte eine Konzentration auf die rechtlichen Rahmenbedingungen der Standortbestimmung mittels Mobilfunkgeräten.

6.1 Gefährdungslage

Werden die Positionsdaten über einen längeren Zeitraum gesammelt, lassen sich Bewegungsprofile und Sozialprofile der Nutzer erstellen.[327] Anhand dieser Profile lassen sich nicht nur die Wohn- und Arbeitsorte und die anderen Nutzer, die er dort trifft, bestimmen, sondern es können auch Vorhersagen über die Bewegungen und Kontakte des Nutzers getroffen werden.

Im Rahmen des CO-TRAVELER-Programms versucht die NSA, Beziehungen zwischen Benutzern anhand ihrer Bewegungsmuster zu erkennen. Hierzu werden über die zeitlich genau feststellbare Zugehörigkeit zu verschiedenen Funkzellen die Bewegungsmuster der zu analysierenden Nutzer erstellt. Diese Muster werden für alle Nutzer auf Überlappungen durchsucht.[328] Wenn sich Nutzer immer wieder zu gleichen Zeiten auf den gleichen Wegen befinden, kann davon ausgegangen werden, dass zwischen diesen Nutzer eine Verbindung besteht, zum Beispiel weil sie gemeinsam an Treffen teilnehmen. Anhand der Bewegungsprofile können Nutzer auch wiedererkannt und voneinander unterschieden werden.

Die Positionsbestimmung erfolgt häufig mit Zustimmung des Nutzers oder wird durch ihn initiiert. Neben klassischen Anwendungen wie Navigations-Systemen, gibt es Dienste wie Facebook Places, Foursqua-

---

326 S. *Hahn/Herfert/Lange* 2015, 64.
327 S. ausführlich *Hahn/Herfert/Lange* 2015, 65.
328 S. ausführlich *Hahn/Herfert/Lange* 2015, 48.

re und auch Dating-Apps wie Tinder. Dabei können die Nutzer selbst in bestimmten Geschäften oder Gaststätten „einchecken“, wobei ihre Position dann häufig auch ihren Kontakten mitgeteilt wird. Dienste dieser Art werden häufig genutzt, jeder dritte Smartphone-Nutzer teilt auf diese Weise seinen Standort mit.[329]

Neben der Positionsbestimmung über das Mobilfunknetz können bei Smartphones die Positionsbestimmung auch durch WLAN-Technik, mit Hilfe von Bluetooth Low Energy und durch die Analyse des Stromverbrauchs erfolgen. Die Genauigkeit der Positionsbestimmung kann verbessert werden, indem die verschiedenen Techniken miteinander kombiniert werden. Google Maps verwendet zum Beispiel GPS, WLAN und die Kennung des Mobilfunkmastes um die Position des Nutzers zu bestimmen. Unter iOS werden GPS, WLAN, Mobilfunk und Bluetooth zur Positionsbestimmung verwendet.[330]

Die Standortbestimmung von Mobilfunknutzern und die Speicherung dieser Standortdaten auf Vorrat zur Profilbildung durch die NSA verstoßen gegen geltendes deutsches Telekommunikationsrecht, soweit diese Daten in Deutschland erhoben werden. Dieser massive Datenumgang ist ein nicht zu rechtfertigender Eingriff in das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG aller Betroffenen weltweit. Deutschland treffen staatliche Schutzpflichten, sich schützend und fördernd vor dieses Grundrecht zu stellen.[331]

6.2 Positionsbestimmung im Mobilfunknetz

Der Umgang mit Daten zur Geolokalisation, die über das Mobilfunknetz gewonnen werden, ist im Telekommunikationsgesetz geregelt: Nach der Legaldefinition § 3 Nr. 19 TKG sind Standortdaten solche Daten, die in einem Telekommunikationsnetz oder von einem Tele-

329 S. ausführlich *Hahn/Herfert/Lange* 2015, 65.
330 S. *Hahn/Herfert/Lange* 2015, 66 ff.
331 S. Kapitel 2.2.

kommunikationsdienst erhoben oder verwendet werden und die den Standort des Mobilgeräts angeben. Dagegen umfasst der weitere, allerdings nicht legaldefinierte, Begriff „Positionsdaten“ alle Daten, die die Bestimmung des Ortes eines Mobilfunkgeräts ermöglichen, egal wie sie erhoben wurden.[332]

Die Begriffsbestimmung in § 3 Nr. 19 TKG entspricht Art. 2 Nr. 2 lit. c) Telekommunikations-Datenschutzrichtlinie.[333] Sie verweist auf die Definition des Telekommunikationsnetzes nach § 3 Nr. 27 TKG, des Endnutzers nach § 3 Nr. 8 TKG und des Telekommunikationsdienstes nach § 3 Nr. 24 TKG. Standortdaten sind exakte geografische Standortangaben, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben.[334] Die Legaldefinition ist insbesondere für die Reichweite des § 98 TKG von Bedeutung,[335] der spezielle Vorgaben für Standortdaten macht.

Die Regelungen in § 98 TKG sollen einen Missbrauch von Standortdaten verhindern. Geregelt wird in § 98 Abs. 1 Satz 1 TKG, dass diese für zusätzliche Dienste mit Zusatznutzen nur im erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, „wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat“. Diese Einwilligung ist jederzeit insgesamt oder auch nur zeitweise widerruflich ist. Umgekehrt sind nach § 98 Abs. 3 TKG bei Benutzung bestimmter Notrufnummern die Standortdaten immer zu übermitteln,

---

332 Alle Standortdaten im Sinne von § 3 Nr. 19 TKG sind Positionsdaten, aber nicht alle Positionsdaten sind Standortdaten.

333 Im Rahmen der TKG-Novelle 2012 wurde die Legaldefinition in § 3 Nr. 19 TKG um Daten ergänzt, die „von einem Telekommunikationsdienst“ erhoben werden; damit trägt der Gesetzgeber dem durch Art. 2 Nr. 2 lit. a) RL 2009/136/EG geänderten Wortlaut von Art. 2 lit. c) RL 2002/58/EG Rechnung.

334 S. *Holznagel/Ricke*, in: Spindler/Schuster 2015, § 3 TKG, Rn. 30.

335 *Braun*, in: Geppert/Schütz 2013, § 3 TKG, Rn. 68.

ohne dass dies vom Teilnehmer ausgeschlossen werden kann.[336] Es gibt Schnittmengen zwischen Standort- und Verkehrsdaten. Soweit Daten verwendet werden, die zum Aufbau und zur Aufrechterhaltung einer Verbindung erforderlich sind, dürfen diese als Verkehrsdaten nach § 96 TKG verarbeitet werden. Zu Standortdaten im Sinn von § 98 TKG werden sie, wenn sie darüber hinaus für Dienste mit Zusatznutzen verwendet werden sollen.[337]

Telekommunikationsdienstleister für Mobilfunk haben zusätzlich zu anderen Verkehrsdaten die Standortdaten für vier Wochen auf Vorrat zu speichern. Unter Standortdaten versteht § 113b Abs. 4 TKG die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt werden. Er darf also nicht alle Standortdaten, die im Home Location Register ständig erfasst werden, als Vorratsdaten speichern, sondern nur die Daten zum Standort zu Beginn einer Verbindung.[338] Auch darf er nicht die präziseren Standortdaten, die nach § 98 TKG etwa durch Triangulation zur Bereitstellung von Diensten mit Zusatznutzen erhoben werden, auf Vorrat speichern. Er hat lediglich die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben, damit Ermittler die Funkzelle einem bestimmten geografischen Bereich zuordnen können.[339]

6.3 Positionsbestimmung in anderen Netzen

Eine Ortung ohne Hilfe des Mobilfunknetzes oder des Internets als Telekommunikationsnetz unterliegt nicht den Regelungen des Telekommunikationsgesetzes. Soweit Daten aus GPS oder WLAN-Ortung für Telemedien verwendet werden, findet das Telekommunikations-

336 *Graf*, in: BeckOK StPO 2015, § 98 TKG, Rn. 3.
337 *Eckhardt*, in: Spindler/Schuster 2015, § 98 TKG, Rn. 9.
338 *Roßnagel* NJW 2016, 533 (535).
339 *Roßnagel* NJW 2016, 533 (535).

gesetz keine Anwendung.[340] Anders als das Telekommunikationsgesetz enthalten weder das Telemediengesetz noch das Bundesdatenschutzgesetz besondere Regelungen für die Nutzung von Standortdaten. Aus Sicht des verantwortlichen Dienstes richtet sich der Umgang mit Standortdaten des Nutzers nach den jeweils geltenden allgemeinen Bestimmungen.

So sind Positionsdaten für den Telemediendienstanbieter eines Locations Based Service in der Regel notwendig zu erhebende Nutzungsdaten im Sinn von § 15 Abs. 1 TMG, da sie die Inanspruchnahme des Dienstes erst ermöglichen.[341]

6.4 Befugnisse der Ermittlungsbehörden

Nach § 100g StPO dürfen Verkehrsdaten erhoben werden, wozu – unter Rückgriff auf § 96 Abs. 1 Nr. 1 TKG – auch gespeicherte Standortdaten zählen. Dazu bedarf es dafür keiner laufenden Kommunikation, das Mobilgerät muss also zum Zeitpunkt der Datenerhebung nicht genutzt werden, sondern lediglich angeschaltet sein. Beide Maßnahmen stehen unter Richtervorbehalt. § 100g Abs. 3 StPO enthält eine einschränkende Regelung der Funkzellenabfrage. Da durch sie alle in einer Funkzelle angefallenen Verkehrsdaten erhoben werden, werden unvermeidbar Verkehrsdaten aller Personen erfasst, die in der abgefragten Funkzelle mit ihrem Mobiltelefon kommuniziert haben.[342] Solche Abfragen sollen nur zulässig sein, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat, begangen oder zu begehen versucht hat oder eine entsprechende Straftat vorbereitet. Zudem muss die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Schließlich muss die Erforschung des

340 Ausführlich zur Einordung von Positionsdaten als Nutzungsdaten und zum Verhältnis von § 98 TKG zu § 15 TMG *Jandt* 2008, 135 ff.

341 S. *Schnabel* 2008, 206f. und 290 ff.

342 *Roßnagel* NJW 2016, 533 (536).

Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert sein. Auf die nach § 113b TKG auf Vorrat gespeicherten Daten darf die Funkzellenabfrage nur unter den Voraussetzungen des § 100g Abs. 2 StPO zurückgreifen.

6.5 Erlaubnis von Positionsverschleierung

Nach deutschem Recht ist die Nutzung von Techniken und Diensten zur Standortverschleierung für den Nutzer uneingeschränkt gestattet. Weder das Telekommunikationsgesetz noch das Telemediengesetz noch andere Vorschriften, auch nicht das Strafgesetzbuch, halten davon ab, den Standort eines Mobilgeräts gegenüber Dienstanbietern oder Dritten zu verschleiern.

Die tatsächlichen Möglichkeiten zur Standortverschleierung sind jedoch gering. Auf dem Endgerät lässt sich die Positionsbestimmung mit Hilfe des Mobilfunknetzes nicht verhindern. Es gibt lediglich die Möglichkeit, Angriffe mit Hilfe spezieller Apps zu erkennen. Auch kann der Nutzer sich gegen einige der vorgestellten Techniken zur Positionsbestimmung schützen, indem er die entsprechende Hardware in seinem Smartphone deaktiviert. Mit Hilfe von „Fake Location"-Apps können falsche GPS-Daten eingegeben werden, die echte Position des Nutzers kann dann durch andere Apps mittels GPS nicht mehr bestimmt werden.[343]

6.6 Rechtsfortbildung

Die Position des Nutzers wird ständig von unterschiedlichen Akteuren bestimmt. Dies erfolgt teilweise ohne Wissen und Einwilligung des Nutzers, wie im Fall der Positionsbestimmungen mittels Mobilfunk durch staatliche Behörden, und teilweise bewusst durch die aktive Nutzung von Diensten und Apps. Dabei steht die freigiebige Weitergabe der eigenen Position durch die Nutzer für unterschiedlichste

[343] S. *Hahn/Herfert/Lange* 2015, 68.

Apps im starken Kontrast zur Bedeutung der eigenen Position für die informationelle Selbstbestimmung.

Der Nutzer kann sich nur in sehr begrenztem Umfang vor den verschiedenen Möglichkeiten der Positionsbestimmung schützen. Es ist für ihn kaum möglich, sein Mobiltelefon aktiv zu nutzen und gleichzeitig die eigene Position zu verschleiern oder sogar ganz zu verbergen.[344]

In folgenden Bereichen wird gesetzlicher Anpassungsbedarf bezügliches des Selbstdatenschutzes von Positionsdaten gesehen:

6.6.1 Rechtsrahmen für Positionsdatenverschleierung

Es sollten Techniken zur Verschleierung von Positionsdaten gefördert werden, indem ein Rechtsrahmen gesetzt wird, der ihre Erforschung und ihren Einsatz begünstigt. Der Schutz von Standortdaten ist angesichts einer totalen Überwachung der Tele- und Internetkommunikation genauso wichtig, wie der Schutz von Verbindungs- und Kommunikationsinhaltsdaten. Diese heute zur Verschleierung von Standortdaten einsetzbaren technischen Lösungen sind rudimentär und zu wenig verbreitet. Zur Erfüllung grundrechtlicher Schutzpflichten sollte Deutschland diese Techniken fördern – wenigstens durch Forschungsförderung auf diesem Gebiet. Überdacht werden muss dabei der ordnungspolitische telekommunikationsrechtliche Rahmen. Privacy by Design könnte bereits bei der Netzwerkarchitektur ansetzen.[345]

Für den Schutz der Positionsdaten macht es einen großen Unterschied, wo diese erhoben und gespeichert werden. Erfolgt dies im Endgerät des Nutzers, kann er durch seine Einstellung, ob ein Programm Zugriff auf seine Positionsdaten hat, allgemein oder in Einzelfall bestimmen, wer seine Positionsdaten für welchen Zweck erhalten soll. Wer-

344 S. *Hahn/Herfert/Lange* 2015, 71.
345 S. *Hahn/Herfert/Lange* 2015, 70.

den die Positionsdaten vom Diensteanbieter erhoben, hat er keinen unmittelbaren Einfluss darauf, wer für welche Zwecke die Positionsdaten erhält und einsetzt. Rechtliche Anforderungen an ein Privacy by Design könnte vorgeben, dass – soweit dies möglich ist (z.B. bei der Positionsbestimmung über GPS) – die Positionsdaten im Endgerät des Nutzers gehalten werden müssen und nur nach eindeutiger technischer Freigabe von anderen Programmen und Diensteanbietern genutzt werden können. Für die zentrale Speicherung von Positionsdaten müssten rechtliche Vorgaben eine Unterrichtung des Nutzers fordern, wenn die Positionsdaten genutzt oder weitergegeben werden sollen. Der Nutzer muss dies technisch effektiv verhindern können.

6.6.2 Vertrauensdienst für Positionsdatenverschleierung

Damit Positionsdatenverschleierung (Anonymisierung oder Pseudonymisierung) rechtsverträglich gestaltet und rechtmäßig erbracht wird, könnte eine Regulierung analog der Vertrauensdienste nach der eIDAS-Verordnung etabliert werden.[346] Ein Vertrauensdienst der die effektive Positionsdatenverschleierung gegenüber Dritten ermöglicht, aber im Falle des rechtswidrigen Missbrauchs die rechtmäßige Überwachung durch Strafverfolgungsbehörden ermöglicht, könnte eine Vertrauenslücke schließen und zur Stärkung der Aufmerksamkeit und der Bewusstwerdung [347] von Bürgern beitragen.

[346] S. dazu Kapitel 5.11.2 und Kapitel 4.4.3.
[347] S. *Hahn/Herfert/Lange* 2015, 70.

7 Smart Home

Der Begriff „Smart Home“ bezeichnet eine Vielzahl von Geräten am und im Haus, die mit Sensoren und Netzwerkverbindungen ausgestattet sind und durch intelligente Funktionen die Wohnqualität erhöhen sollen. Es gibt keine einheitliche rechtliche Definition des Begriffs „Smart Home“.[348] In einem Smart Home ist einer oder zahlreichen Geräte der Hausautomation, Haushaltstechnik, Konsumelektronik und Kommunikationseinrichtungen intelligent in dem Sinne als das es oder sie sich an Bedürfnissen der Bewohner orientiert oder orientieren. Durch Vernetzung dieser Gegenstände untereinander können neue Assistenzfunktionen und Dienste zum Nutzen des Bewohners bereitgestellt werden und einen Mehrwert generieren, der über den einzelnen Nutzen der im Haus vorhandenen Anwendungen hinausgeht.[349]

Die Geräte lassen sich kategorisieren:[350] Durch den Begriff der *Haus- oder Gebäudeautomation* werden die fest am Haus installierten Einrichtungen wie Außen- und Innensensoren, Alarmanlagen, gesteuerte Rollläden, Einfahrt- und Garagentore, Außen- und Innenbeleuchtung und Heizung zusammengefasst.[351]

Smart Metering ist eine andere Komponente, intelligenten Strom-, Wasser- oder Gaszählern umfasst. Die Verwendung von Smart Metern für Strom, Erdgas, Fernheizung und Warmwasser ist seit 2006 durch eine EU-Richtlinie[352] geregelt und soll in Deutschland für Haushalte mit einem Verbrauch über 6.000 Kilowattstunden pro Jahr verpflichtend

348 *Raabe/Weis*, RDV 2014, 231.
349 S. z.B. *Skistims* 2016, 33 ff., 68 ff.; *Strese/SeideljKnape/Botthof* 2010, 8.
350 S. *Hahn/Herfert/Lange* 2015, 72f.
351 S. *Hahn/Herfert/Lange* 2015, 73.
352 Richtlinie 2006/32/EG des Europäischen Parlaments und des Rates vom 5. April 2006 über Endenergieeffizienz und Energiedienstleistungen und zur Aufhebung der Richtlinie 93/76/EWG.

sein.[353] Als Smart Meter werden Zähler bezeichnet, die einen Mikroprozessor enthalten. Der tatsächliche Verbrauch wie auch die tatsächliche Nutzungszeit von Energie kann zu jeder Zeit angezeigt und über ein Kommunikationsnetz an Dritte, wie etwa den Energieversorger oder einen Energiemanager, übermittelt werden.[354]

Schließlich bilden *netzwerkfähige elektronische Geräte* wie Kühlschränke, Spielekonsolen, vernetzte E-Book-Lesegeräte[355] oder Smart-TVs weitere Komponenten des Smart Home.[356] So bieten sich zum Beispiel Spielekonsolen zunehmend als Allround-Multimedia-Geräte an. Sie vereinen Fernseher, Blu-Ray-Player, Musikanlage, Internet und Spielmöglichkeiten. Der technische Funktionsumfang einer modernen Spielekonsole umfasst unter anderem die Erkennung des Nutzers durch HD-3D-Kamera mit Infrarot und Gesichtserkennung, die Analyse von Gesichtsausdrücken, die Zuordnung von Person und Stimme über Mikrofon und Kamera, die Analyse von Bewegungen des Nutzers durch Kameraauswertung, die Aufzeichnung aller Geräusche durch Mikrofon sowie die Übermittlung aller gespeicherten Daten und Informationen über das Internet.[357] Dadurch ergeben sich verschiedene Missbrauchsmöglichkeiten und Gefahrenpotenziale. So kann der Konsolenbetreiber große Datensammlungen über die Nutzer anlegen und Profile bilden. Dies ist bedenklich, da Möglichkeiten zum Abschalten der Funktionen der Datenaufzeichnung, -sammlung und -übermittlung in der Regel fehlen.[358] Schließlich ist auch denkbar dass der Zugriff durch Malware auch bei Spielekonsolen erfolgen kann und die –

---

353 Die Umsetzung erfolgte im Energiewirtschaftsgesetz (EnWG) – s. dazu *Jandt/Roßnagel/Volland*, ZD 2011, 99. Der rechtliche Rahmen soll künftig durch das Gesetz zur Digitalisierung der Energiewende, BR-Drs. 543/15 vom 18.12.2015, neu gefasst werden, das das als Energiewirtschaftsgesetz ändert und ein Messstellenbetriebsgesetz neu einführt.

354 S. *Hahn/Herfert/Lange* 2015, 74.

355 S. *Hahn/Herfert/Lange* 2015, 78.

356 S. zu weiteren Beispielen des Smart Home *Skistims* 2016, 37 ff.; *Hahn/Herfert/Lange* 2015, 75.

357 S. *Hahn/Herfert/Lange* 2015, 76.

358 S. zu den Risiken ausführlich *Skistims* 2016, 136 ff.

unautorisierte – Aktivierung von Sensoren die Aufzeichnung und Übermittlung von Daten an unbefugte Dritte zur Folge haben kann.[359]

Innerhalb der Smart Home-Anwendungen geben aber besonders Smart-TVs Anlass für eine Schwerpunktanalyse.[360] Die große Verbreitung und das hohe Risikopotenzial machen die Suche nach Technologien zum Selbstdatenschutz besonders notwendig.[361]

Als *Smart-TV* werden Fernsehgeräte bezeichnet, die über zusätzliche Funktionen und Schnittstellen wie Internetanschluss, USB, Speicherkarten und Netzwerkanschluss verfügen. Neben der einfachen Fernsehfunktion werden Medieninhalte zur laufenden Sendung oder damit verbundene Inhalte aus einer Mediathek zur Verfügung gestellt. Ein Smart-TV ist ein Multimedia-Center, das auch verwendet werden kann, um im Internet zu surfen, Bilder anzuschauen, Musik zu hören oder Video-Telefonie zu betreiben. Durch umfangreiche Sensoren können Daten der Nutzer erfasst werden. Die Integration von Web Technologien ermöglicht die Nutzung unterschiedlicher Kommunikationsdienste, wie zum Beispiel Musik-Player, E-Mail, Spiele, Social Media, VoIP und Bezahlungsdienste oder Online-Banking. Web-Browser und Kommunikationsdienste werden dem Nutzer in Form von Apps zur Verfügung gestellt. Durch den erweiterten Funktionsumfang von Smart-TVs können externe Kommunikations- und Fernsehdienste mit anderen Multimediaanwendungen verbunden werden.[362]

7.1 Personenbezug erfasster Daten

Abhängig von der Art der verwendeten Geräte in einem Smart Home, können personenbezogene Daten von Hausbewohnern, Gästen und sonstigen Nutzern erhoben werden. Je nach Ausgestaltung könnten

359 S. *Hahn/Herfert/Lange* 2015, 77.
360 S. ausführlich *Skistims* 2016, 62 f.; *Hahn/Herfert/Lange* 2015, 78 ff.
361 S. insb. *Ghiglieri/Hansen/Nebel/Pörschke/Simo* 2016; *Hahn/Herfert/Lange* 2015, 79.
362 S. *Hahn/Herfert/Lange* 2015, 78 ff.

die Sensoren und Applikationen schon relevanten Schlüsse auf persönlich sachliche Verhältnisse der Betroffenen ermöglichen. Zu erwarten ist aber auch, dass bei der Einbeziehung der Sensorik von Smartphones oder von Sensoren mit dediziertem Ortsbezug innerhäusliche Bewegungsprofile der Anwesenden erstellt werden. Dies ist sowohl in Echtzeit als auch historisch aufbereitet möglich. Ebenso können zum Beispiel Daten aus gesundheitsbezogenen Sensoren die Erstellung eines Gesundheitsprofils des Betroffenen erlauben. Durch freie Kombination der Datenquellen ist folglich die Erfassung relativ exakter Lebensquerschnitte der Betroffenen möglich. Im Fall der Verwendung von Smart Metern, wurde zum Beispiel schon nachgewiesen, dass sogar das zu einem gegebenen Zeitpunkt konsumierte Fernsehprogramm aus fein aufgelösten Strommessdaten extrahiert werden kann. Bei der Nutzung von Smart-TV entsteht eine Vielzahl von personenbezogenen Daten der Nutzer. Dies sind personenbezogene Daten, die durch die Anmeldung oder Registrierung zu Anwendungen erhoben und verarbeitet werden, sowie Daten über das Nutzungsverhalten. Diese Daten, zum Beispiel Lieblingsprogramme und –Internetdienste, Suchbegriffe oder die Nutzungsdauer hinsichtlich einzelner Sender oder Sendungen, knüpfen hinsichtlich der Identifizierung an die IP-Adresse des Nutzers oder (im Falle einer Anmeldung oder Registrierung) unmittelbar an das Smart-TV-Nutzerkonto an.

Von wem über wen dabei personenbezogene Daten erhoben und verarbeitet werden, ist im Geflecht der beteiligten Akteure nicht immer einfach zu bestimmen. Zum Beispiel lassen sich bei Smart-TV die Akteure Gerätehersteller und Servicetechniker, TV-Sender, Inhaltsanbieter,[363] Kommunikationsnetze und Infrastrukturbetreiber, Werbetreibende und Bezahldienste ausmachen, die mit Daten von Nutzern umgehen könnten. Weitere Akteure sind Nutzer, sowohl Zuschauer als auch weitere Privatpersonen, die ein Smart-TV nutzen oder in dessen

[363] Inhaltsanbieter stellen Apps mit moderierten und sonstigen Inhalten zur Verfügung, s. *Hahn/Herfert/Lange* 2015, 82.

Sensorik-Bereich gelangen, um neben traditionellen Rundfunkdiensten auch zusätzliche über das Internet erreichbare interaktive Medieninhalte zu konsumieren. Dieses Beziehungsgeflecht, in dem für den Nutzer nicht immer sofort eindeutig ist wer wann, welche Daten über ihn verarbeitet und übermittelt, spiegelt sich im Risikopotenzial von Smart-TV wieder.[364]

Möglich ist zum Beispiel, dass die TV-Sender selbst das Nutzerverhalten Einzelner verfolgen können und Benutzerprofile erstellen. Auch die Smart-TV-Geräte-Hersteller können das Nutzerverhalten vollständig protokollieren, inklusive des Fernsehverhaltens, des Surfverhaltens und der wiedergegebenen Multimediainhalte. Die Protokollierung des Nutzerverhaltens kann zur personalisierten Werbung verwendet werden. Dabei lässt sich die Datenübermittlung durch Nutzer kaum verhindern, ohne das Einschränkungen im Funktionsumfang in Kauf zu nehmen wären. Inhaltsanbieter, Werbetreibende und Bezahldienste bietet sich über Smart-TV die Möglichkeit, umfassende Nutzerprofile zu Seh- und Surfverhalten zu erstellen und dann selbst zu nutzen oder weiterzuvermitteln. Schließlich besteht auch eine Bedrohung durch Beobachter und Schad- und Spähsoftware. Denkbar ist, dass Dritte unautorisiert Zugriff auf Netzwerk und Sensorik des Smart-TV erhalten. Dadurch könnten diese zum Beispiel unbemerkt die Kontrolle über kritische Hardware-Module wie Kameras und Mikrofon zu erlangen, auf Daten wie Kontakte, Passwörter, Kreditkartenummern und Standort des Gerätes zugreifen oder sogar das Gerät zum Absturz zu bringen.[365]

7.2 Gefährdung von Grundrechten

Die mittels Smart Home-Anwendungen generierten Daten ermöglichen Überwachungsmaßnahmen. Smart-TV-Geräte verbinden sich zu den Servern der TV-Sender oder TV-Hersteller und informieren, zu

364 S. *Hahn/Herfert/Lange* 2015, 81-83.
365 S. *Ghiglieri/Hansen/Nebel/Pörschke/Simo* 2016; *Hahn/Herfert/Lange* 2015, 83 ff.

welcher Zeit der Nutzer einen Sender eingeschaltet hat. Auf diese Weise können detaillierte Nutzerprofile erstellt werden, aus denen sehr genau die Vorlieben und Abneigungen eines Nutzers herausgelesen werden können.[366] Aus Daten von kompromittierten Smart-TV-Sensoren lassen sich ohne Wissen und Einverständnis der Nutzer Informationen über Aktivitäten und Verhaltensweisen der Nutzer sowie über die Ausstattung in sensiblen Bereichen des Haushalts ableiten. Dadurch wird eine Massenüberwachung in der Wohnung aller Nutzer möglich.[367]

Die Wohnung ist aber der elementare Lebensraum und Mittelpunkt menschlicher Existenz.[368] Daher unterliegt sie dem besonderen verfassungsrechtlichen Schutz des Art. 13 GG, der ihre Unverletzlichkeit gewährleistet. Sie dient als absolut geschützter Eigenbereich der freien Entfaltung der Persönlichkeit.[369] Vom Schutzbereich umfasst ist die räumliche Sphäre der Wohnung, die der allgemeinen Zugänglichkeit durch eine räumliche Abschirmung entzogen und zur Stätte privaten Lebens und Wirkens gemacht wird.[370] Vernetzte Haustechnologie eröffnet die Möglichkeit, das in der Wohnung stattfindende Privatleben aufzuzeichnen und so in den geschützten Eigenbereich vorzudringen. Unabhängig von dem durch Art. 13 GG gewährten Schutz sieht das Grundgesetz in bestimmten Fällen eine weitere, speziellere grundrechtliche Garantie vor, die das Individuum vor Angriffen auf und durch Haustechnologien bewahrt: Smart Home-Technologien stellen sogenannte eigengenutzte, informationstechnische Systeme dar. Kernmerkmal jener informationstechnischen Systeme ist es, dass sie allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können,

366 S. *Hahn/Herfert/Lange* 2015, 88.
367 S. *Hahn/Herfert/Lange* 2015, 88; *Ghiglieri/Hansen/Nebel/Pörschke/Simo* 2016.
368 BVerfGE 18, 121 (131f.).
369 BVerfGE 42, 212 (219); 89, 1 (12); *Gornig*, in: v. Mangoldt/Klein/Starck 2011, Art. 13 GG, Rn. 1.
370 BGHSt 44, 138 (140).

dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erstellen.[371] Die Vertraulichkeit und Integrität derartiger Systeme wird durch das Computergrundrecht geschützt.[372] Kommuniziert das Haussystem mit Systemen außerhalb der Wohnung, wird die Vertraulichkeit dieser Kommunikation nach außen durch das Fernmeldegeheimnis aus Art. 10 GG geschützt. Im Herrschaftsbereich der Wohnung unterliegen personenbezogene Daten zudem der informationellen Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

7.3 Bewertung nach geltendem Datenschutzrecht

Smart Home-Anwendungen und Geräte werden zumeist im privaten Umfeld eingesetzt. Trotzdem unterfallen sie zumeist dem Regelungsbereich jeweils einschlägiger Datenschutzgesetzgebung. Von der konkreten Gestaltung des Systems ist es abhängig, ob das entsprechende System zum Beispiel als ein Telemediendienst einzustufen ist. Voraussetzung ist, dass es eigene Inhalte wie Informations- und Kommunikationsdienste generiert und diese sinnlich wahrnehmbar darstellt.

Besteht die Funktion nur in der Übertragung von Signalen über Telekommunikationsnetze, handelt es sich um einen Telekommunikationsdienst. Auch Mischsysteme sind denkbar, je nach Ausgestaltung kommt dann das Telemedien- oder Telekommunikationsgesetz zur Anwendung.[373]

Soweit weder das Telemediengesetz noch das Telekommunikationsgesetz Anwendung finden, wird die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach den Datenschutzgesetzen des Bundes oder der Länder beurteilt. Von einer Privilegierung der Datenverwendung im persönlichen oder familiären Bereich kann nur in den Fällen

371 *Lang*, in: BeckOK GG 2015, Art. 2 GG, Rn. 46.
372 BVerfGE 120, 274.
373 *Skistims* 2016, 366 ff.

ausgegangen werden, in denen keine Vernetzung nach außen stattfindet und kein dritter Diensteanbieter involviert ist.

Grundsätzlich besteht die Möglichkeit, dass der private Nutzer in seinen Rechten verletzt wird, indem zum Beispiel ohne sein Wissen durch den Diensteanbieter Daten über sein Nutzungsverhalten verarbeitet werden. Darüber hinaus ist es aber auch denkbar, dass private Nutzer haftbar sind für Verletzungen der Rechte Dritter, wie zum Beispiel von Gästen. Auf Privatpersonen sind in der Regel weder die Normen des Telemediengesetzes noch des Telekommunikationsgesetzes anwendbar. Beide Gesetze wenden sich ausschließlich an „Anbieter". Unter diesen Begriff fällt derjenige, der etwa einen Smart TV in seinem Wohnzimmer stehen hat und ihn bestimmungsgemäß nutzt, gerade nicht.[374]

Die Zulässigkeit der Daten, die bei der Nutzung des Systems anfallen, durch den Telemediendiensteanbieter oder den Telekommunikationsdiensteanbieter wird nach Telemediengesetz oder Telekommunikationsgesetz beurteilt. Bestandsdaten nach § 14 TMG und § 95 TKG sind solche Daten, die zur Begründung, Ausgestaltung und Änderung eines Vertragsverhältnisses erforderlich sind. Dazu gehören Name, Kontaktdaten und Zahlungsinformationen des Nutzers. Je nach spezifischem Dienst können aber auch weitere Daten zur Ausgestaltung des Dienstes unerlässlich sein. Nutzungs- und Verkehrsdaten nach § 15 TMG und § 96 TKG dürfen nur dazu verwendet werden, um die Inanspruchnahme des Dienstes zu ermöglichen und abzurechnen. Diese Daten sind auf die konkrete Nutzung oder Sitzung bezogen, etwa IP-Adressen, Cookies, Systeminformationen oder aber Daten über Beginn und Ende der jeweiligen Nutzung. Die Einordnung ist stark abhängig von der konkreten Funktion des Dienstes oder Systems. Je mehr ein System mit Nutzern interagiert oder auf ihre Bedürfnisse reagiert, desto mehr Daten sind erforderlich, um den Dienst zu erbringen, die da-

374 *Raabe/Weis*, RDV 2014, 231.

mit in die Kategorie der Nutzungs- oder Verkehrsdaten fallen. Alle übrigen anfallenden Daten sind sogenannte Inhaltsdaten. Wann die Verarbeitung dieser Daten zulässig ist, richtet sich bei der Verarbeitung für eigene Geschäftszwecke nach § 28 BDSG. Entscheidend ist dann vor allem, ob die Kenntnis der Daten erforderlich ist, um den bestellten Dienst zu erbringen. Ist dies nicht der Fall, dürfte die heimliche Erfassung von Inhaltsdaten in der Regel rechtswidrig sein, weil die schutzwürdigen Interessen des Betroffenen die – eventuell – berechtigten Interessen des Datenverarbeiters überwiegen.

Grundsätzlich ist der Umgang mit all diesen Daten durch die verantwortliche Stelle rechtmäßig, wenn eine Einwilligung der Betroffenen vorliegt. Die Einwilligungserklärung im Smart Home-Kontext transparent zu gestalten, bereitet genau solche Schwierigkeiten wie den Datenumgang transparent für den Nutzer selbst umzusetzen. Besonders bei Smart-TV ist dem Nutzer nicht immer bewusst, dass sein Fernsehgerät solche Daten häufig auch ohne konkreten Hinweis erfasst und weiterleitet.[375] Besonders problematisch dabei ist, dass Nutzer in den allermeisten Fällen auch keinen Anlass haben dagegen vorzugehen, weil eine Übermittlung von Daten oder eine Verbindung mit dem Internet gar nicht erwartet wird. Damit ermöglicht die Systemgestaltung heutiger Smart-TVs eine Erhebung und Verarbeitung dieser Daten ohne Mitwirkung der Betroffenen. Nicht nur verlieren Nutzer so die Gerätehoheit über ihr TV-Gerät, auch bewirkt die intransparente Datenübermittlung einen eklatanten Verstoß gegen ein Prinzip des Datenschutzes.

7.4 Rechtsfortbildung

Trotz der hohen Verbreitung von internetfähigen modernen Fernsehgeräten und anderen Smart Home-Anwendungen, existieren nur unzureichende Schutzmaßnahmen, um die informationelle Selbstbestimmung und die Integrität und Vertraulichkeit informationstechni-

375 S. *Hahn/Herfert/Lange* 2015, 88.

scher Systeme ausreichend zu schützen. Daher besteht ein hoher gesetzlicher Anpassungsbedarf bezüglich des Selbstdatenschutzes in Smart Home-Umgebungen. Aus der geschilderten Risikolage und dem geringen Angebot und der unzureichenden Verbreitung von Techniken zur Durchsetzung von Datensparsamkeit und Transparenz stellen sich spezifische Aufgaben für die Rechtsfortbildung.

7.4.1 Datenaggregation und Verschlüsselung

Durch Datenaggregation und Verschlüsselung können Nutzerdaten effektiv anonymisiert werden. Solche Maßnahmen zur Anonymisierung verhindern Personenbezug der entstehenden Daten. Dadurch werden Verletzungen der informationellen Selbstbestimmung vermieden und der Anwendungsbereich der datenschutzrechtliche Normen nicht tangiert. Hierfür ist der telemedienrechtliche Rahmen der Regulierung von Smart Home-Diensten dahingehend fortzuentwickeln, dass die Anonymisierung der Daten, die für die Erbringung der vom Nutzer bestellten Dienste nicht erforderlich sind, noch im Smart-TV verpflichtend ist. Dabei geht es auch um Anforderungen gegenüber den Herstellern zu einem Privacy by Design, ohne dass sie auf intransparente und Take-it-or-Leave-it-Einwilligungsmodelle ausweichen können.

7.4.2 Herstellung von Transparenz

Ein besonderes Problem bei Smart Home-Anwendungen ist die Herstellung von Transparenz.[376] Um ein gewisses Maß an Transparenz sicherzustellen, sollten die Anbieter von Smart Home-Anwendungen verpflichtet werden, Informationen über die Funktionalitäten und Risiken des Smart Home dauerhaft – etwa auf einer Web-Seite – bereitzustellen und zu aktualisieren. Inhalt der Information müssten vor allem die Logik der Datenverarbeitungsstruktur des Smart Home sein. Neben dieser zusammen- und umfassenden Informationen müssten

[376] S. hierzu auch *Skistims* 2016, 541f.

auch situationsgerecht Hinweise erfolgen, etwa wenn neue Personen mit den Systemen des Smart Home in Kontakt kommen, sich Änderungen in der Funktionalität ergeben oder erstmals Daten an einen Empfänger übertragen werden. Besonders relevante, weil besonders invasive Praktiken betreffende Informationen sind zu priorisieren. Dies könnte beispielsweise der prominent präsentierte Hinweis sein, dass Daten ins außereuropäische Ausland fließen.[377]

7.4.3 Anpassung des Urheberrechts und Wettbewerbsrechts

Auch das Urheberrecht und Wettbewerbsrecht sollten angepasst werden, um Änderungsrechte der Nutzer und Dritter an datenschutzunverträglichen Smart Home-Anwendungen zu ermöglichen.[378] Solche Änderungen sollten bereits nachgeltendem Recht als zulässig anerkannt werden, da sie nur eine „Notwehr" gegen Angriffe auf die Grundrechte der Nutzer darstellen. Da dies jedoch umstritten ist, sollte der Gesetzgeber Rechtssicherheit und Rechtsklarheit durch entsprechende Gesetzesänderungen gewährleisten. Der Vertrieb und Einsatz von datenschutzfreundlichen Steuerungsgeräten, wie dem Privacy Protector und Datenscannern, sollte dadurch rechtlich ermöglicht und abgesichert werden. Außerdem sollten Hersteller von Smart Home-Systemen verpflichtet werden, gängige oder einheitliche Schnittstellen und Funktionen ihrer Systeme anzubieten und offenzulegen, um die Entwicklung und Nutzung von Softwareagenten zur Ausübung von Betroffenenrechten zu ermöglichen. Die Konkretisierung dieser Verpflichtung sollte den Entwicklern, Herstellern und Anbietern im Wege der Selbstregulierung ermöglicht werden.[379]

---

377 S. z.B. *Roßnagel/Geminn/Jandt/Richter* 2016, Kapitel 4.2.2.

378 S. *Richter/Bodden/Rasthofe/Roßnagel*, DuD 2013, 720.

379 S. z.B. *Roßnagel/Richter/Nebel*, ZD 2013, 107; *Roßnagel/Geminn/Jandt/Richter* 2016, Kapitel 4.2.

7.4.4 Moderne Technikregulierung

Herausforderungen aus Smart Home-Anwendungen ergeben sich aus datenschutzrechtlicher Sicht insbesondere für das Transparenzprinzip und dem Verschwimmen der Grenzen der bekannten Datenkategorien. Dies führt dazu, dass zukünftig keine eindeutige Zuordnung der Datenkategorien und Verantwortlichkeiten im Smart Home nach der bestehenden Dreiteilung von anwendungsbezogenem Inhaltsdatenschutz, telemedienrechtlichen Obligationen und dem transportbezogenen Telekommunikationsrecht mehr vorgenommen werden kann. Dies lässt eine risikospezifische Regulierung von Smart Home-Anwendungen notwendig erscheinen, [380] wofür sich erste Ansätze einer regulatorischen Konzeption in der modernen Technikregulierung des Energiewirtschaftsgesetzes und künftig des Messstellenbetriebsgesetzes finden.

[380] S. hierzu auch *Skistims* 2016, 534 ff.; *Roßnagel/Geminn/Jandt/Richter* 2016, Kapitel 4.2.2.

8 Schlussbemerkung

Das Explorationsprojekt „Pro Privacy“ des Fraunhofer-Instituts „Sicherheit in der Informationstechnik“ in Darmstadt und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel hatte zum Ziel, die Frage zu explorieren, wie der Einzelne seine Grundrechte durch Selbstschutztechniken besser schützen kann. Dabei war nicht intendiert, diese Frage abschließend zu beantworten, sondern auszukundschaften, wo der Stand der Forschung ist, welche Unterfragen beantwortet sind, welcher Forschungsbedarf besteht und welche Wege sich für die weitere Verbesserung von Selbstdatenschutz eröffnen.

Diese Fragen können sinnvoll nur interdisziplinär von Informatikern und Juristen bearbeitet werden, weil die technischen Möglichkeiten in der Praxis vom geltenden Rechtsrahmen abhängen, dessen Verständnis und Fortentwicklung aber wiederum von den technischen Instrumenten und Potentialen abhängt. Daher erwies sich die Kooperation zwischen SIT und provet in der Durchführung des Projekts als äußerst fruchtbar.

Für die exemplarisch ausgewählten Anwendungsbereiche des Selbstschutzes von

- Kommunikationsinhalten,
- Verbindungsdaten,
- Positionsbestimmung und
- personenbezogenen Daten im Smart Home

konnten die konzeptionellen Mittel für die zukünftige Entwicklung neuer Techniken zum Selbstdatenschutz und ihre staatliche Förderung durch gesetzgeberische Maßnahmen untersucht werden. Dabei zeigt sich, dass nach dem geltenden Recht eine gewisse Freiheit besteht, die

technisch möglichen Selbstschutzmittel einzusetzen, dass das Recht aber keinen förderlichen Rahmen bietet, um diese Selbstschutzmittel zu verbreiten und breit zu nutzen. Dies liegt zum einen daran, dass das Verhältnis zwischen Selbstschutz der Grundrechte und anderen Rechtszielen nicht grundsätzlich gelöst ist und deswegen auch kein systematisches Konzept besteht, wie dieser Selbstschutz in die Rechtsordnung integriert werden soll. Zum anderen wirken sich Regelungen des Telekommunikations- und des Strafprozessrechts, die andere Ziele verfolgen, ungeplant als Beschränkungen oder Hemmnisse für den grundrechtlichen Selbstschutz aus. Deren Verhältnis zueinander ist bislang unzureichend bedacht und sollte auf der Grundlage eine systematischen Konzepts geklärt und besser abgestimmt werden.

Die vorgestellten Untersuchungen haben gezeigt, dass und wie Recht und Selbstschutz künftig besser aufeinander abgestimmt werden können. Die vorgestellten Gesetzgebungsvorschläge haben jedoch nur das Ziel aufzuzeigen, dass und wie Recht und Technik in dieser Frage harmonisiert werden können. Sie begründen jedoch noch vielfältigen Forschungsbedarf, wie diese Vorschläge zu einem systematisches Konzept zur Integration des Selbstschutzes von Grundrechten in der digitalen Welt in die Rechtsordnung fortentwickelt werden können und wie die verschiedenen Zielkonflikte in der detaillierten Umsetzung der Vorschläge gelöst werden können.

Literatur

Albers, M., Grundrechtsschutz der Privatheit, DVBl. 2010, 1061.

Bäumler, H. / Mutius A. (Hrsg.), Anonymität im Internet, Braunschweig 2003.

Borges, G., Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, 3334.

Borges, G., Rechtsfragen der Haftung im Zusammenhang mit dem elektronischem Identitätsnachweis, Baden-Baden 2011.

Brunst, P., Staatliche (Anti-)Krypto-Strategien, DuD 2012, 333.

Brunst, P. W., Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009.

Byszi, F. / Houdeau, D. / Meister, G. / Wolfenstetter, K.-D., Elektronische Identifikation in Europa: die neue EU-Verordnung, DuD 2013, 169.

Calliess, C., Sicherheit im freiheitlichen Rechtsstaat, ZRP 2002, 1.

Dreier, H. (Hrsg.), Grundgesetz-Kommentar, Band 1, 3. Aufl., Tübingen 2013 (zitiert als Bearbeiter, in: Dreier 2013).

Durner, W., Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet, ZUM 2010, 833.

Epping, V. / Hillgruber, C. (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, 27. Edition, München, Stand: 1. Dezember 2015 (zitiert als *Bearbeiter*, in: BeckOK GG 2015).

Ewer, W. / Thienel, T. , Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30.

Federrath, H. / Golembiewski, Speicherung von Nutzungsdaten durch Anonymisierungsdienste im Internet, DuD 2004, 486.

Fischer-Dieskau, S. / Roßnagel, A. / Steidle, R., Beweisführung am seidenen Bit-String? Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand, MMR 2004, 451.

Forum Privatheit, Whitepaper Selbstdatenschutz, 2014, http://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php.

Geminn, C. L.: Die Debatte um nationales Routing – eine Scheindebatte? Eine kritische Analyse der Argumentationslinien, MMR 2015, 98.

Geminn, C. L.: Crypto Wars Reloaded?, DuD 2015, 546.

Geminn, C. L. / Roßnagel, A., „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703.

Geppert, M. / Schütz, R. (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. München 2013 (zitiert als *Bearbeiter,* in: Geppert/Schütz 2013).

Gerhards, J., (Grund-)Recht auf Verschlüsselung, Baden-Baden 2010.

Ghiglieri, M. / Hansen, M. / Nebel, M. / Pörschke, J. V. / Simo Fhom, H., Smart-TV und Privacy: Bedrohungspotenziale und Handlungsmöglichkeiten, White Paper des Forums Privatheit – Selbstbestimmtes Leben in einer digitalisierten Welt, Karlsruhe 2016.

Gitter, R. / Schnabel, C., Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411.

Graf, J. P. (Hrsg.), Beck'scher Online-Kommentar Strafprozessordnung mit RiStBV und MiStra, Edition 21, München, Stand 15. Januar 2015 (zitiert als *Bearbeiter,* in: BeckOK StPO 2015).

Greenwald, G., Die globale Überwachung, München 2014.

Härting, N., Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065.

Hahn, T. / Johannes, P. C. / Lange, B., Schutzschilde gegen die NSA, DuD 2015, 71.

Hahn, T. / Herfert, M. / Lange, B., PRO PRIVACY – Abschlussbericht des Fraunhofer SIT, Darmstadt 2015, https://www.sit.fraunhofer.de/.

Hansen, M., Datenschutz nach dem Summer of Snowden, DuD 2014, 439.

Heckmann, D., Persönlichkeitsschutz im Internet, NJW 2012, 2631.

Heckmann, D. (Hrsg.), Internetrecht, Telemediengesetz, E-Commerce, EGovernment, Juris Praxiskommentar, 4. Aufl. Saarbrücken 2014 (zitiert als *Bearbeiter*, in: Heckmann 2014).

Herzog, R. / Scholz, R. / Herdegen, M. / Klein, H. H. (Hrsg.), Grundgesetz Kommentar, Band I, 72. Ergl. München 2014 (zitiert *Bearbeiter,* in: Maunz/Dürig 2014).

Hoffmann, C. / Schulz, S./ Borchers, K., Grundrechtliche Wirkungsdimensionen im digitalen Raum – Bedrohungslagen im Internet und staatliche Reaktionsmöglichkeiten, MMR 2014, 89.

Hoffman-Riem, W., Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 1998, 532 (534).

Hoffmann-Riem, W., Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2015, 53.

Hoffmann-Riem, W., Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014, MAT-A SV 2/1 zu Ausschuss-Drucksache 54.

Hoeren, T., Das Telemediengesetz, NJW 2007, 801.

Hoeren, T. / Sieber, U. / Holznagel, B. (Hrsg.), Multimedia-Recht, 42. Ergl. München 2015 (zitiert als Bearbeiter, in: *Hoeren/Sieber/Holznagel* 2015).

Hornung, G, / Möller, J., Passgesetz - Personalausweisgesetz: PassG/ PAuswG – Kommentar, München 2011.

Huber, P.M., Die Verantwortung für den Schutz vor terroristischen Angriffen, ZUR 2004, 1.

Jandt, S. / Roßnagel, A. / Volland, B., Datenschutz für Smart Meter – Spezifische Neuregelungen im EnWG, ZD 2011, 99.

Jarras, H. D. / Pieroth, B., Grundgesetz für die Bundesrepublik Deutschland, 11. Aufl. München 2013.

Jandt, S., Vertrauen im Mobile Commerce – Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services, Baden-Baden 2008.

Kilian, W. / Heussen, B.(Hrsg.), Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. Ergl. München 2008.

Kipker, D.-K. / Voskamp, F., PRISM und staatliche Schutzpflichten – ein politisches Märchen?, RDV 2014, 84.

Klink, J. / Straub, T., Anonymisierungsdienste nach der Vorratsdatenspeicherung, DuD 2008, 123.

Kloepfer, M., Verfassungsrecht Band II – Grundrechte, München 2010.

Leupold, A., Geschäftsgeheimnisse gehören in die (Private) Cloud, MMR 2014, 145.

Marauhn, T., Sicherheit in der Kommunikationstechnik durch legislatives Risikomanagement, KritV 1999, 57.

Maurer, O., Staatsrecht I, 6. Aufl. München 2010.

Meyer-Goßner, L. / Schmitt, B., Strafprozessordnung: StPO Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 58. Aufl. München 2015.

Müller-Broich, J. D., Telemediengesetz, Baden-Baden 2012.

Nebel, M., Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, 517.

Nedden, B., Datenschutz und „Privacy Enhancing Technologies", Risiken und Chancen für das Datenschutzrecht, in: Roßnagel, A.

(Hrsg.), Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001, 67.

Papier, H.-J. , Gutachterliche Stellungnahme Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des deutschen Bundestags 18. Wahlperiode, MAT-A SV 2/2 zu Ausschuss-Drucksache 54.

Pohlmann, N., Lehren aus der IT-Sicherheitskrise ziehen!, DuD 2014, 47.

Polenz, S., Der neue elektronische Personalausweis – E-Government im Scheckkartenformat, MMR 2010, 671.

Raabe, O., Wie können die Regelungsbereiche des Teledienstерechts zum Telekommunikationsrecht horizontal voneinander abgegrenzt werden?, CR 2003, 268.

Raabe, O. / Weis, E., Datenschutz im „SmartHome", RDV 2014, 177.

Rau, M. / Behrens, C., Catch me if cou can … : Anonymisierungsdienste und die Haftung für mittelbare Rechtsverletzungen, K&R 2009, 766.

Richter, P. / Bodden, E. / Rasthofer, S. / Roßnagel, A., Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps - Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps, DuD 2013, 720.

Roos, P., Der Entwurf eines IT-Sicherheitsgesetzes: Regelungsinhalte und ihre Übereinstimmung mit dem Richtlinienvorschlag der EU-Kommission, K&R 2013, 769.

Rosenbach, M. / Stark, H., Der NSA-Komplex, München 2014.

Roßnagel, A., Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, ZRP 1997, 27.

Roßnagel, A., Die elektronische Signatur im Verwaltungsrecht – Modernisierung des VwVfG und des VwZG, DÖV 2001, 221.

Roßnagel, A., Die elektronische Verwaltung, NJW 2003, 469.

Roßnagel, A. (Hrsg.), Handbuch des Datenschutzrechts, München 2003 (zitiert als *Bearbeiter*, in: Roßnagel 2003).

Roßnagel, A., Sicherheit für Freiheit? Grundlagen und Fragen, in: ders. (Hrsg.), Sicherheit für Freiheit? Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft. Baden-Baden 2003(a), 17.

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

Roßnagel, A., Beck'scher Kommentar zum Recht der Telemediendienste, München 2013, (zitiert als *Bearbeiter*, in: Roßnagel 2013).

Roßnagel, A., Neue Regeln für sichere elektronische Transaktionen - Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686.

Roßnagel, A., Neue Maßstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung MMR 2014, 372.

Roßnagel, A., Das IT-Sicherheitsgesetz, DVBl. 2015, 1206.

Roßnagel, A., Die neue Vorratsdatenspeicherung, NJW 2016, 533.

Roßnagel, A. / Geminn, C. L. / Jandt, S. / Richter, P., Datenschutzrecht 2016 – „Smart" genug für die Zukunft?, Kassel 2016.

Roßnagel, A. / Johannes, P. C., Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste Neue Regeln für elektronische Sicherheitsdienste, ZD 2013, 65.

Roßnagel, A. / Jandt, S. / Richter, P., Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-Überwachung, DuD 2014, 545.

Roßnagel, A. / Moser-Knierim, A. / Schweda, S., Interessenausgleich im Rahmen der Vorratsdatenspeicherung – Analysen und Empfehlungen, Baden-Baden 2013.

Roßnagel, A. / Richter, P. / Nebel, M., Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der Datenschutz-Grundverordnung, ZD 2013, 103.

Roßnagel, A. / Scholz, P., Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Ruhmann, I., NSA, IT-Sicherheit und die Folgen, DuD 2014, 40.

Säcker, F. J. (Hrsg.), Telekommunikationsgesetz Kommentar, 3. Aufl. Frankfurt am Main 2013 (zitiert als *Bearbeiter*, in: Säcker 2013).

Saeltzer, G., Vorsicht! krimineller „Datenschutz" und gefährliche „Datensicherheit", DuD 2014, 333.

Schaar, P., Lässt sich die globale Internetüberwachung noch bändigen, ZRP 2013, 214.

Scheder-Bieschin, F., Modernes Filesharing, Oldenburg 2014.

Schellenberg, U., Verschläft die Rechtspolitik den NSA-Skandal?, AnwBl. 2013, 631.

Schmahl, S., Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?, JZ 2014, 220.

Schnabel, C., Datenschutz bei profilbasierten Location Based Services – Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation, Kassel 2009.

Sieber, U., Verantwortlichkeit im Internet. Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen. Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, München 1999.

Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014 (zitiert als *Bearbeiter*, in: Simitis 2014).

Skistim, H., Smart Homes – Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung

der Vertraulichkeit und Integrität informationstechnischer System, Baden-Baden 2015.

Spindler, G. / Schuster, F. (Hrsg.), Recht der elektronischen Medien, 3. Aufl. München 2015 (zitiert als *Bearbeiter*, in: Spindler / Schuster 2015).

Starck, C. (Hrsg.), Kommentar zum Grundgesetz, 6. Aufl. München 2011 (zitiert als Bearbeiter, in: v. Mangoldt/Klein/Starck 2011).

Strese, H. / Seidel, U. / Knape, T. / Botthof, A., Smart Home in Deutschland - Untersuchung im Rahmen der wissenschaftlichen Begleitung zum Programm Next Generation Media (NGM) des Bundesministeriums für Wirtschaft und Technologie, Berlin 2010.

Taeger, J. /Gabel, D., BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. Frankfurt am Main 2013.

Voss, A., NSA-Untersuchungsbericht: Schutz der Privatsphäre ist ein Grundrecht und muss gelebte Realität bleiben, ZD 2014, 218.

Wagner, E., Der Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission, DuD 2012, 676.

Wagner, E., PRISM, TEMPORA und die Folgen. Selbstdatenschutz tut Not!, DuD 2013, 676.

Waidner, M, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014, MAT-A SV 1/2 zu Ausschuss-Drucksache 53.

Weidner-Braun, R., Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung. Am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichem Recht, Berlin 2012.

Wicker, M., Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, 765.

Wolf, J., Der rechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre“, JZ 2013, 1039.

Wolff, H. A. / Brink, S. (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 15. Edition, München, Stand: 1. Februar 2016 (zitiert als *Bearbeiter*, in: BeckOK Datenschutzrecht 2016).

Wüllrich, P., Das Persönlichkeitsrecht des Einzelnen im Internet, Jena 2006.

Abkürzungen

a. A.	anderer Ansicht
AEUV	Vertrag über die Arbeitsweise der europäischen Union
AnwBl.	Anwaltsblatt
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
Bd.	Band
BeckRS	Beck-Rechtsprechung
BeckOK	Beck‘scher Online-Kommentar
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des BGH in Zivilsachen
BMI	Bundesministerium des Innern
BMWi	Bundesministerium der Wirtschaft
BNetzA	Bundesnetzagentur
BND	Bundesnachrichtendienst
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Dr.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CR	Computer und Recht (Zeitschrift)
d. h.	das heißt
dies.	dieselbe
ders.	derselbe
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
DSGVO	Datenschutzgrundverordnung
EG	Europäische Gemeinschaft
eGovG	E-Government-Gesetz
eID	elektronische Identifizierung
Einl.	Einleitung

eIDAS-VO	Verordnung für elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EMRK	Europäische Menschenrechtskonvention
ENISA	Europäische Agentur für Netz- und Informationssicherheit
Ergl.	Ergänzungslieferung
et al.	et alteri (und andere)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
f. / ff.	folgende / fortfolgende
F.A.Z.	Frankfurter Allgemeine Zeitung
GG	Grundgesetz
ggf.	gegebenenfalls
GHCQ	Government Communications Headquarters
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union
Fn.	Fußnote
h. M.	herrschende Meinung
Hrsg.	Herausgeber
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
i. d. F.	in der Fassung
IM	Information Management (Zeitschrift)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
iOS	Iphone Operating System
IP	Internetprotokoll
ISO	International Standards Organisation
IT	Informationstechnologie
ITRB	IT-Rechtsberater
ITeG	Wissenschaftliches Zentrum für Informationstechnik-Gestaltung
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation und Recht
KK-StPO	Karlsruher Kommentar zur StPO

KOM	Dokumente der Kommission der EG
KritV	Die Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LG	Landgericht
m. w. N.	mit weiteren Nennungen
MMR	Multimedia und Recht
NJW	Neue Juristische Wochenzeitschrift
Nr.	Nummer
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OLG	Oberlandesgericht
PGP	Pretty Good Privacy
PKI	Public-Key-Infrastruktur
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer
S. / s.	Siehe
S/MIME	Secure / Multipurpose Internet Mail Extensions
SigG	Signaturgesetz
SigV	Signaturverordnung
SPON	Spiegel Online Nachrichten
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWD	Arbeitsunterlagen der Kommissionsdienststellen
SZ	Süddeutsche Zeitung
TDSV	Telekommunikations-Datenschutzverordnung
TMG	Telemediengesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TR	Technische Richtlinie
u. a.	unter anderem
Urt.	Urteil
USA	United States of America
VO	Verordnung
Vol.	Volume (Band)
Vorb.	Vorbemerkung

VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
WLAN	Wireless Local Area Network
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht

Angesichts der Bedrohungen der Grundrechte durch Ausspähaktivitäten von Geheimdiensten und anderen Angreifern ist es notwendig zu wissen, wie der Einzelne auch selbst seine Grundrechte durch Selbstschutztechniken besser schützen kann. Welche technischen Möglichkeiten eingesetzt werden können, ist in der Praxis auch vom geltenden Rechtsrahmen abhängig. Für die exemplarisch ausgewählten Anwendungsbereiche des Selbstschutzes von

- Kommunikationsinhalten,
- Verbindungsdaten,
- Positionsbestimmungen und
- personenbezogenen Daten im Smart Home

untersucht die Studie die konzeptionellen Mittel für die zukünftige Entwicklung neuer Techniken und ihre staatliche Förderung durch gesetzgeberische Maßnahmen. Dabei zeigt sich, dass nach dem geltenden Recht eine gewisse Freiheit besteht, die technisch möglichen Selbstschutzmittel einzusetzen, dass das Recht aber keinen förderlichen Rahmen bietet, um sie zu verbreiten und breit zu nutzen. Daher wird auch geprüft, wie Recht und Selbstschutz künftig besser aufeinander abgestimmt werden können.

ISBN 978-3-7376-0126-9