Konstantin Salz

Der elektronische Rechtsverkehr am Beispiel des elektronischen Gerichts- und Verwaltungspostfachs

kassel university press

Konstantin Salz

Der elektronische Rechtsverkehr am Beispiel des elektronischen Gerichts- und Verwaltungspostfachs

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Rechtswissenschaften (Dr. jur.) angenommen.

Gutachter: Prof. Dr. Alexander Roßnagel
Prof. Dr. Dr. Walter Blocher

Tag der mündlichen Prüfung: 22. Januar 2019

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.

Zugl.: Kassel, Univ., Diss. 2019
ISBN 978-3-7376-0712-4 (print)
ISBN 978-3-7376-0713-1 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737607131
URN: https://nbn-resolving.org/urn:nbn:de:0002-407135

www.upress.uni-kassel.de

Printed in Germany

Vorwort und Danksagung

Die folgende Arbeit entstand im Zeitraum zwischen Herbst 2013 und Dezember 2017, erfuhr aber zahlreiche Aktualisierungen bis Anfang 2019. In dieser Zeit hat der elektronische Rechtsverkehr in Deutschland einen Sprung von einem kaum bekannten Phänomen zu einem zumindest in der Anwaltschaft allgegenwärtigen Thema gemacht. Der Dreh- und Angelpunkt der Diskussion waren zu Beginn des Gesetzgebungsverfahrens für ein Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten zunächst Themen wie der Anschluss- und Benutzungszwang oder das elektronische Empfangsbekenntnis. Heute dreht sich die Diskussion vor allem um das besondere elektronische Anwaltspostfach (beA) mit seinen Vor- und Nachteilen.
Durch die Begleitung des Gesetzgebungsprozesses und die Beschäftigung mit dem elektronischen Gerichts- und Verwaltungspostfach (EGVP), das als Grundlage für das beA dient, will ich mit dieser Arbeit einen Beitrag nicht nur zur wissenschaftlichen Durchdringung des elektronischen Rechtsverkehrs, sondern auch zur Versachlichung der Diskussion um eben diesen leisten.
Die Arbeit berücksichtigt den Entwicklungsstand von Anfang April 2019, die Quellen wurden (soweit möglich) auf den entsprechenden Stand aktualisiert.

Mein besonderer Dank gilt all jenen, die diese Arbeit möglich gemacht haben: Meinem Doktorvater Prof. Dr. Alexander Roßnagel, der die Arbeit mit großer Gewissenhaftigkeit und noch größerer Geduld betreut hat; Prof. Dr. Dr. Walter Blocher für das Zweitgutachten; meiner Frau Corinna für Ihr Verständnis und ihre Geduld während dieses langen Unterfangens sowie meinen Eltern und meiner Familie für ihre moralische Unterstützung. Dank gilt außerdem all jenen, die auf andere Weise ihren Beitrag zum Gelingen der Arbeit geleistet haben: Meinem guten Freund Johannes Faust für sein wertvolles Feedback, dem Team von CMS Hasche Sigle und insbesondere dem Legal-Tech-Team; Dr. Frederik Leenen und Dr. Stefanie Klein-Jahns für die Schaffung eines wunderbaren Arbeitsumfelds; meinen ehemaligen Kollegen Dr. David Kruchen und Dr. Pierre Zickert.
Wie alle Auflistungen dieser Art muss auch diese notwendigerweise unvollständig bleiben, daher danke ich auch all jenen, die aus dem ein oder anderen Grund nicht in dieser Auflistung genannt wurden.

Hohen Neuendorf, Juni 2019
Konstantin Salz

Inhaltsverzeichnis

Literaturverzeichnis

1&1 Mail & Media GmbH, GMX: De-Mail-Preisliste, 2.11.2015. Abrufbar unter [https://ident.gmx.net/document/price-list/109223] (Stand vom 7.4.2019). (Zit: GMX-Preisliste)

Abel, Ralf Bernd (Hrsg.), Datenschutz in Anwaltschaft, Notariat und Justiz, 2. Aufl., München 2003 (Zit: *Bearbeiter* in *Abel*).

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht - von der Richtlinie zur Verordnung; Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, Computer und Recht 2016, 88.

Apitzsch, Jörg/Hartnick, Werner/Krause, Harald/Lüttich, Klaus u. a., S.A.F.E.-Feinkonzept - Dokument 1: System- und Schnittstellenspezifikation Föderiertes Identity Management, Abrufbar unter [https://web.archive.org/web/20171215111516/http://www.justiz.de/elektronischer_rechtsverkehr/grob-und-feinkonzept/20080331_safe_dokument1_fim-schnittstellenspec_v1-4_a__signed.pdf] (Stand vom 7.4.2019). (Zit: SAFE-Schnittstellenspezifikation)

Arbeitsgruppe „IT-Standards in der Justiz" der Bund-Länder-Kommission, SAFE - Die Übersicht, Abrufbar unter [https://web.archive.org/web/20150323134725/http://www.justiz.de/elektronischer_rechtsverkehr/grob-und-feinkonzept/Anlage_safe_die_uebersicht_stand_2017_07_15.pdf] (Stand vom 7.4.2019). (Zit: SAFE-Übersicht)

Arbeitsgruppe „IT-Standards in der Justiz" der Bund-Länder-Kommission, SAFE-Rollenmodell, Abrufbar unter [https://web.archive.org/web/20150323022756/http://www.justiz.de/elektronischer_rechtsverkehr/grob-und-feinkonzept/20131029_Anlage_SAFE_Rollen_2013_10_13.pdf] (Stand vom 7.4.2019). (Zit: SAFE-Rollenmodell)

Arndt, Hans-Wolfgang/Fetzer, Thomas/Scherer, Joachim/Graulich, Kurt (Hrsg.), TKG: Telekommunikationsgesetz ; Kommentar, 2., völlig neu bearb. und wesentlich erw. Aufl., Berlin 2015 (Zit: *Bearbeiter* in *Arndt*/*Fetzer*/*Scherer*/*Graulich*).

Auernhammer, Herbert (Hrsg.), BDSG: Kommentar zum Bundesdatenschutzgesetz - Nebengesetze, 4. Aufl., Köln 2014 (Zit: *Bearbeiter* in *Auernhammer*).

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016 (Zit: *Bearbeiter* in *Auer-Reinsdorff*/*Conrad*).

Bäcker, Matthias/Hornung, Gerrit, EU-Richtline für die Datenverarbeitung bei Polizei und Justiz in Europa - Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeireicht, Zeitschrift für Datenschutz 2012, 147.

Backs, Volker/Kühnelt, Andreas/Sandkühler, Christoph/Schmid, Irene u. a., Stellungnahme Nr. 6/2012 - Diskussionsentwurf einer Bundesratsinitiative für ein Gesetz zur Förderung des elektronischen Rechtsverkehrs mit der Justiz, Abrufbar unter [http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2012/februar/stellungnahme-der-brak-2012-06.pdf] (Stand vom 7.4.2019). (Zit: BRAK-Stellungnahme Nr. 6/2012)

Barthel, Torsten Frank, Praxis der Kommunalverwaltung - Niedersächsisches Justizgesetz (NJG),

Berlin 2016.

Bauer, Craig P., Secret History: The Story of Cryptology, Boca Raton/London/New York 2013.

Baumbach, Adolf/Lauterbach, Wolfgang/Albers, Jan/Hartmann, Peter (Hrsg.), Beck'sche Kurzkommentare Band 1: Zivilprozessordnung mit FamFG, GVG und anderen Nebengesetzen, 76. Aufl., München 2018 (Zit: *Bearbeiter* in *Baumbach*/*Lauterbach*/*Albers*/*Hartmann*).

Baumgartner, Tobias, Privatvervielfältigung im digitalen Umfeld, Dissertation, Zürich [u.a.] 2006.

Bergfelder, Martin, Der Beweis im elektronischen Rechtsverkehr, Dissertation, Hamburg 2006.

Berlit, Uwe, Das Elektronische Gerichts- und Verwaltungspostfach bei Bundesfinanzhof und Bundesverwaltungsgericht, JurPC Web-Dok. 13/2006 Abrufbar unter [http://www.jurpc.de/jurpc/show?id=20060013] (Stand vom 7.4.2019).

Beuth, Patrick, Alles Wichtige zum NSA-Skandal, ZEIT ONLINE 28.10.2013, Abrufbar unter [http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal] (Stand vom 7.4.2019).

Biermann, Kai, Datenschutz: Was Vorratsdaten über uns verraten, Zeit Online 3.9.2015, Abrufbar unter [http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz] (Stand vom 7.4.2019).

Böck, Hanno, BeA: Bundesrechtsanwaltskammer verteilt HTTPS-Hintertüre - Golem.de, 23.12.2018. Abrufbar unter [https://www.golem.de/news/bea-bundesrechtsanwaltskammer-verteilt-https-hintertuere-1712-131845.html] (Stand vom 7.4.2019). (Zit: BRAK verteilt HTTPS-Hintertüre)

Bodenschatz, Nadine, Der europäische Datenschutzstandard, Dissertation, Frankfurt a. M. [u.a.] 2010.

Borchers, Detlef, beA: Schwere Panne beim „besonderen elektronischen Anwaltspostfach" | heise online, 22.12.2017. Abrufbar unter [https://www.heise.de/newsticker/meldung/beA-Schwere-Panne-beim-besonderen-elektronischen-Anwaltspostfach-3927314.html] (Stand vom 7.4.2019). (Zit: Heise-Newsticker 22.12.2017)

Borchers, Detlef/Wilkens, Andreas, De-Mail integriert Ende-zu-Ende-Verschlüsselung mit PGP | heise online, 9.3.2015. Abrufbar unter [http://www.heise.de/newsticker/meldung/De-Mail-integriert-Ende-zu-Ende-Verschluesselung-mit-PGP-2570632.html] (Stand vom 7.4.2019). (Zit: Heise-Newsticker 9.3.2015)

Borges, Georg, Verträge im elektronischen Geschäftsverkehr: Vertragsabschluß, Beweis, Form, Lokalisierung, anwendbares Recht, 2. unveränderte Aufl., Habilitation, Baden-Baden 2007.

Bösing, Sebastian, Authentifizierung und Autorisierung im elektronischen Rechtsverkehr, Dissertation, Baden-Baden 2005.

Boysen, Uwe, E-Justice: Sachverständigenstellungnahme des DVBS zur öffentlichen Anhörung des Rechtsausschuss des Deutschen Bundestages, 12.4.2013. Abrufbar unter [http://www.dvbs-online.de/news515.htm] (Stand vom 18.12.2017). (Zit: DVBS-Sachverständigenstellungnahme vom 12. April 2013)

Braum, Stefan, „Parallelwertungen in der Laiensphäre": Der EuGH und die Vorratsdatenspeicherung, Zeitschrift für Rechtspolitik 2009, 174.

Briegleb, Volker, Smartphones: Android und iOS hängen alle ab, 19.8.2016. Abrufbar unter [http://www.heise.de/newsticker/meldung/Smartphones-Android-und-iOS-haengen-alle-ab-3300959.html] (Stand vom 7.4.2019).

Briegleb, Volker, VDSL-Turbo: Bundesnetzagentur gibt grünes Licht für Vectoring, Abrufbar unter [http://www.heise.de/newsticker/meldung/VDSL-Turbo-Bundesnetzagentur-gibt-gruenes-Licht-fuer-Vectoring-3311840.html] (Stand vom 7.4.2019).

Brosch, Christopher/Fiebig, Peggy, beA - sicher. Die Sicherheitsarchitektur des beA, BRAK-Magazin 4/2015 10.

Buchner, Benedikt, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, Datenschutz und Datensicherheit 2016, 155.

Bull, Hans Peter, Netzpolitik: Freiheit und Rechtsschutz im Internet, 1. Aufl., Baden-Baden 2013.

Bünder, Helmut, De-Mail - Die Elektropost wird zum Milliardenmarkt, FAZ.NET 11.12.2013, Abrufbar unter [http://www.faz.net/aktuell/wirtschaft/unternehmen/de-mail-die-elektropost-wird-zum-milliardenmarkt-12706575.html] (Stand vom 7.4.2019).

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge 14. Ergänzungslieferung - IT-Grundschutz-Kataloge_2014_EL14_DE.pdf, Abrufbar unter [https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2014_EL14_DE.pdf] (Stand vom 7.4.2019). (Zit: IT-Grundschutzkataloge)

Bundesamt für Sicherheit in der Informationstechnik, BSI: Akkreditierte De-Mail Diensteanbieter, Abrufbar unter [https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA_node.html] (Stand vom 7.4.2019). (Zit: Akkreditierte De-Mail Diensteanbieter)

Bundesamt für Sicherheit in der Informationstechnik, De-Mail - Sicherer elektronischer Nachrichtenverkehr - einfach und nachweisbar, Abrufbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/De-Mail-Broschuere.pdf?__blob=publicationFile&v=6] (Stand vom 7.4.2019). (Zit: De-Mail-Broschüre)

Bundesamt für Sicherheit in der Informationstechnik, BSI Technische Richtlinie 03138 Ersetzendes Scannen - TR RESISCAN Version 1.1, 2.3.2017. Abrufbar unter [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf?__blob=publicationFile&v=4] (Stand vom 7.4.2019). (Zit: TR RESISCAN)

Bundesamt für Sicherheit in der Informationstechnik, BSI: BSI stuft „Heartbleed Bug“ als kritisch ein, 11.4.2014. Abrufbar unter [https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Heartbleed_11042014.html;jsessionid=60BC8C9D98C56259B0670E6E7F368C60.2_cid368] (Stand vom 7.4.2019). (Zit: Pressemitteilung vom 11.4.2014)

Bundesamt für Sicherheit in der Informationstechnik, BSI: BKA und BSI warnen vor einer aktuellen digitalen Erpressungswelle bei der Internetnutzung, Abrufbar unter [https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Neue_Erpressungswelle_Ransomware_29012013.html] (Stand vom 7.4.2019). (Zit: digitale Erpressungswelle)

Bundesamt für Sicherheit in der Informationstechnik, BSI TR-02102-1 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2016-01, 15.2.2016. Abrufbar unter

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile] (Stand vom 7.4.2019). (Zit: BSI-TR-02102-1)

Bundesministerium für Verkehr und digitale Infrastruktur, Aktuelle Breitbandverfügbarkeit in Deutschland (Stand Mitte 2016). Erhebung des TÜV Rheinland im Auftrag des BMVI, 29.8.2016. Abrufbar unter [http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/breitbandverfuegbarkeit-ende-2016.pdf?__blob=publicationFile] (Stand vom 7.4.2019). (Zit: Breitbandverfügbarkeit)

Bundesministerium für Wirtschaft und Energie, Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, 18.10.2016. Abrufbar unter [https://www.bmwi.de/Redaktion/DE/Downloads/E/eldas-vo-entwurf.pdf?__blob=publicationFile&v=4] (Stand vom 7.4.2019). (Zit: Referentenentwurf VDG)

Bundesnetzagentur, Jahresbericht 2012, 6.3.2013. Abrufbar unter [http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2013/130506_Jahresbericht2012.pdf?__blob=publicationFile&v=4] (Stand vom 7.4.2019).

Bundesrechtsanwaltskammer, Presseerklärung 12/2016, 29.9.2016. Abrufbar unter [https://www.brak.de/fuer-journalisten/pressemitteilungen-archiv/2016/presseerklaerung-12-2016/] (Stand vom 7.4.2019). (Zit: Presseerklärung 12/2016)

Bundesrechtsanwaltskammer, Der Newsletter zum besonderen elektronischen Anwaltspostfach, Ausgabe 14/2017, 6.4.2017. Abrufbar unter [https://www.brak.de/zur-rechtspolitik/newsletter/bea-newsletter/2017/ausgabe-14-2017-v-06042017.news.html] (Stand vom 7.4.2019). (Zit: beA-Newsletter)

Bundesrechtsanwaltskammer, Acht Schriftsätze pro Sekunde, BRAK-Magazin 2/2014 6.

Bundesrechtsanwaltskammer, Technische Informationen zum Verschlüsselungsverfahren beim beA, Abrufbar unter [http://bea.brak.de/technische-informationen-zum-verschluesselungsverfahren-beim-bea/] (Stand vom 7.4.2019). (Zit: beA-Verschlüsselungsverfahren)

Bundesrechtsanwaltskammer, Das beA und die BRAK, Abrufbar unter [https://web.archive.org/web/20180501232227/http://bea.brak.de:80/was-ist-das-bea/bea-und-die-brak/] (Stand vom 7.4.2019). (Zit: das beA und die BRAK)

Bundesrechtsanwaltskammer, Teilnehmer am elektronischen Rechtsverkehr ERV, Abrufbar unter [https://web.archive.org/web/20180526043312/http://bea.brak.de/was-ist-das-bea/teilnehmer/] (Stand vom 7.4.2019). (Zit: Teilnehmer am ERV)

Bundesrechtsanwaltskammer, Zugang zum beA, Abrufbar unter [http://bea.brak.de/wie-funktioniert-bea/zugang/] (Stand vom 7.4.2019). (Zit: Zugang zum beA)

Bundesrechtsanwaltskammer, Zugriffsrechte, Abrufbar unter [https://web.archive.org/web/20180526043319/http://bea.brak.de:80/wie-funktioniert-bea/zugriffsrechte/] (Stand vom 7.4.2019). (Zit: Zugriffsrechte)

Bundesrechtsanwaltskammer, Sichere Anmeldung, Abrufbar unter [https://web.archive.org/web/20180619014803/http://bea.brak.de:80/wie-sicher-ist-das-bea/sichere-anmeldung/] (Stand vom 7.4.2019). (Zit: Sichere Anmeldung)

Bundesrechtsanwaltskammer, Nachrichtenerstellung und -versand, Abrufbar unter [https://web.archive.org/web/20180616091957/http://bea.brak.de:80/wie-funktioniert-bea/nachrichtenerstellung/] (Stand vom 7.4.2019). (Zit: Nachrichtenerstellung und Versand)

Bundesrechtsanwaltskammer, beA - Grundlegende Fragen, Abrufbar unter [https://web.archive.org/web/20180619014735/http://bea.brak.de:80/fragen-und-antworten/a-grundlegende-fragen/] (Stand vom 7.4.2019). (Zit: Grundlegende Fragen)

Bundesrechtsanwaltskammer, Vorschläge zur Verbesserung der Akzeptanz des elektronischen Rechtsverkehrs, 6.8.2008. Abrufbar unter [http://www.brak.de/w/files/stellungnahmen/Vorschlaege_Akzeptanz_ERV.pdf] (Stand vom 7.4.2019). (Zit: Vorschläge ERV)

Bundesrechtsanwaltskammer, Was kostet das beA?, Abrufbar unter [https://web.archive.org/web/20180618064355/http://bea.brak.de:80/was-ist-das-bea/was-kostet-das-bea/] (Stand vom 7.4.2019). (Zit: Was kostet das beA?)

Bundesrechtsanwaltskammer, Browser oder Kanzleisoftware, Abrufbar unter [http://bea.brak.de/was-braucht-man-fur-bea/browser-oder-kanzleisoftware/] (Stand vom 7.4.2019). (Zit: Browser oder Kanzleisoftware)

Bundesrechtsanwaltskammer, Unterstützte Browser und Betriebssysteme, Abrufbar unter [https://web.archive.org/web/20180617183919/http://bea.brak.de:80/was-braucht-man-fur-bea/browser-und-betriebssysteme/] (Stand vom 7.4.2019). (Zit: Unterstützte Browser und Betriebssysteme)

Bundesrechtsanwaltskammer, Technische Fragen, Abrufbar unter [http://bea.brak.de/fragen-und-antworten/c-technische-fragen/] (Stand vom 7.4.2019). (Zit: Technische Fragen)

Bundesrechtsanwaltskammer, Alles zur Erstregistrierung, Abrufbar unter [https://web.archive.org/web/20180422120934/http://bea.brak.de:80/wie-funktioniert-bea/zugang/alles-zur-erstregistrierung/] (Stand vom 7.4.2019). (Zit: Erstregistrierung)

Bundesrechtsanwaltskammer, Das Postfach, Abrufbar unter [https://web.archive.org/web/20180618064406/http://bea.brak.de:80/wie-funktioniert-bea/das-postfach/] (Stand vom 7.4.2019). (Zit: Das Postfach)

Bundesrechtsanwaltskammer, Wartungsarbeiten am beA, 22.12.2017. Abrufbar unter [https://bea.brak.de/2017/12/22/wartungsarbeiten-am-bea/] (Stand vom 7.4.2019). (Zit: Wartungsarbeiten am beA)

Bundesrechtsanwaltskammer, beA muss vorerst offline bleiben – Sicherheit und Datenschutz haben Priorität, 27.12.2017. Abrufbar unter [https://bea.brak.de/2017/12/27/bea-muss-vorerst-offline-bleiben-sicherheit-und-datenschutz-haben-prioritaet/] (Stand vom 7.4.2019). (Zit: bea vorerst offline)

Bundesrechtsanwaltskammer, Presseerklärung 19/2018, 27.6.2018. Abrufbar unter [https://www.brak.de/fuer-journalisten/pressemitteilungen-archiv/2018/presseerklaerung-19-2018/] (Stand vom 7.4.2019). (Zit: Presseerklärung 19/2018)

Bundesrechtsanwaltskammer, Der Newsletter zum besonderen elektronischen Anwaltspostfach, 20.8.2018. Abrufbar unter [https://www.brak.de/zur-rechtspolitik/newsletter/bea-newsletter/2018/sondernewsletter-v-20082018.news.html] (Stand vom 7.4.2019). (Zit: beA-Sondernewsletter)

Bundesrechtsanwaltskammer, Sichere Nachrichtenübermittlung, Abrufbar unter [https://web.archive.org/web/20180428180302/http://bea.brak.de:80/wie-sicher-ist-das-bea/sichere-nachrichtenuebermittlung/] (Stand vom 7.4.2019). (Zit: Sichere Nachrichtenübermittlung)

Bundesrechtsanwaltskammer, Zuverlässigkeit, Abrufbar unter [https://web.archive.org/web/20180422120322/http://bea.brak.de:80/wie-sicher-ist-das-bea/zuverlassigkeit/] (Stand vom 7.4.2019). (Zit: Zuverlässigkeit)

Bundesrechtsanwaltskammer, Screenshots, Abrufbar unter [https://web.archive.org/web/20180526041828/http://bea.brak.de:80/wie-funktioniert-bea/screenshots/] (Stand vom 7.4.2019). (Zit: Screenshots)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Stellungnahme zur Bundesratsinitiative E-Justice, zum Diskussionsentwurf Elektronischer Rechtsverkehr und zum Diskussionsentwurf eines Gesetzes zur Einführung einer Akte in Strafsachen, 21.11.2012. Abrufbar unter [http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/17_wp/E-Rechtsverkehr_Gerichten_reg/stellung_bitkom_diske.pdf?__blob=publicationFile] (Stand vom 7.4.2019). (Zit: Stellungnahme Diskussionsentwurf ERVG)

Bund-Länder-Kommission für Informationstechnik in der Justiz, Barrierefreiheit in der Informationstechnik der Justiz - Themenpapier der AG Zukunft der Bund-Länder-Kommission für Informationstechnik in der Justiz, 29.1.2015. Abrufbar unter [http://www.justiz.de/BLK/berichte/barrierefreiheit.pdf;jsessionid=DE40576B9C406E34788971B6CDE9F739] (Stand vom 7.4.2019). (Zit: Barrierefreiheit)

Calliess, Christian/Ruffert, Matthias (Hrsg.), EUV/AEUV - Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Aufl., München 2016 (Zit: *Bearbeiter* in *Calliess*/*Ruffert*).

Comans, Clemens David, Ein „modernes" europäisches Datenschutzrecht: Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, Dissertation, Frankfurt am Main [u.a.] 2012.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.), , Bundesdatenschutzgesetz - Kompaktkommentar zum BDSG, 5., vollständig neu bearbeitete Aufl., Frankfurt am Main 2016 (Zit: *Bearbeiter* in *Däubler*/*Klebe*/*Wedde*/*Weichert*).

Deutscher Anwaltverein, Justiz stellt EGVP-Client bis Ende 2017 bereit, 1.6.2016. Abrufbar unter [https://digital.anwaltverein.de/de/news/details/egvp-client-steht-bis-ende-2017-zur-verfuegung] (Stand vom 18.12.2017). (Zit: längere EGVP-Verfügbarkeit)

Deutscher Anwaltverein, Bundesgerichtshof zum beA: Umlage der Kosten ist rechtmäßig, 17.2.2016. Abrufbar unter [https://web.archive.org/web/20160324220253/http://digital.anwaltverein.de/de/news/details/bundesgerichtshof-zum-bea-umlage-der-kosten-ist-rechtmaessig] (Stand vom 7.4.2019). (Zit: Digitale Anwaltschaft News vom 17.2.2016)

Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), Handbuch zur Entwicklung XÖV-konformer IT-Standards, Version 1.0, 2.3.2010. Abrufbar unter [http://www.xoev.de/sixcms/media.php/13/2010-03-02-Handbuch-final.pdf] (Stand vom 7.4.2019). (Zit: XÖV-Handbuch 1.0)

Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), SAGA-Modul Technische

Spezifikationen Version de.bund 5.0.0, 3.11.2011. Abrufbar unter [http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/SAGA/saga_modul_tech_spez_de_bund_5_0_download.pdf?__blob=publicationFile] (Stand vom 7.4.2019). (Zit: SAGA-Modul Technische Spezifikationen Version de.bund 5.0.0)

Diffie, Whitfield/Hellman, Martin Edward, New Directions in Cryptography, IEEE Transactions on Information Theory, IT-22 6 1976, 644.

Diller, Martin/Klein, Anke, Die fünf häufigsten Anwaltshaftungsfälle - und wie man sie vermeiden kann!, BRAK-Mitteilungen 2013, 65.

Dobmeier, Gerhard, Datenschutz in der Anwaltskanzlei, Dissertation, Regensburg 2004.

Dörr, Oliver/Grote, Rainer/Marauhn, Thilo (Hrsg.), EMRK/GG: Konkordanzkommentar zum europäischen und deutschen Grundechtsschutz, Bd. 2: Kapitel 20 - 33, Register, 2. Auflage, Tübingen 2013 (Zit: *Bearbeiter* in *Dörr*/*Grote*/*Marauhn*).

egvp.de, Weiterentwicklung EGVP - Informationen zur Entwicklung der EGVP-Anwendungen Classic und Enterprise, 4.2011. Abrufbar unter [http://web.archive.org/web/20140801203555/http://www.egvp.de/beh_allgemeine_info/Info_EGVP_Classic_Enterprise.pdf] (Stand vom 7.4.2019). (Zit: Weiterentwicklung EGVP)

egvp.de, Änderungen beim Zugang zum elektronischen Rechtsverkehr ab 01.01.2016, Abrufbar unter [https://web.archive.org/web/20151226220711/http://www.egvp.de/] (Stand vom 7.4.2019). (Zit: Änderungen zum 1.1.2016)

egvp.de, Wichtige Hinweise zur Nutzung von Signaturkarten (Hardwarezertifikaten) für das Öffen von Postfächern und das Versenden von Nachrichten, Abrufbar unter [https://web.archive.org/web/20170209010254/http://www.egvp.de/pdf/technik/EGVP_Hinweise_Einsatz_Hardwarezertifikate_fuer_Ver_und_Entschluesselung_von_Postfaechern_und_Nachrichten.pdf] (Stand vom 7.4.2019). (Zit: Hinweise Hardwarezertifikate)

egvp.de, EGVP-Version 2.9 (Classic) ab 16.06.2014 - Was ist neu?, Abrufbar unter [https://web.archive.org/web/20170209071220/http://www.egvp.de/beh_allgemeine_info/Informationen_EGVP_Classic_2_9.pdf] (Stand vom 7.4.2019). (Zit: Neuerungen EGVP 2.9)

egvp.de, Teilnahme von Produkten am OSCI-gestützten Rechtsverkehr - Testkonzept, Abrufbar unter [http://www.egvp.de/Drittprodukte/EGVP_Testkonzept_Antragsverfahren_Teilnahme_von_Drittprodukten_V1_0.pdf] (Stand vom 7.4.2019). (Zit: Testkonzept)

Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Auflage, Berlin [u.a.] 2014 (Zit: *Bearbeiter* in *Ehlers*).

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO : Datenschutz-Grundverordnung : Kommentar, 2. Aufl., München 2018 (Zit: *Bearbeiter* in *Ehmann*/*Selmayr*).

Ehrmann, Jürgen/Wöhrmann, Meinhard/Streckel, Birger/Krause, Harald, SAFE Grobkonzept, 31.12.2007. Abrufbar unter [https://web.archive.org/web/20141024073712/http://www.justiz.de/elektronischer_rechtsverkehr/grob-und-feinkonzept/20070731_safe_grobkonzept-v1_1_signed.pdf] (Stand vom 7.4.2019).

Electronic Frontier Foundation, Investigating Machine Identification Code Technology in Color Laser Printers, 22.7.2005. Abrufbar unter [https://www.eff.org/wp/investigating-machine-

identification-code-technology-color-laser-printers] (Stand vom 7.4.2019). (Zit: Machine Identification Code in Printers)

Electronic Frontier Foundation, List of Printers Which Do or Do Not Display Tracking Dots | Electronic Frontier Foundation, Abrufbar unter [https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots] (Stand vom 7.4.2019). (Zit: Druckerliste)

Engel-Flechsig, Stefan/Maennel, Frithjof A./Tettenborn, Alexander (Hrsg.), Beck'scher IuKDG Kommentar, München 2001 (Zit: *Bearbeiter* in IuKDG-Komm).

Engels, Thomas, Pflicht zur Überprüfung der Telefaxnummer, Der IT-Rechts-Berater 2013, 28.

Epping, Volker/Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, 39. Ed, München 2018 (Zit: *Bearbeiter* in *Epping/Hillgruber*).

Erbs, Georg/Kohlhaas, Max (Hrsg.), Beck'sche Kurzkommentare Band 17 - Strafrechtliche Nebengesetze, 222. EL, 2018 (Zit: *Bearbeiter* in *Erbs/Kohlhaas*).

Eren, Evren/Detken, Kai-Oliver, Mobile Security: Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit, Wien 2006.

Falliere, Nicolas/O Murchu, Liam/Chien, Eric, W32.Stuxnet Dossier, 1.2.2011. Abrufbar unter [https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf] (Stand vom 7.4.2019).

Feuerich, Wilhelm E./Weyland, Dag (Hrsg.), Bundesrechtsanwaltsordnung: Berufsordnung, Fachanwaltsordnung, Partnerschaftsgesellschaftsgesetz, Recht für Anwälte aus dem Gebiet der Europäischen Union, Patentanwaltsordnung ; Kommentar, 9. Aufl., München 2016 (Zit: *Bearbeiter* in *Feuerich/Weyland*).

Fiebig, Peggy, Wieso, weshalb, warum.....? - Fragen und Antworten zum elektronischen Rechtsverkehr, BRAK-Magazin 02/2014 4–5.

Filges, Axel C., Digital und trotzdem sicher, BRAK-Mitteilungen 2014, 113.

Fischer, Nikolaj, Justiz-Kommunikation: Überlegungen zur Elektronifizierung der Ziviljustiz und von zivilgerichtlichen Verfahren am Beispiel des „Justizkommunikationsgesetzes", Berlin 2004.

Fischer, Nikolaj, Justiz-Kommunikation - „Reform der Form"?, Deutsche Richterzeitung 2005, 90.

Fox, Dirk, Eine kritische Würdigung des SigG, Datenschutz und Datensicherheit 1999, 508.

Friauf, Karl Heinrich/Höfling, Wolfram (Hrsg.), Berliner Kommentar zum Grundgesetz, EL 3/2018, Berlin 2018 (Zit: *Bearbeiter* in *Friauf/Höfling*).

Gass, Wolfram, Digitale Wasserzeichen als urheberrechtlicher Schutz digitaler Werke?, Zeitschrift für Urheber- und Medienrecht 1999, 815.

Geier, Eric, 5 Wi-Fi security myths you must abandon now, 7.10.2013. Abrufbar unter [http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html] (Stand vom 7.4.2019).

Geis, Ivo, Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce, Multimedia und Recht 2000, 667 ff.

Gerhards, Julia, (Grund-)Recht auf Verschlüsselung?, 1. Aufl., Dissertation, Baden-Baden 2010.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., München 2018 (Zit: *Bearbeiter* in *Gola*).

Gola, Peter/Klug, Christoph, Grundzüge des Datenschutzrechts, München 2003.

Gola, Peter/Klug, Christoph/Reif, Yvette, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung", Neue Juristische Wochenschrift 2007, 2599.

Gola, Peter/Schomerus, Rudolf (Hrsg.), BDSG Bundesdatenschutzgesetz: Kommentar, 12. Aufl., München 2015 (Zit: *Bearbeiter* in *Gola*/*Schomerus*).

Governikus GmbH & Co. KG, Anwenderdokumentation Elektronisches Gerichts- und Verwaltungspostfach - Sichere Kommunikation mit Gerichten und Behörden -, EGVP Version 3.0.1.0, 5.1.2017. Abrufbar unter [https://web.archive.org/web/20181125231819/https://egvp.justiz.de/pdf/dokumentationen/Anwenderdokumentation1.pdf] (Stand vom 7.4.2019). (Zit: EGVP-Anwenderdokumentation)

Governikus GmbH & Co. KG, Anwenderhandbuch Governikus Prüfprotokoll, 16.8.2016. Abrufbar unter [https://web.archive.org/web/20170209054156/http://www.egvp.de/pdf/dokumentationen/Governikus-Pruefprotokoll.pdf] (Stand vom 7.4.2019). (Zit: Governikus-Prüfprotokoll)

Governikus GmbH & Co. KG, Governikus KG: Governikus KG auf dem 25. EDV-Gerichtstag in Saarbrücken, 8.9.2016. Abrufbar unter [https://web.archive.org/web/20170202175512/https://www.governikus.de/newsroom-presse/details/?tx_ttnews%5Btt_news%5D=421&cHash=57e273fb8c3362b18fc103548d7e16f0] (Stand vom 7.4.2019). (Zit: 25. EDVGT)

Grabenwarter, Christoph/Pabel, Katharina, Europäische Menschenrechtskonvention: ein Studienbuch, 5. Aufl., München 2012.

Groeben, von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.), Europäisches Unionsrecht, 7. Aufl., 2015 (Zit: *Bearbeiter* in *Groeben*/*Schwarze*/*Hatje*).

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.), Art. 1 bis 55 EUV, Art. 1 bis 54 GRC, Art. 1 bis 66 AEUV, 7. Aufl., Baden-Baden 2015 (Zit: *Bearbeiter* in *Groeben*/*Schwarze*/*Hatje*).

Häder, Michael, Der Datenschutz in den Sozialwissenschaften Anmerkungen zur Praxis sozialwissenschaftlicher Erhebungen und Datenverarbeitung in Deutschland - RatSWD Working Paper No. 90, Abrufbar unter [http://www.ratswd.de/download/RatSWD_WP_2009/RatSWD_WP_90.pdf] (Stand vom 7.4.2019).

Hähnchen, Susanne, Elektronische Akten bei Gericht - Chancen und Hindernisse, Neue Juristische Wochenschrift 2005, 2257.

Halderman, J. Alex/Schoen, Seth D./Heninger, Nadia/Clarkson, William u. a., Lest We Remember: Cold Boot Attacks on Encryption Keys, Abrufbar unter [http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf] (Stand vom 7.4.2019).

Härting, Niko, Starke Behörden, schwaches Recht - der neue EU-Datenschutzentwurf, Betriebsberater 2012, 459.

Härting, Niko, Anwaltsgeheimnis: Schutz vor dem Datenschutz, Anwaltsblatt 2011, 50.

Härting, Niko, Datenschutz und Anwaltsgeheimnis - Subsidiarität oder Spezialität?, Anwaltsblatt 2005, 131.

Häublein, Martin, Zustellungsrecht - Zustellung von „Anwalt zu Anwalt“ nach der Reform, Monatsschrift für deutsches Recht 2002, 563.

Heckmann, Dirk (Hrsg.), juris PraxisKommentar Internetrecht, 5. Aufl., Saarbrücken 2017 (Zit: *Bearbeiter* in *Heckmann*).

Heckmann, Dirk/Seidl, Alexander/Maisch, Michael Marc, Adäquates Sicherheitsniveau bei der elektronischen Kommunikation: der Einsatz des E-Postbriefs bei Berufsgeheimnisträgern, Stuttgart u.a. 2012.

Hecksteden, Ralph, Die Ende-zu-Ende-Verschlüsselung des besonderen elektronischen Anwaltspostfachs, Abrufbar unter [https://gersheim.rechtsanwaltskanzlei-saarland.de/aJX1_bea_ende_zu_ende_verschluesselung.shtml] (Stand vom 7.4.2019). (Zit: Ende-zu-Ende-Verschlüsselung)

Henschler, Katja, Internet im Schneckentempo: Weder vertretbar noch zeitgemäß, 13.11.2015. Abrufbar unter [http://www.tagesspiegel.de/themen/breitbandausbau-in-deutschland/schnelles-internet-internet-im-schneckentempo-weder-vertretbar-noch-zeitgemaess/12584490.html] (Stand vom 7.4.2019). (Zit: Internet im Schneckentempo)

Henssler, Martin, Das anwaltliche Berufsgeheimnis, Neue Juristische Wochenschrift 1994, 1817.

Hessisches Ministerium der Justiz, Länderbericht - Hessen, 7.2016. Abrufbar unter [http://www.justiz.de/BLK/laenderberichte/hessen.pdf;jsessionid=768162089EC5EB8E9CEC25930F4874F6] (Stand vom 7.4.2019). (Zit: Länderbericht 2016)

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, 47. EL, München 2018 (Zit: *Bearbeiter* in *Hoeren*/*Sieber*/*Holznagel*).

Hoffmann, Christian/Borchers, Kim Corinna, Das besondere elektronische Anwaltspostfach - Eine Förderung des elektronischen Rechtsverkehrs mit den Gerichten, Computer und Recht 2014, 62.

Hoffmann, Christian/Luch, Anika D./Schulz, Sönke E./Tallich, Maximilian u. a., Der E-Postbrief in der öffentlichen Verwaltung, Kiel 2011.

Holland, Martin, Gehackte Kreditkartendaten: Mehr als 1000 US-Unternehmen betroffen | heise Security, 23.8.2014. Abrufbar unter [http://www.heise.de/security/meldung/Gehackte-Kreditkartendaten-Mehr-als-1000-US-Unternehmen-betroffen-2301320.html] (Stand vom 7.4.2019). (Zit: Kreditkartenhack)

Hornung, Gerrit, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012, Zeitschrift für Datenschutz 2012, 99.

Hornung, Gerrit, Ein neues Grundrecht - Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, Computer und Recht 2008, 299.

Huber, Peter, Auslegung und Anwendung der Charta der Grundrechte, Neue Juristische Wochenschrift 2011, 2385–2390.

Ion, Iulia/Reeder, Rob/Consolvo, Sunny, „...no one can hack my mind“: Comparing Expert and Non-Expert Security Practices, Abrufbar unter [https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf] (Stand vom 7.4.2019).

Jarass, Hans Dieter (Hrsg.), Charta der Grundrechte der Europäischen Union, 3. Aufl., München 2016 (Zit: *Bearbeiter* in *Jarass*).

Jarass, Hans Dieter/Pieroth, Bodo (Hrsg.), Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 15. Aufl., München 2018 (Zit: *Bearbeiter* in *Jarass*/*Pieroth*).

Jaspers, Andreas, Die EU-Datenschutz-Grundverordnung, Datenschutz und Datensicherheit 2012, 571.

Johannes, Paul Christopher, Entwurf des eIDAS-Durchführungsgesetzes in der Ressortabstimmung, ZD-Aktuell 21 2016, 05423.

Kannenberg, Axel, „Statistisch gesehen“: Windows 7 auf Desktops immer noch deutlich vor Windows 10, 28.9.2016. Abrufbar unter [http://www.heise.de/newsticker/meldung/Statistisch-gesehen-Windows-7-auf-Desktops-immer-noch-deutlich-vor-Windows-10-3334979.html] (Stand vom 7.4.2019). (Zit: „Statistisch gesehen“: Windows 7 auf Desktops immer noch deutlich vor Windows 10)

Kessler, Gary Craig, ISDN: concepts, facilities, and services, 2. Auflage, New York [u.a.] 1993.

Kilian, Matthias/Rimkus, Felix, Elektronischer Rechtsverkehr: Wie gut ist die Anwaltschaft vorbereitet?, Anwaltsblatt 2014, 913.

Kleinz, Torsten/Kuri, Jürgen, Die Telekom und der NSA-Skandal: Auf ins Schengen-Netz, 11.11.2013. Abrufbar unter [http://www.heise.de/netze/meldung/Die-Telekom-und-der-NSA-Skandal-Auf-ins-Schengen-Netz-2043536.html] (Stand vom 7.4.2019). (Zit: Die Telekom und der NSA-Skandal)

Klink, Judith, Datenschutz in der elektronischen Justiz, Dissertation, Kassel 2010.

Kossens, Michael/Heide, Dirk von der/Maaß, Michael (Hrsg.), SGB IX, 4. Aufl., München 2015 (Zit: *Bearbeiter* in *Kossens*/*Heide, von der*/*Maaß*).

Kramer, Philipp, Verbot mit Erlaubnisvorbehalt zeitgemäß?, Datenschutz und Datensicherheit 2013, 380.

Krempl, Stefan, Verband Breko warnt: Breitbandziel der Bundesregierung wird verfehlt, Abrufbar unter [http://www.heise.de/newsticker/meldung/Verband-Breko-warnt-Breitbandziel-der-Bundesregierung-wird-verfehlt-3318481.html] (Stand vom 7.4.2019).

Kröger, Detlef/Hoffmann, Dirk (Hrsg.), Rechts-Handbuch zum E-Government, Köln 2005 (Zit: *Bearbeiter* in E-Government).

Kruchen, David, Telekommunikationskontrolle zur Prävention und Aufdeckung von Straftaten im Arbeitsverhältnis, Dissertation, Frankfurt am Main 2012.

Krüger, Wolfgang/Rauscher, Thomas (Hrsg.), Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Band 1: §§ 1 - 354, 5. Aufl., München 2016 (Zit: *Bearbeiter* in MüKo-ZPO Band 1).

Krüger, Wolfgang/Rauscher, Thomas (Hrsg.), Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Band 2: §§ 355 - 1024, 5. Aufl., München 2016 (Zit: *Bearbeiter* in MüKo-ZPO Band 2).

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., 2018 (Zit: *Bearbeiter* in *Kühling*/*Buchner*).

Kühling, Jürgen/Schall, Tobias, WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, Computer und Recht 2015, 641–655.

Lapp, Thomas, Brauchen wir De-Mail und Bürgerportale? Überflüssige Anwendung mit Geburtsfehlern, Datenschutz und Datensicherheit 2011, 651.

Leutheusser-Schnarrenberger, Sabine, Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, Zeitschrift für Rechtspolitik 2007, 9.

Limperg, Bettina, Elektronisch einreichen und zustellen: Erleichterung oder Haftungsfalle für Anwälte? Haftungsrechtliche Probleme im Zusammenhang mit dem Elektronischen Rechtsverkehr, AnwBl 2013, 98–101.

Lindloff, Dirk, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, Dissertation, Marburg 2005.

Lorenz, Pia, AGH: Keine Nutzungspflicht, solange das beA offline ist, Legal Tribune Online, 8.8.2018. Abrufbar unter [https://www.lto.de/recht/juristen/b/agh-berlin-ii-agh-2-18-elektronisches-anwaltspostfach-keine-passive-nutzungspflicht-solange-bea-offline/] (Stand vom 7.4.2019). (Zit: beA-Nutzungspflicht)

Lorenz, Pia, beA: Der Gegner weiß, ob Sie schon angemeldet sind, Legal Tribune Online, 6.9.2018. Abrufbar unter [https://www.lto.de/recht/juristen/b/bea-anwaltspostfach-zeigt-nutzerstatus-anwaltliche-pflicht-nutzung/] (Stand vom 7.4.2019). (Zit: beA-Anmeldung)

Lucke, Jörn von/Reinermann, Heinrich, Speyerer Definition von Electronic Government - Online-Publikation, Speyer 2000. Abrufbar unter [http://www.joernvonlucke.de/ruvii/Sp-EGov.pdf] (Stand vom 7.4.2019).

Mao, Wenbo/Paterson, Kenneth G., On the plausible deniability feature of internet protocols, 2002. Abrufbar unter [http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.2401&rep=rep1&type=pdf] (Stand vom 7.4.2019).

Maunz, Theodor/Dürig, Günter (Hrsg.), Grundgesetz-Kommentar, 85. EL, 2018 (Zit: *Bearbeiter* in *Maunz*/*Dürig*).

Meyer-Seitz, Christian, Förderung des elektronischen Rechtsverkehrs mit den Gerichten - Modernisierung der Kommunikation im Prozess - Bundesregierung legt Gesetzentwurf vor, AnwBl 2013, 89–91.

Mikkilineni, Aravind K./Khanna, Nitin/Delp, Edward J., Texture Based Attacks on Intrinsic Signature Based Printer Identification, Abrufbar unter [https://engineering.purdue.edu/~prints/public/papers/khanna_spie_2010.pdf] (Stand vom 7.4.2019).

Ministerium der Justiz und für Europa Baden-Württemberg, Elektronisches Gerichts- und Verwaltungspostfach (EGVP), 25.2.2016. Abrufbar unter [http://www.ejustice-

bw.de/pb/,Lde/Startseite/Behoerden/Elektronisches+Gerichts_+und+Verwaltungspostfach+_EGVP_] (Stand vom 7.4.2019). (Zit: EGVP)

Müller, Matthias, Die Digitalisierung der Justiz in Deutschland: Entwicklung und rechtliche Würdigung des EJustizG am Beispiel des Zivilprozesses, Hamburg 2015.

Musielak, Hans-Joachim/Voit, Wolfgang (Hrsg.), Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz, 15. Aufl., München 2018 (Zit: *Bearbeiter* in *Musielak*/*Voit*).

Neal, Dave, AES encryption is cracked | The Inquirer, 17.8.2011. Abrufbar unter [http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked] (Stand vom 7.4.2019). (Zit: AES is cracked)

Neumann, Linus, Chaos Computer Club - Stellungnahme zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, 20.3.2013. Abrufbar unter [http://ccc.de/system/uploads/126/original/stellungnahme-demail2013.pdf] (Stand vom 7.4.2019). (Zit: Stellungnahme EGovG)

NotarNet GmbH, Nachweis es Eingangs einer Nachricht im EGVP, Abrufbar unter [http://elrv.info/_medien/faq/EGVP-Eingangsnachweis.pdf] (Stand vom 7.4.2019). (Zit: Eingangsnachweis)

Opitz, Rudolf, Xerox-Multifunktionsgeräte vertauschen Ziffern bei klein gedruckten Scan-Vorlagen, c't - magazin für computer technik 19/2013 40.

OSCI Leitstelle, Projektauftrag OSCI-Transport 1.2, 2.4.2002. Abrufbar unter [http://www.xoev.de/sixcms/media.php/13/projektauftrag%20osci-transport%201_2.pdf] (Stand vom 7.4.2019). (Zit: Projektauftrag OSCI Transport 1.2)

OSCI Leitstelle, OSCI-Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen, 6.6.2002. Abrufbar unter [www.xoev.de/sixcms/media.php/13/osci_entwurfsprinzipien_1_2.pdf] (Stand vom 7.4.2019). (Zit: OSCI-Transport 1.2 Entwurfsprinzipien)

OSCI Leitstelle, OSCI-Transport 1.2 - Spezifikation, 6.6.2002. Abrufbar unter [http://www.xoev.de/sixcms/media.php/13/osci_spezifikation_1_2_deutsch.pdf] (Stand vom 7.4.2019). (Zit: OSCI-Transport 1.2 Spezifikation)

Otter, Thomas/Rieck, Olaf, Vortragsfolien „Projekt eJustice Akzeptanzstudie", 3.9.2012. Abrufbar unter [https://justizministerium.hessen.de/sites/default/files/HMdJIE/04_kommunikation_zwischen_anwaelten_und_justiz.pdf] (Stand vom 7.4.2019). (Zit: Vortrag eJustice-Akzeptanzstudie)

Peterson, Andrea, LOVEINT: When NSA officers use their spying power on love interests, washingtonpost.com 24.8.2013, Abrufbar unter [https://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests] (Stand vom 7.4.2019).

Piegdon, David R., Hacking in physically addressable memory - a proof of concept, Abrufbar unter [http://eh2008.koeln.ccc.de/fahrplan/attachments/1067_SEAT1394-svn-r432-paper.pdf] (Stand vom 7.4.2019).

Plath, Kai-Uwe (Hrsg.), BDSG: Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, 2. Aufl., Köln 2013 (Zit: *Bearbeiter* in *Plath*).

Puschke, Jens/Singelnstein, Tobias, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, Neue Juristische Wochenschrift 2008, 113.

Rechtsanwaltskammer München, Fragen zur Einführung des elektronischen Rechtsverkehrs mit den Gerichten, 24.2.2014. Abrufbar unter [https://rak-muenchen.de/fileadmin/downloads/06-Mitgliederservice/11-ElektronischerRechtsverkehr/FragenERV20140224.pdf] (Stand vom 7.4.2019). (Zit: Fragen zum ERV)

Rechtsanwaltskammer Sachsen, FAQ zu ERV, 25.8.2014. Abrufbar unter [http://www.rak-sachsen.de/elektronischer-rechtsverkehr/faq/] (Stand vom 7.4.2019). (Zit: FAQ zu ERV)

Redeker, Helmut, EU-Signaturrichtlinie und Umsetzungsbedarf im deutschen Recht, Computer und Recht 2000, 455 ff.

Redeker, Helmut/Conrad, Isabell/Härting, Niko/Huppertz, Peter u. a., Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zur Bundesratsinitiative der Länder Baden-Württemberg, Sachsen und Hessen zur Förderung des elektronischen Rechtsverkehrs, Abrufbar unter [https://anwaltverein.de/de/newsroom/id-2012-14] (Stand vom 7.4.2019). (Zit: DAV-Stellungnahme 14/2012)

Redeker, Helmut/Conrad, Isabell/Härting, Niko/Huppertz, Peter u. a., Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zum Diskussionsentwurf des Bundesministeriums der Justiz Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs bei den Gerichten, Abrufbar unter [http://anwaltverein.de/de/newsroom/id-2012-64?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2012/2012-64-Stellungnahme.pdf] (Stand vom 7.4.2019). (Zit: DAV-Stellungnahme 64/2012)

Roßnagel, Alexander (Hrsg.), Beck'scher Kommentar zum Recht der Telemediendienste : Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr, München 2013 (Zit: *Bearbeiter* in Telemediendienste).

Roßnagel, Alexander, Das Recht der Vertrauensdienste, Baden-Baden 2016.

Roßnagel, Alexander, Das Signaturgesetz, Datenschutz und Datensicherheit 1997, 75 ff.

Roßnagel, Alexander, Das Gesetz und die Verordnung zur digitalen Signatur - Entstehung und Regelungsgehalt, Recht der Datenverarbeitung 1998, 5 ff.

Roßnagel, Alexander, Digitale Signaturen im europäischen elektronischen Rechtsverkehr, Kommunikation und Recht 2000, 314 ff.

Roßnagel, Alexander, Das neue Recht elektronischer Signaturen, Neue Juristische Wochenschrift 2001, 1817–1826.

Roßnagel, Alexander, Vorratsdatenspeicherung rechtlich vor dem Aus?, Neue Juristische Wochenschrift 2017, 696–698.

Roßnagel, Alexander, Wie zukunftsfähig ist die Datenschutz-Grundverordnung?, Datenschutz und Datensicherheit 2017, 561.

Roßnagel, Alexander (Hrsg.), Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts, 1. Aufl., Baden-Baden 2017 (Zit: *Bearbeiter*

in Europäische Datenschutz-Grundverordnung).

Roßnagel, Alexander (Hrsg.), Besondere Datenschutzpflichten, München 2003 (Zit: *Bearbeiter* in Handbuch Datenschutzrecht).

Roßnagel, Alexander, Der Anwendungsvorrang der eIDAS-Verordnung, Multimedia und Recht 2015, 359.

Roßnagel, Alexander, Neue Regeln für sichere elektronische Transaktionen, Neue Juristische Wochenschrift 2014, 3686.

Roßnagel, Alexander/Hornung, Gerrit/Knopp, Michael/Wilke, Daniel, De-Mail und Bürgerportale, Datenschutz und Datensicherheit 2009, 728–734.

Roßnagel, Alexander/Hornung, Gerrit/Schnabel, Christoph, Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht, Datenschutz und Datensicherheit 2008, 168.

Roßnagel, Alexander/Kroschwald, Steffen, Was wird aus der Datenschutzgrundverordnung? Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, Zeitschrift für Datenschutz 2014, 495.

Roßnagel, Alexander/Pfitzmann, Andreas, Der Beweiswert von E-Mail, Neue Juristische Wochenschrift 2003, 1209.

Roßnagel, Alexander/Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, Neue Juristische Wochenschrift 2008, 3534–3538.

Rüpke, Giselher, Freie Advokatur, anwaltliche Informationsverarbeitung und Datenschutzrecht: berufs- und verfassungsrechtliche Aspekte; mit zusammenfassenden Leitsätzen, München 1995.

Rüpke, Giselher, Anwaltsrecht und Datenschutzrecht, Neue Juristische Wochenschrift 1993, 3097.

Sachs, Michael/Battis, Ulrich (Hrsg.), Grundgesetz: Kommentar, 8. Aufl., München 2018 (Zit: *Bearbeiter* in *Sachs*/*Battis*).

Sandhu, Aqilah, Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union. – Anmerkung zum Urteil des EuGH vom 21.12.2016 in der Rs. EUGH Aktenzeichen C-203/15 (Tele2), Europarecht 2017, 453–470.

Sandkühler, Christoph, Elektronischer Rechtsverkehr ante portas, KammerMitteilungen Rechtsanwaltskammer Düsseldorf 1/2014 45 f.

Schatz, Bradley/Mohay, George/Clark, Andrew, A correlation method for establishing provenance of timestamps in digital evidence, Digital Investigation 3S 2006, Abrufbar unter [http://dfrws.org/2006/proceedings/13-%20Schatz.pdf] (Stand vom 7.4.2019).

Scherf, Uwe Jürgen/Schmieszek, Hans-Peter/Viefhues, Dr. Wolfram (Hrsg.), Elektronischer Rechtsverkehr: Kommentar und Handbuch, Karlsruhe 2006 (Zit: *Bearbeiter* in *Scherf*/*Schmieszek*/*Viefhues*).

Scherschel, Fabian A., Aufgepasst: Neue Ransomware Goldeneye verbreitet sich rasant, 6.12.2016.

Abrufbar unter [http://www.heise.de/security/meldung/Aufgepasst-Neuer-Verschluesselungstrojaner-Goldeneye-verbreitet-sich-rasant-3561396.html] (Stand vom 7.4.2019). (Zit: Goldeneye)

Schirrmacher, Dennis, 1&1, GMX und Web.de: Millionen E-Mail-Postfächer waren angreifbar, Abrufbar unter [http://www.heise.de/security/meldung/1-1-GMX-und-Web-de-Millionen-E-Mail-Postfaecher-waren-angreifbar-2782618.html] (Stand vom 7.4.2019). (Zit: WebMail)

Schirrmacher, Dennis/Mett, Matthias, TrueCrypt ist tot, es lebe VeraCrypt - Ein Blick hinter die Kulissen des Verschlüsselungs-Tools VeraCrypt, c't - magazin für computer technik 14/2016 136.

Schmidhuber, Martin, Verhaltenskodizes im nationalen und Grenzüberschreitenden elektronischen Geschäftsverkehr, Dissertation, Frankfurt am Main 2004.

Schmidt, Jürgen, Krypto für jedermann - richtig verschlüsseln mit Linux, c't - magazin für computer technik 11/2011 192.

Schmidt-Bleibtreu, Bruno/Hofmann, Hans/Henneke, Hans-Günter (Hrsg.), GG: Kommentar zum Grundgesetz, 14. Aufl., Köln 2018 (Zit: *Bearbeiter* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*).

Schmittmann, Michael/Kempermann, Philip, Vorratsdatenspeicherung: Verfassungsmäßigkeit der Pläne der EU?, AfP - Zeitschrift für Medien- und Kommunikationsrecht 2005, 254.

Schmundt, Hilmar, Datendiebstahl aus der Luft, Der Spiegel 14.8.2006, Abrufbar unter [http://www.spiegel.de/spiegel/print/d-48262933.html] (Stand vom 7.4.2019).

Schnee-Gronauer, Bärbel/Schnee-Gronauer, Andreas, Software in Kanzleien: Marktüberblick, Trends und Hinweise für die Praxis. Ergebnisse einer Untersuchung der Arbeitsgemeinschaft Kanzleimanagement im DAV, Anwaltsblatt 2013, 776.

Schneider, Jochen/Härting, Niko, Warum wir ein neues BDSG brauchen - Kritischer Beitrag zum BDSG und dessen Defiziten, Zeitschrift für Datenschutz 2016, 63.

Schneier, Bruce, Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, 1. Aufl., Bonn/Reading/Menlo Park u.a. 1996.

Schneier, Bruce, „Evil Maid" Attacks on Encrypted Hard Drives - Schneier on Security, Abrufbar unter [https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html] (Stand vom 7.4.2019). (Zit: Schneier on Security 10/2009)

Scholz, Bernhard Joachim, Stellungnahme des Deutschen Richterbundes zum Diskussionsentwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs in der Justiz (E-Justice Bundesratsinitiative; Stand: 8. Januar 2012), 2.2012. Abrufbar unter [https://web.archive.org/web/20170320134258/http://www.drb.de/stellungnahmen/2012/e-justice.html] (Stand vom 7.4.2019). (Zit: DRB Stellungnahme Nr. 04/12)

Schultze, Christine/Deutsche Presse-Agentur, Viele Firmen kämpfen auch 2016 mit Breitband-Lücken, Abrufbar unter [http://www.heise.de/newsticker/meldung/Viele-Firmen-kaempfen-auch-2016-mit-Breitband-Luecken-3057228.html] (Stand vom 7.4.2019).

Schumacher, Stephan, Einigung auf EU-Signaturrichtlinie, Computer und Recht 1999, 473 ff.

Schuster, Fabian, E-Mail-Dienste als Telekommunikationsdienste?, Computer und Recht 2016, 173–185.

Schwoerer, Max, Die elektronische Justiz: ein Beitrag zum elektronischen Rechtsverkehr und zur elektronischen Akte unter Berücksichtigung des Justizkommunikationsgesetzes, Berlin 2005.

secunet Security Networks AG, Technische Analyse und Konzeptprüfung des beA, Abschlussgutachten im Auftrag der Bundesrechtsanwaltskammer, Version 1.0, 18.6.2018. Abrufbar unter [https://www.brak.de/w/files/04_fuer_journalisten/presseerklaerungen/pe-18-anlage1.pdf] (Stand vom 7.4.2019). (Zit: beA-Abschlussgutachten)

Segura, Jérôme, Large Malvertising Campaign Goes (Almost) Undetected, 14.9.2015. Abrufbar unter [https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/] (Stand vom 7.4.2019). (Zit: Malvertising)

Sellner, Michael, Die Justiz im elektronischen Zeitalter: elektronischer Rechtsverkehr und elektronische Akte in der Justiz, Dissertation, Jena 2012.

Shannon, Claude Elwood/Weaver, Warren, The mathematical theory of communication, Urbana, University of Illinois Press 1963.

Shantz, Peter/Wolff, Heinrich Amadeus (Hrsg.), Das neue Datenschutzrecht, München 2017 (Zit: *Bearbeiter* in *Shantz*/*Wolff*).

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8., neu bearb. Aufl., Baden-Baden 2014 (Zit: *Bearbeiter* in *Simitis*).

Sommerschuh, Nicole, Berufshaftung und Berufsaufsicht: Wirtschaftsprüfer, Rechtsanwälte und Notare im Vergleich, 1. Aufl., Baden-Baden 2003.

Sosna, Sabine, EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten – eIDAS-Verordnung, Computer und Recht 2014, 825–832.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien: Kommentar, 3. Aufl., München 2015 (Zit: *Bearbeiter* in *Spindler*/*Schuster*).

Spolsky, Joel, The Absolute Minimum Every Software Developer Absolutely, Positively Must Know About Unicode and Character Sets (No Excuses!) - Joel on Software, 8.10.2003. Abrufbar unter [http://www.joelonsoftware.com/articles/Unicode.html] (Stand vom 7.4.2019). (Zit: Unicode and Character Sets)

Stern, Klaus/Becker, Florian (Hrsg.), Grundrechte-Kommentar, 2. Aufl., Köln 2016 (Zit: *Bearbeiter* in *Stern*/*Becker*).

Stinson, Douglas R., Cryptography: Theory and Practice, 2. Aufl., Boca Raton/London/New York u.a. 2002.

Stollhof, Sabine, Datenschutzgerechtes E-Government: Eine Untersuchung am Beispiel des Einheitlichen Ansprechpartners nach der Europäischen Dienstleistungsrichtlinie, Dissertation, Baden-Baden 2012.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2., überarb. Aufl., Frankfurt am Main 2013 (Zit: *Bearbeiter* in *Taeger*/*Gabel*).

Telekom, T-Online: Leistungsbeschreibung und Preise De-Mail Basic, 2.9.2013. Abrufbar unter [https://web.archive.org/web/20171230131530/https://www.telekom.de/dlp/agb/pdf/43269.pdf] (Stand vom 7.4.2019). (Zit: T-Online: De-Mail-Preisliste)

Tettenborn, Alexander, Die Novelle des Signaturgesetzes, Computer und Recht 2000, 683 ff.

Thomale, Hans-Christoph, Haftung und Prävention nach dem Signaturgesetz, Dissertation, Baden-Baden 2003.

Tjensvold, Jan Magne, Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards, Abrufbar unter [https://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf] (Stand vom 7.4.2019).

Verbraucherzentrale.de, Trojaner im Anmarsch, 29.3.2017. Abrufbar unter [https://www.verbraucherzentrale.de/gefaehrliche-e-mail-anhaenge] (Stand vom 7.4.2019). (Zit: Trojaner)

Viefhues, Wolfram, Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, Neue Juristische Wochenschrift 2005, 1009–1016.

Volk, Ulrich/Burianski, Markus/Feil, Thomas/Redeker, Helmut u. a., Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Elektronischer Rechtsverkehr zum Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, Abrufbar unter [https://anwaltverein.de/de/newsroom/id-2012-87] (Stand vom 7.4.2019). (Zit: DAV-Stellungnahme 87/2012)

Volk, Ulrich/Burianski, Markus/Redeker, Helmut/Schafhausen, Martin u. a., Stellungnahme Nr. 6/2016 des Deutschen Anwaltvereins durch den Ausschuss Elektronischer Rechtsverkehr zur Einführung und Ausgestaltung des besonderen elektronischen Anwaltspostfachs (beA), Abrufbar unter [https://anwaltverein.de/de/newsroom/sn-6-2016-zur-einfuehrung-und-ausgestaltung-des-besonderen-elektronischen-anwaltpostfachs-bea?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2016/DAV-SN-%206.pdf] (Stand vom 7.4.2019). (Zit: DAV-StN. Nr. 6/2016)

Vossius, Oliver, Stellungnahme Deutscher Notarverein - Diskussionsentwurf einer Bundesratsinitiative für ein Gesetz zur Förderung des elektronischen Rechtsverkehrs in der Justiz (nachfolgend „DiskE“) - Zum Schreiben vom 27. Dezember 2011, Abrufbar unter [http://www.dnotv.de/_files/Dokumente/Stellungnahmen/StellungnahmeE-Rechtsverkehr-endg.pdf] (Stand vom 7.4.2019). (Zit: DNotV-StN. vom 29.2.2012)

Weber, Rolf H., E-Commerce und Recht, Zürich 2010.

Welte, Harald, Sichere und vertrauenswürdige elektronische Kommunikation via De-Mail - Stellungnahme des Chaos Computer Clubs, 3.2.2011. Abrufbar unter [http://www.ccc.de/system/uploads/64/original/CCC-de-mail-2011.pdf] (Stand vom 7.4.2019).

Welti, Felix, Behinderung und Rehabilitation im sozialen Rechtsstaat: Freiheit, Gleichheit und Teilhabe behinderter Menschen, Habilitation, Tübingen 2005.

Werner, Dennis/Wegener, Christoph, Bürgerportale - Technische und rechtliche Hintergründe von DE-Mail und Co., Computer und Recht 2009, 310.

Wilkens, Andreas, „Recht auf Vergessen“: Google muss Links zu personenbezogenen Daten entfernen | heise online, 13.5.2014. Abrufbar unter [http://www.heise.de/newsticker/meldung/Recht-auf-Vergessen-Google-muss-Links-zu-personenbezogenen-Daten-entfernen-2188014.html] (Stand vom 7.4.2019). (Zit: Heise-Newsticker 13.5.2014)

Wirtgen, Dirk, Android-Verteilung: erstmals wächst nur Android 6 „Marshmallow“, 4.5.2016.

Abrufbar unter [http://www.heise.de/newsticker/meldung/Android-Verteilung-erstmals-waechst-nur-Android-6-Marshmallow-3196790.html] (Stand vom 7.4.2019).

Wirtz, Bernd W. (Hrsg.), E-Government: Grundlagen, Instrumente, Strategien, Speyer 2010 (Zit: *Bearbeiter* in *Wirtz*).

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), BeckOK Datenschutzrecht, 26. Ed., 2018 (Zit: *Bearbeiter* in *Wolff/Brink*).

Wybitul, Tim, EU-Datenschutz-Grundverordnung in der Praxis - was ändert sich durch das neue Datenschutzrecht?, Betriebsberater 2016, 1077.

Zertifizierungsstelle der Bundesnotarkammer (Hrsg.), Anleitung zur Schlüsselverwaltung Ihrer beA-Karte, 9.2016. Abrufbar unter [https://bea.bnotk.de/documents/Schluesselverwaltung_beA.pdf] (Stand vom 7.4.2019). (Zit: Anleitung beA-Schlüsselverwaltung)

Ziebarth, Wolfgang, Die Vorratsdatenspeicherung im Wandel der EuGH-Rechtsprechung, Zeitschrift für Urheber- und Medienrecht 2017, 398–405.

Zöller, Richard (Hrsg.), Zivilprozessordnung, 32. Aufl., Köln 2018 (Zit: *Bearbeiter* in *Zöller*).

Abkürzungsverzeichnis

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
b2a	business to administration
b2b	business to business
b2c	business to consumer/client
beA	besonderes elektronisches Anwaltspostfach
CA	Certificate Authority
CAD	Computer-Aided Design
CAM	Computer-Aided Manufacturing
CD	Compact Disc
CD-R	Compact Disc-Recordable
DES	Data Encryption Standard
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EDV	Elektronische Datenverarbeitung
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
FTP	File Transfer Protocol
GCHQ	Government Communications Headquarters
GnuPG/GPG	GNU Privacy Guard
HSM	Hardware Security Module/Hardware-Sicherheitsmodul
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
IT	Information Technology/Informationstechnologie

ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LUKS	Linux Unified Key Setup
MAC	Media Access Control
nPA	neuer Personalausweis
NSA	National Security Agency
OSCI	Online Services Computer Interface
OTR	Off-The-Record Messaging
PC	Personal Computer
PDF	Portable Document Format
PGP	Pretty Good Privacy
PIN	Personal Identification Number/Persönliche Identifikationsnummer
POP3	Post Office Protocol Version 3
qeS	Qualifizierte elektronische Signatur
RAM	Random Access Memory
RSA	Rivest, Shamir, Aldermann (benannt nach den Erfindern des Kryptosystems)
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAFE	Secure Access to Federated E-Government/E-Justice
SAGA	Standards und Architekturen für E-Government-Anwendungen
SI	Système internationale d‘unités
IP	Internet Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VNC	Virtual Network Computing
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access Version 2
XML	Extensible Markup Language
XÖV	XML in der öffentlichen Verwaltung

1. Teil – Grundlagen

1 Einleitung

Die Informationstechnologie hat die Art, wie wir leben und arbeiten, nachhaltig verändert. Die Benutzung mobiler Endgeräte, die verbreitete Verfügbarkeit schneller Internetverbindungen und die rapide wachsenden Informationsspeicher eröffnen neue Möglichkeiten, aber auch neue Herausforderungen. Obwohl die Nutzung von digitalen Medien und insbesondere des Internets in der Mitte der Gesellschaft angekommen ist, finden viele dieser Neuerungen noch keine Verwendung in der Justiz.[1] Es gab in der Vergangenheit immer wieder Versuche, einen allgemein akzeptierten elektronischen Rechtsverkehr aus der Taufe zu heben. So wurde mit dem Signaturgesetz von 1997 begonnen, erstmals rechtliche Rahmenbedingungen für elektronische Signaturen festzulegen.[2] Mit dem Formvorschriftenanpassungsgesetz von 2001[3] wurden die rechtlichen Grundlagen für eine Gleichstellung von elektronischen Dokumenten mit handschriftlich signierten analogen Dokumenten geschaffen. Dem folgte die Anpassung prozessualer Regelungen an elektronische Kommunikation durch das Justizkommunikationsgesetz[4] von 2005.

Trotz all dieser Bemühungen hat der elektronische Rechtsverkehr noch keine große Verbreitung erfahren. Wenngleich die rechtlichen Möglichkeiten hierfür schon länger durch die genannten Gesetze bestehen, haben erst wenige Bundesländer die nötige Infrastruktur geschaffen, um den elektronischen Rechtsverkehr auch zu nutzen.[5] Die damit verbundene föderale Zersplitterung wird von manchen als ein Hindernis für den elektronischen Rechtsverkehr betrachtet.[6] Entsprechend fehlt es bisher auch an der Akzeptanz bei der Anwaltschaft als professionelle Nutzer des elektronischen Rechtsverkehrs. Der elektronische Rechtsverkehr ist somit nach wie vor als Randerscheinung zu klassifizieren. Daran hat auch die Verfügbarkeit des elektronischen Gerichts- und Verwaltungspostfachs, eines Systems, das für sichere elektronische Kommunikation mit Gerichten und Verwaltung entwickelt wurde und mittlerweile von vielen Gerichten und Behörden in Deutschland unterstützt wird[7], nichts geändert.

1 *Meyer-Seitz*, AnwBl 2013, 89.
2 *Roßnagel* in Telemediendienste, Einl SigG Rn. 1.
3 Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, BGBl. I 1542.
4 Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 22. März 2005, BGBl. I 837.
5 Eine Übersicht findet sich bei *Sellner*, 48.
6 Exemplarisch sind hier die Stellungnahmen der Bundesrechtsanwaltskammer (vgl. *Backs/Kühnelt/Sandkühler/Schmid u. a.*, BRAK-Stellungnahme Nr. 6/2012) sowie des Deutschen Anwaltvereins (vgl. *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 14/2012) zu nennen.
7 Eine Übersicht der teilnehmenden Gerichte findet sich unter http://www.egvp.de/gerichte/index.php, zuletzt abgerufen am 18.12.2017.

Dieser Zustand soll jedoch durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (ERV-Gesetz – ERVG)[8] behoben werden. Das Gesetz beruht auf zwei teilweise kongruenten Gesetzesentwürfen, von denen einer auf die Länder zurückgeht, der andere auf das Bundesjustizministerium.

Auf Initiative der Länder Baden-Württemberg, Sachsen und Hessen wurde Anfang 2012 die erste Fassung eines Diskussionsentwurfs eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs veröffentlicht[9]. Eine überarbeitete Fassung wurde am 30. August 2012 als Gesetzesentwurf in den Bundesrat eingebracht. Der Entwurf hat das Ziel, „durch ein Bündel von Maßnahmen den elektronischen Rechtsverkehr und die elektronische Aktenführung in der Justiz zu fördern und damit zugleich einen zeitgemäßen weiteren Schritt in Richtung Bürgernähe zu vollziehen.“[10]

Am 21. Dezember 2012 folgte die Bundesregierung mit ihrem Entwurf eines „Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten. Auch nach diesem Entwurf soll „das Potential der jüngeren technischen Entwicklungen […] mit gesetzlichen Maßnahmen zur Förderung des elektronischen Rechtsverkehrs auf prozessualem Gebiet genutzt, die Zugangshürden für die elektronische Kommunikation mit der Justiz gesenkt und das Nutzervertrauen im Umgang mit dem neuen Kommunikationsweg gestärkt werden“.[11]

Die Gesetzesentwürfe geben beide zumindest teilweise der qualifizierten elektronischen Signatur die Schuld an der mangelnden Akzeptanz des elektronischen Rechtsverkehrs in der Anwaltschaft. Dies erscheint jedoch zweifelhaft. So legt eine vom Hessischen Ministerium für Justiz, Integration und Europa in Auftrag gegebene Studie der Goethe-Universität Frankfurt am Main nahe, dass der vorrangige Grund für eine Nichtnutzung des elektronischen Rechtsverkehrs in Form des EGVP darin zu sehen ist, dass die potentiellen Anwender keinen Nutzen im elektronischen Rechtsverkehr für sich erkennen können.[12]

Die vorliegende Arbeit möchte einen Beitrag dazu leisten, das Thema elektronischer Rechtsverkehr wissenschaftlich zu erschließen und Chancen und Risiken aufzeigen. Der Fokus soll hierbei auf das elektronische Gerichts- und Verwaltungspostfach EGVP gelegt werden, da sich dieses durch seine – im Vergleich zu anderen Technologien für den elektronischen Rechtsverkehr – hohe Verbreitung

8 BGBl. I 3786.
9 Diskussionsentwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs in der Justiz, abrufbar unter https://edvgt.de/wp-content/uploads/2016/02/E-Justice_Bundesratsinitiative_-_Diskussionsentwurf_Stand_8_Januar_2012.pdf, zuletzt abgerufen am 18.12.2017.
10 Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs in der Justiz, BT-Drs. 17/11691, 1.
11 Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, BT-Drs. 17/12634, 1.
12 Die Ergebnisse der Studie sind noch nicht veröffentlicht, zu den vorläufigen Ergebnissen vgl. *Otter/Rieck*, Vortrag eJustice-Akzeptanzstudie, 22.

auszeichnet. Zudem bildet das System – wenn auch nicht die gleichnamige Software – EGVP die technische Grundlage für das zum 28. November 2016 durch die Bundesrechtsanwaltskammer für alle zugelassenen Rechtsanwälte eingerichtete beA (besonderes elektronisches Anwaltspostfach). Dieses wird mit der Einfügung des § 130d ZPO durch das ERV-Gesetz, mit dem Rechtsanwälte und andere „professionelle Einreicher" zur elektronischen Einreichung von bestimmenden Schriftsätzen verpflichtet werden, besondere Bedeutung erlangen. Demgegenüber steht eine bisher kaum erfolgte juristische Auseinandersetzung mit dieser konkreten Ausgestaltung des elektronischen Rechtsverkehrs. Denn wenngleich zum Thema elektronischer Rechtsverkehr diverse Aufsätze und Monografien existieren, behandeln diese den elektronischen Rechtsverkehr entweder aus einem anderen Blickwinkel, oder thematisieren Gestaltungen des elektronischen Rechtsverkehrs, die mittlerweile durch die neuen Entwicklungen wie das beA überholt worden sind. So beschreibt die Dissertation von *Klink*[13] aus dem Jahre 2010 den elektronischen Rechtsverkehr unter dem Gesichtspunkt des Datenschutzes, ohne sich jedoch auf eine konkrete Gestaltung festzulegen. Eine weitere Dissertation zum Thema elektronischer Rechtsverkehr von *Bergfelder*[14] thematisiert die Möglichkeiten, Beweise mittels des elektronischen Rechtsverkehrs in Gerichtsverfahren einzubringen. Die Dissertation von *Sellner*[15] hingegen untersucht die Gesetzgebungsgeschichte des elektronischen Rechtsverkehrs, ohne aber auf die konkrete Umsetzung mittels des EGVP einzugehen. Die Dissertation von *Müller*[16] schließlich bietet einen Gesamtüberblick über den elektronischen Rechtsverkehr, wählt als Schwerpunkt jedoch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten und behandelt das EGVP und dessen Ausprägung beA nur als eine Umsetzung unter vielen.

Im Gegensatz zu den genannten Arbeiten soll die vorliegende Arbeit eine rechtliche Einordnung des Systems EGVP und seiner neuen, konkreten Ausgestaltung als beA vornehmen. Hierbei soll der Fokus nicht auf die Justizseite gelegt werden, sondern auf die zur Nutzung des elektronischen Rechtsverkehrs verpflichteten Anwälte. Die zu beantwortende Forschungsfrage ist, in wieweit das System EGVP und seine Ausgestaltung, das beA, geeignet sind, um Anforderungen an einen rechtskonformen elektronischen Rechtsverkehr zu genügen. Zur Eingrenzung der Thematik beschränkt sich diese Arbeit auf die zivilprozessuale Sichtweise. Insbesondere soll der elektronische Rechtsverkehr für den Bereich des Strafrechts ausgeklammert werden, da dieser anderen Regeln als der Zivilprozess unterworfen ist und durch zusätzliche, erst nach dem ERV-Gesetz erlassene Regeln

13 *Klink*, Datenschutz in der elektronischen Justiz.
14 *Bergfelder*, Der Beweis im elektronischen Rechtsverkehr.
15 *Sellner*, Die Justiz im elektronischen Zeitalter.
16 *Müller*, Die Digitalisierung der Justiz in Deutschland: Entwicklung und rechtliche Würdigung des EJustizG am Beispiel des Zivilprozesses.

beispielsweise hinsichtlich der Anschluss- und Benutzungspflicht der Anwälte gekennzeichnet ist.[17]

Methodisch will sich diese Arbeit dem Problem durch eine technisch-organisatorische Betrachtung des elektronischen Rechtsverkehrs und der hierbei verwendeten Technologien und Produkte nähern. Ausgangspunkt ist dabei die Überzeugung, dass ohne Verständnis der technischen Gegebenheiten eine saubere rechtliche Einordnung nicht möglich ist. So eröffnet beispielsweise die naheliegende Benutzung von Metaphern und Analogien, um komplizierte technische Sachverhalte auf ein handhabbares Maß herunterzubrechen, die Gefahr, dass durch solche Vereinfachungen eine Verschleierung der tatsächlich ablaufenden Prozesse stattfindet, die einer juristischen Einordnung nicht zuträglich ist. Diese Arbeit möchte insofern einen Beitrag dazu leisten, die Debatte um den elektronischen Rechtsverkehr zu versachlichen, indem – wo es nötig ist – auf allzu starke technische Vereinfachungen verzichtet wird.

Diese Arbeit ist in 3 große Teile gegliedert. In diesem ersten Teil wird zunächst eine Klärung der zum Verständnis notwendigen Begriffe und eine Abgrenzung des Themas vorgenommen. Sodann wird die Geschichte des elektronischen Rechtsverkehrs und insbesondere des EGVP erläutert.

Im zweiten Teil der Arbeit untersucht der Autor die Besonderheiten elektronischer Kommunikation und stellt Kriterien für eine sichere und verlässliche elektronische Kommunikation auf. Hierbei werden sowohl die technischen als auch die rechtlichen Voraussetzungen an elektronischen Rechtsverkehr untersucht und die entsprechenden Rechtsgrundlagen vorgestellt.

Anhand dieser Kriterien werden dann im dritten Teil das elektronische Gerichts- und Verwaltungspostfach und das beA als seine konkrete Ausgestaltung untersucht. Schließlich wird ein Fazit aus dem Ergebnis dieser Untersuchung gezogen und Empfehlungen für eine Fortentwicklung des elektronischen Rechtsverkehrs gegeben.

2 Begriffsklärung und Abgrenzung

Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs hat der Gesetzgeber einen Schritt hin zur Modernisierung überkommener Arbeitsweisen und Technologien in der Justiz getan. Um jedoch diesen Schritt und seine Auswirkungen zu verstehen, ist es zunächst notwendig, sich mit dem Begriff des elektronischen Rechtsverkehrs auseinanderzusetzen. Eine Definition ist insofern nicht trivial, als schon der Begriff des Rechtsverkehrs an sich nicht eindeutig definiert ist. Je nach

17 Die Anpassung der strafprozessualen Vorschriften an den elektronischen Rechtsverkehr erfolgte erst am 5. Juli 2017 mit dem Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs, BGBl. I, 2208.

Sichtweise kann man hier von einem sehr weiten Verständnis ausgehen, das jeglichen Austausch von rechtserheblichen Erklärungen umfasst, oder einen prozessualen Betrachtungswinkel wählen, nach dem Rechtsverkehr nur verfahrensrechtlich beachtliche Erklärungen umfasst. Um sich einer Definiton des elektronischen Rechtsverkehrs zu nähern, muss deswegen zunächst eine Abgrenzung gegenüber anderen, verwandten Phänomenen erfolgen.

2.1 E-Commerce

Der Begriff des E-Commerce wird oft auch als elektronischer Geschäftsverkehr, elektronischer Rechtsgeschäftsverkehr oder – verkürzt und weniger trennscharf – als elektronischer Rechtsverkehr bezeichnet.[18] Für die vorliegende Arbeit soll der Begriff des elektronischen Geschäftsverkehrs benutzt werden, um Verwechslungen mit dem elektronischen Rechtsverkehr nach der Definition des Verfassers zu vermeiden. Elektronischer Geschäftsverkehr beschreibt den „entgeltlichen Vertrieb von Waren oder Dienstleistungen über das Internet“.[19] Er umfasst sowohl die Anbahnung als auch die Abwicklung geschäftlicher Transaktionen.[20] Wenngleich die Bezeichnung *elektronisch* technisch gesehen auch Medien wie das Telefon oder das Fax erfassen könnte, da auch über diese Medien eine Signalübertragung mittels elektronischer Impulse stattfindet, wird der Begriff des E-Commerce von den meisten als Geschäftsverkehr über das Internet definiert.[21] Die Grenzen zwischen Telefonie und dem Internet verschwimmen indes durch die Zunahme der Telefonie über das Internet (Voice-over-IP). So nahm im Jahr 2012 nach dem Bericht der Bundesnetzagentur die Nachfrage nach Sprachkommunikation über Voice-over-IP zu, während zugleich die Nachfrage nach den „klassischen“ analogen Telefonanschlüssen sank.[22] Eine Unterscheidung sollte hier somit nicht schematisch nach der Art der Datenvermittlung – die für den Benutzer ohnehin in den wenigsten Fällen transparent ist – geschehen, sondern vielmehr nach der Wahl des Mediums zur Kontaktaufnahme.

Gemeinhin wird der E-Commerce in mehrere Unterformen wie b2b[23], b2c[24] und b2a[25] unterteilt, die sich nach den jeweiligen Akteuren der geschäftlichen Beziehungen bestimmen. Teilweise werden darüber hinaus noch weitere Unterscheidungen wie die zwischen „echtem E-Commerce“ und

18 *Schwoerer*, Die elektronische Justiz, 22.
19 *Borges*, 30 f; ähnlich auch *Fink* in *Spindler*/*Schuster*, Allgemeines A Rn. 48.
20 *Schmidhuber*, 3.
21 *Weber*, 3.
22 *Bundesnetzagentur*, 72.
23 Business to business.
24 Business to consumer bzw. business to client.
25 Business to administration.

„unechtem E-Commerce“ vorgenommen[26].

2.2 E-Government

Der Begriff E-Government beschreibt grob umrissen die Nutzung von elektronischer Kommunikation zur Abwicklung von Regierungs- und Verwaltungshandeln (englisch *Government*).[27] Eine exakte, abschließende Definition des Begriffs existiert nicht, vielmehr hat sich der Begriff zu einem Sammelbegriff für Benutzung von Informations- und Kommunikationstechnologien durch die Verwaltung entwickelt.[28]

Nach der häufig zitierten[29] Speyrer Definition des E-Government beschreibt E-Government „die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien“[30]. Andere Definitionen wie die von *Wirtz* und *Piehler* ergänzen das Verständnis von E-Government um die Zielstellung der Effizienz- und Effektivitätssteigerung bei der Erfüllung öffentlicher Aufgaben.[31] Dieser Zusatz steigert jedoch kaum die Trennschärfe und den Erkenntnisgewinn aus der Definition, sondern fügt ihr im Gegenteil eine weitere Unschärfe hinzu. Denn während die Kriterien der Speyrer Definition objektivierbar sind, ist der intendierte Zweck des E-Government eine subjektive Frage, die sich ob der oft vielfältigen durch eine Umstellung von Arbeitsweisen erhofften Effekte kaum eindeutig beantworten lassen dürfte.

Auch für den Bereich E-Government werden zum Teil weitere Unterkategorien wie E-Government im engeren Sinne, E-Administration und E-Governance beschrieben.[32] Verbindendes Element der unterschiedlichen Definitionsansätze ist, dass Verwaltungs- und Regierungshandeln erfasst werden sollen. Bereits eine Abgrenzung zwischen E-Government und elektronischem Geschäftsverkehr kann jedoch schwerfallen. So wird zum Teil das E-Government als eine bloße Variante des E-Business betrachtet, die sich in der öffentlichen Verwaltung abspielt.[33] Dies begründet allerdings einerseits die Gefahr einer Vermengung der Begriffe, schließt andererseits aber auch andere, nicht mit wirtschaftlichem oder Verwaltungshandeln zusammenhängende Gestaltungsformen des E-

26 *Schmidhuber*, 3.
27 *Müller-Terpitz* in E-Government, 259 Rn. 3.
28 *Stollhof*, 27.
29 Eine Übersicht mit weiteren Nachweisen findet sich bei *Stollhof*, 22.
30 *Lucke, von/Reinermann*, 1.
31 *Wirtz/Piehler* in *Wirtz*, 8 f.
32 *Müller-Terpitz* in E-Government, 260 Rn. 4.
33 *Wirtz/Piehler* in *Wirtz*, 8.

Government wie z.B. E-Democracy-Anwendungen[34] aus.

Eine Unterscheidung vom Begriff des elektronischen Rechtsverkehrs im Sinne des Verfassers kann jedoch anhand der in der Rechtswissenschaft gebräuchlichen Trennlinie zwischen (materiellem) Verwaltungsrecht einerseits und Prozessrecht andererseits erfolgen. Elektronische Kommunikation auf dem Gebiet des Verwaltungsrechts ist damit – auch, wenn sie die Justizverwaltung betrifft – dem E-Government zuzuordnen, die Abwicklung judikativer Vorgänge mittels elektronischer Kommunikation dem elektronischen Rechtsverkehr.

2.3 E-Justice – elektronischer Rechtsverkehr im Sinne dieser Betrachtung

Mit der rein negativen Definition des elektronischen Rechtsverkehrs (E-Justice) als „weder dem elektronischen Geschäftsverkehr noch dem E-Government zuzurechnen“ ist allerdings noch nicht viel gewonnen.

Vielmehr muss auch eine positive Definition des elektronischen Rechtsverkehrs gefunden werden, um die Abgrenzung zu anderen Formen elektronischen Handelns erst verständlich zu machen und in ein in sich logisches System einzubetten. Zum Teil werden unter dem Begriff elektronischer Rechtsverkehr sehr unterschiedliche Sachverhalte zusammengefasst. So ist nach einer Ansicht unter dem elektronischen Rechtsverkehr jeder Austausch rechtsverbindlicher Informationen mittels elektronischer Medien zu verstehen.[35] Nach dieser Definition wäre der elektronische Rechtsverkehr gleichbedeutend mit dem elektronischen Geschäftsverkehr, wie er oben dargestellt wurde. Nach einer anderen Definition umfasst der elektronische Rechtsverkehr alle IT-Anwendungen der Justiz, die Außenbeziehungen betreffen[36]. Dies erscheint für die vorliegende Arbeit zielführender. Insbesondere ist diese Definition naheliegender, da auch der Gesetzgeber im Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten eine solche Lesart vorauszusetzen scheint, indem er mit diesem den Bereich der Kommunikation zwischen Justiz und Dritten regelt.

Der elektronische Rechtsverkehr umfasst damit die Kommunikation zwischen Gerichten und Bürgern, soweit diese die judikative Tätigkeit des Gerichts betrifft, sowie die dazu notwendige Binnenorganisation der Gerichte.

Mit dieser Definition ist klargestellt, dass elektronischer Rechtsverkehr die elektronische

34 Ein Beispiel hierfür ist das elektronische Portal des Petitionsausschusses des Deutschen Bundestages, erreichbar unter https://epetitionen.bundestag.de, zuletzt abgerufen am 18.12.2017.
35 *Bergfelder*, 71.
36 *Klink*, 11.

Kommunikation zwischen Gerichten und Verfahrensbeteiligten sowie Dritten beschreibt, nicht jedoch die Binnenkommunikation der Gerichte. Durch die Beschränkung auf judikative Tätigkeit wird eine Trennlinie zum E-Government im Bereich der Justizverwaltung gezogen. Eine hundertprozentig trennscharfe Abgrenzung zwischen E-Government und elektronischem Rechtsverkehr ist jedoch weder möglich noch sinnvoll, da zum Beispiel die organisatorischen Rahmenbedingungen, um den elektronischen Rechtsverkehr zu ermöglichen, in den Bereich der Justizverwaltung fallen. Um diese nicht völlig auszuklammern, wird mit dem Merkmal der notwendigen Binnenorganisation die Definition so erweitert, dass auch die technischen Rahmenbedingungen, die für die sichere elektronische Kommunikation zwischen Gerichten und Bürgern unerlässlich sind, beschrieben werden können.

Der elektronische Rechtsverkehr in diesem Sinne bedient sich verschiedener Technologien, um die bisherige analoge Kommunikation digital abzubilden. Die wichtigsten dieser Technologien werden im Folgenden kurz dargestellt:

2.3.1 Kryptografie

Aufgrund der noch zu erläuternden Eigenschaft von elektronischer Kommunikation, im Vergleich zu stofflicher Kommunikation oft einfacher und spurloser abhörbar zu sein, erscheinen insbesondere für sensible Bereiche erhöhte Sicherheitsvorkehrungen angebracht. Eine wichtige Rolle hierbei spielt die Kryptografie, d.h. die Wissenschaft der Verschlüsselung von Informationen. Mit Hilfe der Kryptografie ist es möglich, Informationen dergestalt verschlüsselt zu übertragen, dass Dritte, die in den Besitz dieser verschlüsselten Informationen gelangen, gleichwohl keine Kentnis der eigentlichen Kommunikationsinhalte erlangen. Damit ist die Kryptografie für viele Anwendungen des elektronischen Rechtsverkehrs notwendig, um die erforderliche Vertraulichkeit in der Kommunikation herzustellen. Die genauen Prinzipien der heutzutage verwendeten Verschlüsselungsverfahren zu verstehen, setzt umfangreiche Kenntnisse der Höheren Mathematik und Informatik und insbesondere der Kryptografie als Teilwissenschaft dieser voraus. Gleichwohl ist eine zumindest grobe Kenntnis der hierbei verwendeten Verfahren und Begriffe Voraussetzung, um notwendige Gestaltungsentscheidungen für den elektronischen Rechtsverkehr verstehen und einordnen zu können.

In der modernen Kryptografie kann man nach der Funktionsweise zwischen symmetrischen und

asymmetrischen Kryptosystemen unterscheiden, sowie nach dem Anwendungsfall zwischen Transportverschlüsselung und Inhaltsverschlüsselung. Die Technologien hierfür sind in unterschiedlicher Komplexität beinahe so alt wie die menschliche Kommunikation selbst. Zumindest bei Schriftkulturen ist davon auszugehen, dass diese kurz nach der Entwicklung der Schrift auch die Kryptografie entdeckt haben.[37] Da sowohl symmetrische als auch asymmetrische Verfahren für den elektronischen Rechtsverkehr Verwendung finden, werden diese im Folgenden kurz erläutert. Ein Verständnis der Unterscheidung und der verwendeten Terminologie (beispielsweise des Konzeptes von öffentlichen und privaten Schlüsseln) ist sowohl für das Verständnis der Verschlüsselungs- als auch der Signaturverfahren für den elektronischen Rechtsverkehr unabdingbar. Auch die danach erläuterten Konzepte der Transport- und Inhaltsverschlüsselung sind für das Verständnis des elektronischen Rechtsverkehrs, seiner Gestaltung und auch an Kritik, die an bestimmten Umsetzungsvarianten geäußert wurde, notwendig.

2.3.1.1 Symmetrische und asymmetrische Kryptosysteme

Früher wurden für die Verschlüsselung ausschließlich sogenannte symmetrische Kryptosysteme verwendet, d.h. Systeme, bei denen der gleiche Schlüssel für die Ver- wie für die Entschlüsselung der Botschaft benutzt wurde. Um eine verschlüsselte Kommunikation zu beginnen, war somit die Übertragung des Schlüssels notwendig. Wurde der Schlüssel auf dem Weg durch Dritte abgefangen oder erlangte dieser anderweitig Kenntnis des Schlüssels, konnten auch diese die Kommunikation entschlüsseln.

Dies änderte sich 1976 mit einer wissenschaftlichen Veröffentlichung zu einem asymmetrischen Verfahren durch *Diffie* und *Hellman.*[38] Asymmetrische Verfahren bauen auf dem mathematischen Prinzip auf, dass bestimmte Berechnungen unumkehrbar sind (sogenannte Einweg-Funktionen).[39] Auf diese Weise können Nachrichten mit einem Schlüssel – dem sogenannten öffentlichen Schlüssel oder *Public Key*[40] – so chiffriert werden, dass sie mit einem bestimmten *anderen*

37 *Bauer*, 4.
38 *Diffie/Hellman*, IEEE Transactions on Information Theory, IT-22 1976, 644; zu den Auswirkungen vgl. *Stinson*, 155 – wie mittlerweile bekannt wurde, hatte ein Angestellter des britischen Geheimdienstes GCHQ bereits 1970 ein solches Verfahren vorgeschlagen, dieses wurde jedoch nicht veröffentlicht und blieb zudem vom Konkretisierungsgrad hinter der Arbeit von *Diffie* und *Hellman* zurück, vgl. *Stinson*, 156.
39 *Stinson*, 156.
40 Aus dieser Nomenklatur ergibt sich auch die verbreitete Bezeichnung *Public-Key-Kryptografie* für derartige Kryptosysteme.

Schlüssel – dem geheimen Schlüssel oder *Private Key* – wieder dechiffriert werden können, ohne jedoch dabei aus dem Chiffrat oder dem *Public Key* auf den *private key* schließen zu können.

Da asymmetrische Verfahren zwar als sehr sicher, aber auch als langsam gelten, werden in der Praxis regelmäßig hybride Verfahren eingesetzt, die die Sicherheit asymmetrischer Kryptografie mit der Geschwindigkeit symmetrischer Kryptografie verbinden. Am weitesten verbreitet ist hierbei der Schlüsselaustausch nach *Diffie-Hellmann.* Hierbei wird ein für eine einzelne Nachricht generierter symmetrischer Schlüssel mit Hilfe des bekannten öffentlichen Schlüssels des Empfängers verschlüsselt und über den gleichen Kommunikationsweg übertragen wie die mit dem symmetrischen Schlüssel gesicherte Nachricht selbst. Durch dieses Vorgehen wird erreicht, dass mit dem langsamen asymmetrischen Verfahren nur eine relativ kleine Datenmenge – der symmetrische Schlüssel – verschlüsselt (und auf der Empfängerseite wieder entschlüsselt) werden muss. Durch die so abgesicherte Übertragung des symmetrischen Schlüssels kann sodann für die eigentliche Nachricht gefahrlos ein schnelleres symmetrisches Verfahren verwendet werden.

Aufgrund der Unbedenklichkeit der öffentlichen Schlüssel für die Sicherheit der Kommunikation können diese frei verteilt werden, zum Beispiel auf einem öffentlichen, über das Internet zugänglichen Rechner, einem sogenannten *Keyserver.* Von dort kann jeder potentielle Absender den öffentlichen Schlüssel seines Adressaten beziehen, um eine Nachricht an diesen zu verschlüsseln. Die Identität des Schlüsselinhabers und wird dabei entweder durch öffentliche Beglaubigungsstellen (sogenannte Certificate Authorities oder CAs) oder durch ein Netzwerk privater Beglaubigungen (ein sogenanntes *Web of Trust*, d.h. ein Vertrauensnetzwerk) sichergestellt.

2.3.1.2 Transportverschlüsselung

Die Übertragung einer Nachricht in elektronischer Form bringt immer die Gefahr mit sich, dass ein Dritter die Kommunikation belauscht und so den Inhalt der Nachricht in Erfahrung bringen kann. So ist ein Abhören von Telefonverbindungen zumindest bei analogen Telefonnetzen möglich, indem ein weiteres Telefon an die Telefonleitung angeklemmt wird.[41] Das Problem verschärft sich in Zeiten des Internets dadurch, dass die Datenpakete nicht zwingend den kürzesten Weg zwischen Sender und Empfänger nehmen. Dies kann durch die Gestaltung der Durchleitungsverträge zwischen den Internetprovidern zur Folge haben, dass Datenpakete große geografische Umwege nehmen, bevor sie den Empfänger erreichen.[42] Mit der Anzahl der Zwischenstationen und der

41 *Lindloff*, 96.
42 *Kleinz/Kuri*, Die Telekom und der NSA-Skandal.

Menge an beteiligter Netzinfrastruktur wie Switches und Routern erhöht sich auch die Menge der potentiellen Angriffspunkte, um eine Kommunikation „mitzuhören“. Das Internet muss deswegen mangels Kontrolle des Nutzers über die genutzte Infrastruktur als nicht-vertrauenswürdiges Netzwerk angesehen werden. Auch andere, oft aus Bequemlichkeit genutzte Netzwerke wie zum Beispiel öffentliche WLANs[43] fallen unter diese Kategorie und stellen eine Gefahr für die Vertraulichkeit von über sie abgewickelter Kommunikation dar.

Um dennoch eine vertrauliche Kommunikation über unsichere Netzwerke zu erlauben, bedarf es einer sogenannten Transportverschlüsselung. Die Besonderheit hieran ist, dass nicht (nur) die zu übertragende Nachricht selbst verschlüsselt, sondern ein insgesamt verschlüsselter Kanal zwischen Sender- und Empfängerseite aufgebaut wird. Sämtliche über diesen Kanal ausgetauschte Kommunikation wird automatisch vom Sender verschlüsselt und beim Empfänger wieder entschlüsselt. Dieses auch als Link-by-Link-Verschlüsselung bezeichnete Verfahren hat den Vorteil, dass es für den Nutzer transparent abläuft, da schlicht *alle* über die gesicherte Verbindung gehenden Informationen verschlüsselt werden.[44] Zudem kann sie auch nicht vollständig durch eine Verschlüsselung der Kommunikationsinhalte (dazu sogleich) ersetzt werden, da in den bei einer Kommunikation anfallenden Metadaten (beispielsweise Absender, Empfänger, Datum und Uhrzeit einer Nachricht, je nach verwendetem Übertragungsprotokoll zum Teil auch die zur Kommunikation benutzte Software, ihre Version sowie das verwendete Betriebssystem) ebenfalls schutzwürdige Informationen enthalten sein können. So kann je nach Sachlage bereits der bloße Umstand, dass man zu einer bestimmten Zeit mit einem bestimmten Empfänger kommuniziert hat, Rückschlüsse auf die Beziehung zwischen den Kommunikationsbeteiligten, deren Tagesabläufe und ihren Zugang zu Informationen zulassen.[45]

Das gebräuchlichste Verfahren für eine Transportverschlüsselung im Internet ist das Netzwerkprotokoll SSL[46] bzw. TLS[47]. SSL wurde ursprünglich von der Firma Netscape entwickelt, um eine Verschlüsselung zwischen und Authentifizierung von Rechnern im Internet zu ermöglichen.[48] Ein großer Vorteil des Protokolls ist seine Unabhängigkeit von der jeweiligen

43 Die Abkürzung WLAN bedeutet „Wireless Local Area Network“ und beschreibt ein örtlich begrenztes Computernetzwerk über Nahbereichsfunk.

44 *Schneier*, 257.

45 Ein plastisches Beispiel hierfür lieferte der Grünenpolitiker Malte Spitz für den Bereich des Mobilfunks, indem er sich die von der Telekom über ihn gespeicherten Vorratsdaten (die sich allesamt nur auf Metadaten der Kommunikationsvorgänge beschränken) aushändigen ließ und öffentlich verfügbar machte, vgl. *Biermann*, Zeit Online 3.9.2015, Datenschutz: Was Vorratsdaten über uns verraten, 1.

46 Secure Socket Layer.

47 Transport Layer Security.

48 *Eren/Detken*, 213; die Autoren sprechen jedoch etwas missverständlich davon, dass SSL für sichere Ende-zu-Ende-Kommunikation entwickelt wurde, obwohl nach der hier zugrunde gelegten Terminologie damit eine Transportverschlüsselung gemeint ist.

Anwendung, so dass andere Netzwerkprotokolle unproblematisch auf SSL aufsetzen und dieses zur Verschlüsselung ihrer Kommunikation verwenden können.[49] In seiner dritten Version (SSLv3) wurde SSL von dem Internet-Standardisierungsgremium IETF[50] zum Standard TLS erhoben.[51] Der ursprüngliche Standard TLS 1.0 wurde im Januar 1999 veröffentlicht[52], die aktuelle Version des Standards ist TLS 1.2 vom August 2006[53].

Die aus Nutzersicht wohl bedeutsamsten Anwendungen für SSL/TLS sind die Verschlüsselung zwischen Webservern und Browsern und die Verschlüsselung zwischen Mailservern und E-Mail-Programmen.

Zu beachten ist jedoch, dass die Transportverschlüsselung nicht notwendigerweise zwischen dem ursprünglichen Absender und dem letztendlichen Empfänger der Nachricht eingesetzt werden muss.

Wird eine Verbindung über mehrere Zwischenstationen (Kommunikationsknoten) geleitet, hängt die Sicherheit der Verschlüsselung davon ab, ob jeweils nur für den nächsten Kommunikationsknoten verschlüsselt wird oder für den letztendlichen Empfänger. Im Falle einer Verschlüsselung nur für den nächsten Kommunikationsknoten schützt diese nur vor einer Kenntnisnahme durch Dritte, nicht jedoch vor einer Kenntniserlangung vom Inhalt der Nachricht durch den empfangenden Knoten selbst.[54]

2.3.1.3 Inhaltsverschlüsselung

Für eine vor dem Abhören durch Dritte gesicherte elektronische Kommunikation ist jedoch eine bloße Transportverschlüsselung in der Regel nicht ausreichend. Beispielsweise ist nicht in jedem Fall erwünscht und möglich, dass beide Kommunikationspartner zur gleichen Zeit sende- und empfangsbereit sind, so dass ein transportverschlüsselter Kommunikationskanal zwischen ihnen ausgehandelt werden kann. Ein Beispiel hierfür ist die E-Mail, bei der ein oder mehrere E-Mail-Anbieter als Mittelsmänner die Nachrichten in Empfang nehmen, damit der Empfänger die Nachrichten später elektronisch abholen kann. Eine Transportverschlüsselung schützt hier nur die Übertragung vom Absender zum E-Mail-Anbieter und vom E-Mail-Anbieter zum Empfänger, verhindert jedoch nicht, dass die Nachricht in einer für den E-Mail-Anbieter lesbaren Form bei

49 *Eren/Detken*, 215.
50 Internet Engineering Taskforce.
51 *Eren/Detken*, 216.
52 Als RFC-2246, abrufbar unter http://datatracker.ietf.org/doc/rfc2246/, zuletzt abgerufen am 18.12.2017.
53 RFC-5246, abrufbar unter http://datatracker.ietf.org/doc/rfc5246/, zuletzt abgerufen am 18.12.2017.
54 *Schneier*, 257.

diesem vorliegt.

Demzufolge wird eine weitere Form der Verschlüsselung benötigt, die der Nachricht selbst anhaftet, selbst wenn diese sich nicht auf dem Transportweg befindet. Hier greift die Inhaltsverschlüsselung: Die Nachricht wird dabei mit einem Schlüssel gesichert, der nur dem beabsichtigten Empfänger bekannt ist. Da die Nachricht damit bei Nutzung eines sicheren Verfahrens und Geheimhaltung des Schlüssels nur vom endgültigen Empfänger entschlüsselt werden kann, spricht man hierbei auch von einer Ende-zu-Ende-Verschlüsselung.[55]

Ein bekanntes Beispiel für eine Ende-zu-Ende-Verschlüsselung ist das Programm *Pretty Good Privacy* (PGP) und der daraus abgeleitete offene Standard *OpenPGP,* der zu der kostenlosen und freien, mit PGP kompatiblen Software *GNU Privacy Guard*[56] *(GnuPG)* geführt hat. Sowohl PGP als auch GnuPG benutzen P*ublic-Key-Kryptografie* (s.o. unter 2.3.1.1) und erlauben neben dem Verschlüsseln von Nachrichten auch das elektronische Signieren. Obwohl sie einen quasi-Standard für die Inhaltsverschlüsselung und elektronische Signaturen in der Kommunikation über das Internet darstellen,[57] ist bisher die Teilnahme am elektronischen Rechtsverkehr mit ihnen nicht zulässig. Dieser Zustand ist vor allem dadurch begründet, dass keine Anzeige nach § 4 Abs. 3 SigG erfolgt ist, die für die Erteilung qualifizierter elektronischer Signaturen erforderlich wäre.[58]

Ein weiteres Verfahren ist S/MIME, welches auf den gleichen Prinzipien beruht und ebenfalls sowohl Verschlüsselung als auch elektronische Signaturen ermöglicht. S/MIME und PGP/GPG sind jedoch zueinander nicht kompatibel.[59]

2.3.2 Die qualifizierte elektronische Signatur (qeS)

Eine weitere Schlüsseltechnologie für den elektronischen Rechtsverkehr ist die Verwendung elektronischer Signaturen, die aufgrund gewisser Eigenschaften elektronischer Kommunikation notwendig sind, um eine mindestens gleichwertige Fälschungssicherheit von Erklärungen herzustellen, wie sie bisher bei analoger (papierbasierter) Kommunikation besteht. Auch hier ist eine Kenntnis zumindest der Grundkonzepte von elektronischen Signaturen und insbesondere der

55 *Schneier*, 257.
56 Das Programm wurde unter anderem vom Bundesamt für Sicherheit in der Informationstechnik gefördert und ist unter http://www.gnupg.org (zuletzt abgerufen 18.12.2017) kostenlos erhältlich.
57 So sind zum Beispiel PGP und GnuPG Teil des IT-Grundschutzkatalogs des Bundesamts für Sicherheit in der Informationstechnik, vgl. *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge M 5.63 – Einsatz von GnuPG oder PGP.
58 Vgl. zu diesem Erfordernis Abschnitt 2.3.2.
59 *Lindloff*, 42 m.w.N.

qualifizierten elektronischen Signatur notwendig, um bestimmte Eigenschaften des elektronischen Rechtsverkehrs nachvollziehen zu können und eine Bewertung der Sicherheit der verwendeten Systeme zu erlauben. Auch war die qualifizierte elektronische Signatur eine ganz wesentliche Technologie für den elektronischen Rechtsverkehr vor Erlass des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten. Ein Verständnis der Unterschiede zwischen der früheren rechtlichen Regelung des elektronischen Rechtsverkehrs und der Umsetzung durch das ERV-Gesetz erfordert somit ein Verständnis von Sinn, Funktionsweise und rechtlichen Rahmenbedingungen der qualifizierten elektronischen Signatur.

Die Eigenschaften asymmetrischer kryptografischer Verfahren[60] eröffnen neben dem Senden verschlüsselter Botschaften als weiteren Anwendungsbereich elektronische Signaturen. Hierbei wird eine Prüfsumme aus der zu signierenden Nachricht – das sogenannte *Hash* – gebildet und diese mit dem privaten Schlüssel des Urhebers verschlüsselt.[61] Ein Dritter kann mit dem öffentlichen Schlüssel des Urhebers diese Prüfsumme wieder entschlüsseln und bei einer Übereinstimmung der entschlüsselten Prüfsumme mit der von ihm selbst gebildeten Prüfsumme des Dokuments sicher sein, dass die Nachricht seit dem Signieren nicht verändert wurde.[62]

Der Grundgedanke einer elektronischen Signatur ist die Sicherstellung von Authentizität und Integrität einer elektronischen Nachricht. Ein Bedürfnis hierzu besteht durch Eigenschaften von elektronischen Mitteilungen, spurlos veränderbar zu sein.[63]

Der Gesetzgeber hat mit dem Gesetz zur Digitalen Signatur (Signaturgesetz – SigG) von 1997[64], das 2001 durch das neue Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften[65] ersetzt wurde, die Grundlagen geschaffen, um die gesetzlich geforderte Schriftform in bestimmten Fällen durch eine elektronische Form ersetzen zu können.[66] Signaturgesetz und Signaturverordnung bereiteten dabei jedoch nur den Boden hierfür, da sie lediglich elektronische Signaturen und die Anforderungen an diese beschrieben.[67] Die Ableitung materiellrechtlicher Wirkungen an die Benutzung von elektronischen Signaturen blieb anderen Gesetzen wie dem BGB (dort insbesondere § 126a BGB, der die elektronische Form regelt), der Zivilprozessordnung (§ 130a und § 130b) und dem VwVfG (§ 3a) vorbehalten. Ab dem 1. Juli 2016

60 Vgl. hierzu oben unter 2.3.1.1.
61 *Bösing*, 22.
62 *Bösing*, 23.
63 Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste, BT-Drs. 13/7385, 26; zur genannten Eigenschaft elektronischer Kommuikation siehe auch unten unter Abschnitt 4.2)
64 BGBl. I 1870, 1872 ff.
65 BGBl. I 876.
66 *Roßnagel* in Telemediendienste, Einl SigG Rn. 39.
67 *Roßnagel* in Telemediendienste, Einl SigG Rn. 46.

gilt zudem die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung – eIDAS-VO), durch die die Signaturrichtlinie als bisherige Grundlage für das Signaturgesetz ersetzt wurde.[68] Durch die unmittelbare Anwendbarkeit der eIDAS-Verordnung sind auch die Vorschriften des Signaturgesetzes – soweit sie in den Anwendungsbereich der eIDAS-Verordnung fielen und dieser widersprochen haben – unanwendbar geworden. Zur Angleichung des deutschen Rechts an die unmittelbar geltende Verordnung hat der deutsche Gesetzgeber das Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 18. Juli 2016 (eIDAS-Durchführungsgesetz – eIDAS-DG)[69] erlassen. Kernbestandteil dieses Artikelgesetzes war das Vertrauensdienstegesetz (VDG). Nach Art. 12 eIDAS-DG trat gleichzeitig mit Inkrafttreten des eIDAS-DG sowohl das Signaturgesetz als auch die Signaturverordnung außer Kraft.[70]

Durch das Signaturgesetz hatte der Gesetzgeber die rechtlichen Rahmenbedingungen geschaffen, nach denen elektronische Signaturen erteilt werden sollen (§ 1 Abs. 1 SigG). Diese genossen – mit Ausnahme der einfachen elektronischen Signatur – im Gegenzug ein erhöhtes Vertrauen, an das weitere Rechtsfolgen geknüpft werden konnten. Hierbei gab es drei Stufen: Die (einfache) elektronische Signatur nach § 2 Nr. 1 SigG, die fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG und die qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG. Eine einfache elektronische Signatur war hierbei jedes nach den obengenannten Prinzipien die Integrität einer elektronischen Nachricht sicherstellendes Verfahren sowie einfache, mit der Nachricht nicht verknüpfte elektronische Authentifizierungsdaten. Unter letztere fiel z.B. auch der einfache Scan einer Unterschrift unter einer Textdatei oder sogar ein lediglich eingetippter Name.[71] Die fortgeschrittene elektronische Signatur musste zwingend logisch mit den signierten Daten verknüpft sein, so dass eine Veränderung im Nachhinein erkannt werden konnte.[72] Hinzu kamen noch die Anforderungen der ausschließlichen Zuordnung des Schlüssels zum Schlüsselinhaber, der Identifizierungsmöglichkeit des Schlüsselinhabers sowie die alleinige Kontrollmöglichkeit des Schlüsselinhabers über die Sicherungsmittel.[73]

68 Abl. L 257/73.
69 BGBl. I 2745.
70 Zum Werdegang der eIDAS-Verordnung und der rechtlichen Einordnung im Bezug auf den elektronischen Rechtsverkehr, vgl. unten unter 3.1.8.
71 *Roßnagel* in Telemediendienste, § 2 SigG Rn. 11.
72 *Roßnagel* in Telemediendienste, § 2 SigG Rn. 27.
73 *Roßnagel* in Telemediendienste, § 2 SigG Rn. 14.

Die höchste Stufe bildete schließlich die qualifizierte elektronische Signatur. Diese vereinigte die Merkmale der fortgeschrittenen elektronischen Signatur in sich und muss zusätzlich auf einem zum Zeitpunkt der Erstellung gültigen qualifizierten Zertifikat beruhen sowie mit einer sicheren Signaturerstellungseinheit erzeugt werden. Über das Merkmal des qualifizierten Zertifikats war sichergestellt, dass der Zertifikatsersteller erhöhte infrastrukturelle Vorgaben und Sorgfaltsanforderungen erfüllten. Eine Genehmigungspflicht für das Betreiben eines Zertifizierungsdienstes, der qualifizierte Zertifikate erteilen durfte, war indes seit der Änderung des Signaturgesetzes von 2001 gemäß § 4 Abs. 1 SigG nicht mehr erforderlich. Allerdings musste so ein Dienst nach § 4 Abs. 3 der zuständigen Behörde, mithin der Bundesnetzagentur, angezeigt werden.

Schließlich gab es noch die freiwillige Möglichkeit für Zertifizierungsdiensteanbieter, sich gemäß § 15 SigG von der Bundesnetzagentur akkreditieren zu lassen. Dies hatte zur Folge, dass die Echtheit und Zuordnung zum Signaturinhaber der Signaturen, die von einem solchen Anbieter erstellt worden sind, widerleglich vermutet wurden.[74] Weitere unmittelbare Rechtsfolgen waren hieran nicht geknüpft, jedoch konnten sich durch Anforderungen wie die der dauerhaften Überprüfbarkeit mittelbare Verweise auf Signaturen von akkreditierten Zertifizierungsdiensteanbieter ergeben, da zumindest für diese eine Überprüfungsmöglichkeit von 30 Jahren nach Ablauf der Gültigkeitsdauer gemäß § 4 Abs. 2 SigV vorgeschrieben war.[75] Zwingend erschien dies freilich nicht, da es auch nicht akkreditierten Zertifizierungsdiensteanbietern freistand, diese Anforderung zu erfüllen.

Auch im Rahmen der eIDAS-Verordnung wurde die durch das Signaturgesetz verwendete Terminologie hinsichtlich der Signaturstufen weitgehend beibehalten. Nach der eIDAS-Verordnung sind die Signaturstufen die elektronische Signatur nach Art. 3 Nr. 10 eIDAS-VO, die fortgeschrittene elektronische Signatur Art. 3 Nr. 11 eIDAS-VO und die qualifizierte elektronische Signatur nach Art. 3 Nr. 12 eIDAS-VO. Durch die eIDAS-VO wurden allerdings die Anforderungen an die Signaturen modifiziert. Für die fortgeschrittene elektronische Signatur nach Art. 3 Nr. 11, Art. 26 eIDAS-VO wird im Gegensatz zur Rechtslage nach dem Signaturgesetz nicht mehr verlangt, dass die Signatur ausschließlich dem Unterzeichner zugeordnet ist, sondern nur noch „eindeutig“, Art. 26 lit. a) eIDAS-VO.[76] Überdies ist nicht mehr erforderlich, dass der Benutzer einer fortgeschrittenen elektronischen Signatur die zur Erstellung verwendeten Mittel uner alleiniger Kontrolle halten kann, wie Signaturrichtlinie und Signaturgesetz dies noch verlangten, sondern nunmehr lediglich, dass der Ersteller die Signatur „unter Verwendung elektronischer

74 *Roßnagel* in Telemediendienste, § 15 SigG Rn. 67 f.
75 *Roßnagel* in Telemediendienste, § 15 SigG Rn. 71.
76 Vgl. hierzu auch die Darstellung bei *Roßnagel*, Vertrauensdienste, 22.

Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann“[77].[78] Für qualifizierte elektronische Signaturen nach Art. 3 Nr. 12 eIDAS-VO gelten außer den soeben für die fortgeschrittene elektronische Signatur genannten Einschränkungen gegenüber der alten Rechtslage nach dem Signaturgesetz keine Besonderheiten. Auch weiterhin ist für diese erforderlich, dass sie von einer qualifizierten Signaturerstellungseinheit erstellt wurden und auf einem qualifizierten Zertifikat für elektronische Signaturen, dessen Anforderungen Art. 28 eIDAS-VO bestimmt, beruhen.

Die qualifizierte elektronische Signatur im Sinne der eIDAS-Verordnung ist bisher die einzige Möglichkeit, Dokumente formwahrend elektronisch bei Gericht einzureichen. Vorschriften hierzu finden sich beispielsweise in § 130a ZPO, § 110a OWiG, § 41a StPO, § 55a VwGO, § 46c ArbGG, § 14 Abs. 2 FamFG, § 52a FGO sowie § 65a SGG. Voraussetzung hierfür ist jedoch stets die für die Bearbeitung geeignete Form sowie die Eröffnung des elektronischen Rechtsverkehrs durch Rechtsverordnung der Bundesregierung oder der Landesregierungen. Dies hat zu einer erheblichen Zersplitterung des elektronischen Rechtsverkehrs geführt, da die Länder in unterschiedlicher Weise von dieser Möglichkeit Gebrauch gemacht haben. So ist in Bayern, Mecklenburg-Vorpommern, dem Saarland und Thüringen ein über Registersachen hinausgehender elektronischer Rechtsverkehr nicht verfügbar. Das andere Extrem bilden Länder wie Berlin, Bremen, Hessen und Sachsen, die in fast allen Verfahrensarten den elektronischen Rechtsverkehr umfassend zugelassen haben. Die übrigen Länder haben den elektronischen Rechtsverkehr zum Teil eröffnet, wobei entweder eine Beschränkung auf bestimmte Verfahrensarten oder aber auf bestimmte Gerichte besteht. Eine Übersicht zum Stand in den einzelnen Bundesländern findet sich auf dem Online-Justizportal des Bundes und der Länder.[79] Auch die Art, in der die Länder den elektronischen Rechtsverkehr zugelassen haben, unterscheidet sich. In den meisten Fällen kommt das unten unter 2.3.3 vorgestellte elektronische Gerichts- und Verwaltungspostfach (EGVP) zum Einsatz, zum Teil wird aber auch die Einreichung über E-Mail oder über eine spezielle Website ermöglicht.

Diese Zersplitterung (die zum Teil auch als „Flickenteppich“ bezeichnet wird[80]) war einer der Gründe, die zum Erlass des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten geführt haben. Die qualifizierte elektronische Signatur findet sich auch in diesem Gesetz wieder, tritt jedoch hier alternativ neben weitere Einreichungsarten, die dann keine qualifizierte elektronische Signatur mehr benötigen sollen, weil sie von sich aus als hinreichend sicher gelten (sichere Übermittlungswege). Regelungen hierzu finden sich in § 130a ZPO n.F., § 46c ArbGG n.F.,

77 Art. 26 lit. c eIDAS-VO.
78 *Roßnagel*, Vertrauensdienste, 22; *Sosna*, CR 2014, 825, 830.
79 http://www.justiz.de, abgerufen am 17.1.2017.
80 *Limperg*, AnwBl 2013, 98.

§ 65a SGG n.F., § 55a VWGO n.F. sowie § 52a FGO n.F.[81]

2.3.3 Das elektronische Gerichts- und Verwaltungspostfach (EGVP)

Das elektronische Gerichts- und Verwaltungspostfach (EGVP) ist ein System für die elektronische Kommunikation mit Gerichten und Behörden, das unter anderem die Grundlage für das besondere elektronische Anwaltspostfach bildet.[82] Die Bezeichnung EGVP kann sich dabei sowohl auf das Gesamtsystem als auch auf die gleichnamige Software beziehen. Zur Klarstellung wird deshalb im Folgenden bei der Software immer die Bezeichnung EGVP-Client[83] benutzt, um eine Abgrenzung zum EGVP-Gesamtsystem zu ermöglichen. Dies ist wichtig, weil das System EGVP grundsätzlich unabhängig vom Bestand der für die Nutzer konzipierten Client-Programme ist.

Das EGVP ist das Produkt einer Kooperation des Bundesverwaltungsgerichts, des Bundesfinanzhofes, des Bundesamts für Sicherheit in der Informationstechnik sowie des Oberverwaltungsgerichts Münster zusammen mit den Ländern Bremen und Hessen[84]. Seine erste Anwendung fand es beim elektronischen Rechtsverkehr mit dem Bundesverwaltungsgericht und dem Bundesfinanzhof, der zum 1. Dezember 2004 eröffnet wurde.[85] Die Programmierung der hierfür notwendigen Software *EGVP Classic* übernahm die 1999 gegründete *bremen online Services GmbH & Co. KG*, deren Komplementär die im Eigentum der Stadt Bremen stehende *Governikus Bremen GmbH* (vormals *bremen online services Beteiligungsgesellschaft mbH*) ist. Auch als Kommanditistin ist die Freie Hansestadt Bremen zu 55,1% beteiligt.[86] Mittlerweile hat das Unternehmen mit seiner Vertriebstochter fusioniert und firmiert jetzt unter der Bezeichnung *Governikus GmbH & Co. KG*, benannt nach einem Softwareprodukt des Unternehmens.[87]

Zur Nutzung des EGVP wird bisher eine Software namens EGVP-Classic-Client (zum Teil auch als EGVP-Bürger-Client, verkürzt auch oft als EGVP Classic bezeichnet) angeboten. Hierbei handelt es sich um eine in der portablen Programmiersprache Java programmierte Anwendung, die unter den

81 Inkrafttreten ab 1. Januar 2018, vgl. Art. 26 Abs. 1 Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten.
82 Vgl. hierzu Abschnitt 2.3.4 unten.
83 Die Bezeichnung Client beschreibt im Allgemeinen eine Software, die mit einem Server kommuniziert. Dabei stellt der Server Dienste bereit, die der Client nutzt.
84 http://www.egvp.de/beh_allgemeine_info/index.php, abgerufen am 18.12.2017.
85 Pressemitteilung des Bundesverwaltungsgerichts Nr. 68/2004 vom 3.12.2004, abrufbar unter http://www.bverwg.de/presse/pressemitteilungen/pressemitteilung.php?jahr=2004&nr=68, abgerufen am 18.12.2017.
86 https://www.governikus.de/unternehmen, abgerufen am 18.12.2017.
87 https://www.governikus.de/unternehmen/historie/, abgerufen am 18.12.2017.

Betriebssystemen Windows und Linux lauffähig ist, nicht jedoch unter MacOS.[88] Sie benutzt zur Kommunikation den Protokollstandard OSCI,[89] der von der Koordinierungsstelle IT-Standards fortentwickelt wird.[90] Die Software soll eine sichere und vertrauliche elektronische Kommunikation zwischen Bürgern – wozu auch professionelle Einreicher wie etwa Rechtsanwälte, Notare und Steuerberater gezählt werden – und Gerichten sowie der Verwaltung ermöglichen. Hierzu benutzt sie zum einen eine Ende-zu-Ende-Verschlüsselung, die sicherstellen soll, dass nur Absender und intendierter Empfänger Kenntnis vom Inhalt einer Nachricht erlangen können. Zum anderen unterstützt der EGVP-Classic-Client qualifizierte elektronische Signaturen mittels eines Hardwarezertifikats (Smartcard).[91] Hierdurch soll die Authentizität und Integrität der Nachrichten sichergestellt werden. Bis zum Inkrafttreten der neuen Formvorschriften durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten ist das Benutzen einer qualifizierten elektronischen Signatur nach Signaturgesetz zudem zur Wahrung der Schriftform notwendig, so dass prozessual wirksame Erklärungen auch nur mit einer solchen abgegeben werden können.

Ein weiteres Merkmal des EGVP-Classic-Clients ist die Adressbuchfunktion. Bei der ersten Benutzung des EGVP-Classic-Clients wird dem Nutzer angeboten, ein EGVP-Postfach anzulegen. Wird dies verneint, ist zwar die Versendung von EGVP-Nachrichten möglich, nicht aber der Empfang, was Beispielsweise auch den Empfang von Eingangsbestätigungen betrifft.[92] Eine direkte Eingabe der Adresse ist jedoch in EGVP Classic – anders als Beispielsweise bei E-Mail – nicht vorgesehen. Vielmehr nutzt die Anwendung einen zentralen Verzeichnisdienst, in dem sämtliche Nutzer aufgeführt sind. Der oder die Adressaten müssen in der verwendeten EGVP-Anwendung aus diesem Verzeichnis, das nach verschiedenen Kriterien durchsucht werden kann, ausgewählt werden. Ein Vorteil dieses Systems ist, dass ein Vertippen bei Eingabe der Adresse nicht mehr möglich ist, jedoch besteht die Gefahr einer versehentlichen Falschauswahl aus dem Verzeichnis. Der Verzeichnisdienst basiert auf dem System SAFE,[93] das eine Aufteilung in mehrere unterschiedliche Adressbereiche mit jeweils eigener Infrastruktur (sogenannter *Trusted Domains* oder *Trust-Domains*) ermöglicht.[94] Auf diese Weise ist zum Beispiel eine Aufteilung der Betriebskosten für

88 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 8 f.
89 Online Services Computer Interface.
90 Auftraggeber für die Koordinierungsstelle ist für alle Standardisierungsfragen der IT-Planungsrat, der auf Grund von Art. 91c GG sowie des Staatsvertrags über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern gegründet wurde und die Koordinierung der IT zwischen Bund und Ländern zur Aufgabe hat.
91 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 12.
92 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 36.
93 Secure Access to Federated E-Government/E-Justice.
94 *Arbeitsgruppe „IT-Standards in der Justiz“ der Bund-Länder-Kommission*, SAFE-Übersicht, 2.

eine Postfachinfrastuktur möglich, da der Verzeichnisdienst und die Postfächer verschiedener *Trusted Domains* nicht notwendigerweise von den gleichen natürlichen oder juristischen Personen betrieben werden müssen. Eine Erreichbarkeit aus jeder anderen *Trusted Domain* ist dennoch gewährleistet, da das SAFE-System für eine Vermittlung der Verzeichnisanfragen und Nachrichten an die jeweils zuständige *Trusted Domain* sorgt.[95] Ein Beispiel für diese Trennung besteht bereits mit der *Trusted Domain Notare*, die von der Bundesnotarkammer betrieben wird. Eine weitere Aufspaltung wird sich ergeben, sobald die *Trusted Domain Rechtsanwälte* in Verwaltung durch die Bundesrechtsanwaltskammer den Betrieb aufnimmt.

Eine weitere Software zur Nutzung des EGVP-Systems stellt EGVP-Enterprise dar. Dieses Programm ist für die Nutzung in (größeren) Unternehmen konzipiert, da es im Gegensatz zum EGVP-Classic-Client keine Einzelplatzanwendung ist, sondern eine Serversoftware ohne eigene Benutzeroberfläche, die im Firmennetzwerk installiert werden kann und Drittprogrammen den Zugriff auf EGVP-Postfächer ermöglicht.[96]

Aufgrund der durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vorgesehenen Einrichtung eines besonderen elektronischen Anwaltspostfaches (beA) durch die Bundesrechtsanwaltskammer wurde die Entwicklung des EGVP-Classic-Clients zum 31.12.2016 eingestellt. Entgegen früherer Ankündigungen wurde damit jedoch nicht auch die Downloadmöglichkeit des EGVP-Clients entfernt. Ein Download des EGVP-Clients soll stattdessen übergangsweise noch bis zum 1.1.2018 möglich bleiben.[97]

2.3.4 Das besondere elektronische Anwaltspostfach (beA)

Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten wurde auch der neue § 31a mit der amtlichen Überschrift „Besonderes elektronisches Anwaltspostfach“ in die Bundesrechtsanwaltsordnung eingefügt. Eine Erwägung hierfür war, durch die Bestimmung eines einheitlichen Systems mit einem hohen Sicherheitsstandard auf die qualifizierte elektronische Signatur nach dem Signaturgesetz verzichten zu können, die zum Teil als Verbreitungshindernis für den elektronischen Rechtsverkehr gesehen wurde.[98] Der neue § 31a BRAO ermächtigt und beauftragt die Bundesrechtsanwaltskammer, nach Überprüfung der Zulassung und Identifizierung

95 *Arbeitsgruppe „IT-Standards in der Justiz“ der Bund-Länder-Kommission*, SAFE-Übersicht, 2.
96 *egvp.de*, Weiterentwicklung EGVP, 4 f.
97 *egvp.de*, Änderungen zum 1.1.2016, Mitteilung auf der Startseite.
98 Vgl. hierzu Abschnitt 3.1.7 zum Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten.

jedem zugelassenen Rechtsanwalt ein besonderes elektronisches Anwaltspostfach (beA) einzurichten. Die Gesetzesbegründung spricht hier etwas unscharf von einem „Verzeichnisdienst besonderer elektronischer Anwaltspostfächer“.[99] Tatsächlich geht es jedoch auch um die Voraussetzungen hierfür, nämlich die Erstellung der besonderen elektronischen Anwaltspostfächer, die dem insofern eindeutigen Wortlaut des § 31a BRAO n.F. nach durch die Bundesrechtsanwaltskammer für jeden Rechtsanwalt eingerichtet werden sollen. Die etwas verwirrende Formulierung, dass die Postfächer „in dem Gesamtverzeichnis nach § 31“ eingerichtet werden sollen, muss wohl dahingehend interpretiert werden, dass diese Postfächer ebenfalls in das Gesamtverzeichnis aufgenommen werden sollen. Ein solcher Hinweis wäre jedoch nach der ebenfalls im Gesetzesentwurf enthaltenen Ergänzung des § 31 Abs. 3 S. 1 BRAO n.F., nach dem die Adresse des besonderen elektronischen Anwaltspostfachs in das Gesamtverzeichnis aufzunehmen ist, ohnehin entbehrlich. Dementsprechend ist die Bundesrechtsanwaltskammer mit dem nicht geringen Unterfangen befasst, eine komplette Kommunikationsinfrastruktur für Rechtsanwälte zu konzipieren und zu errichten.[100]

Das besondere elektronische Anwaltspostfach baut technisch auf dem OSCI-Standard auf, auf dem auch das elektronische Gerichts- und Verwaltungspostfach basiert.[101] Zur Authentifizierung wird das SAFE-System benutzt, innerhalb dessen eine eigene *Trusted Domain*, die ebenfalls durch die Bundesrechtsanwaltskammer einzurichten und zu führen ist, bereitgestellt wird.[102] Zudem soll nicht mehr der wegen seiner umständlichen Bedienung und unattraktiven Erscheinung kritisierte EGVP-Classic-Client genutzt werden. Stattdessen soll es die Möglichkeit geben, über anwaltliche Fachsoftware über Schnittstellen das besondere elektronische Anwaltspostfach zu nutzen.[103] Für Nutzer, die keine Fachsoftware benutzen, soll ein webbasierter Zugang geschaffen werden, der – ähnlich den von E-Mail-Anbietern bekannten Webmail-Angeboten – den Zugang zum beA auch ohne weitere Software allein durch die Nutzung eines Webbrowsers ermöglichen soll. Nicht klar ist bisher, ob das beA auch die oben vorgestellte qualifizierte elektronische Signatur zur Integritäts- und Identitätssicherung der versandten Nachrichten einsetzen wird. Der Präsident der Bundesrechtsanwaltskammer hat in einem Artikel in den BRAK-Mitteilungen vom Juni 2014 erklärt, das beA werde „eine unbemerkte Manipulation der Inhalte der Nachrichten durch die Verwendung qualifizierter elektronischer Signaturen beim Versand und ähnlichem“ ausschließen.[104] Zudem ist nach § 31a Abs. 2 BRAO auch durch die Bundesrechtsanwaltskammer sicherzustellen,

99 BT-Drs. 17/12634, 38.
100 *Fiebig*, BRAK-Magazin 02/2014, 4, 5.
101 *Rechtsanwaltskammer Sachsen*, FAQ zu ERV, Frage 6.
102 BT-Drs. 17/12634, 38.
103 *Fiebig*, BRAK-Magazin 02/2014, 4, 4.
104 *Filges*, BRAK-Mitteilungen 2014, 113, 113.

dass der Zugang zum beA nur mit zwei voneinander unabhängigen Sicherungsmitteln erfolgen können soll. Wenngleich die Kriterien einer Zwei-Faktor-Authentifizierung (Besitz und Wissen) auch durch Signaturkarten für die qualifizierte elektronische Signatur grundsätzlich erfüllt werden würden, da diese zur Authentifizierung Besitz an der Chipkarte und Wissen um die PIN voraussetzen, ist noch unklar, ob die BRAK diese als Sicherungsmittel nutzen wird oder auf andere Sicherungsmittel wie beispielsweise den neuen Personalausweis (nPA) zurückgreifen wird.[105]

Da der technische Unterbau des beA der auch vom EGVP genutzte OSCI-Standard ist, wäre zu erwarten, dass eine Benutzung des beA auch mit dem EGVP-Classic-Client möglich ist. Die für die Weiterentwicklung und Pflege von EGVP Classic zuständige Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (BLK) hat jedoch beschlossen, mit dem Start des besonderen elektronischen Anwaltspostfachs den EGVP-Classic-Client nicht mehr weiterzuentwickeln und -verteilen.[106] Ob das bedeutet, dass eine Nutzung auch vorhandener EGVP-Classic-Installationen ab diesem Zeitpunkt nicht mehr möglich ist, ist noch nicht eindeutig zu beantworten.

2.3.5 De-Mail

Ein weiteres Verfahren für eine sichere Kommunikationsinfrastruktur ist die sogenannte De-Mail. Diese ist ein Versuch, die Sicherheitsnachteile der normalen E-Mail durch spezielle Vorkehrungen wie eine zwingende Transportverschlüsselung und eine verbindliche Identifizierung der Teilnehmer auszugleichen. Die De-Mail geht zurück auf ein Gesetzgebungsvorhaben von 2009, das (damals noch unter der Bezeichnung Bürgerportale) eine sichere Kommunikationsinfrastruktur für Bürger schaffen sollte.[107] Am 28. April 2011 wurde das De-Mail-Gesetz erlassen,[108] dass die rechtlichen Grundlagen der De-Mail festlegt. So müssen sich Anbieter nach § 17 Abs. 1 De-Mail-G von der zuständigen Behörde, dem Bundesamt für Sicherheit in der Informationstechnik (§ 2 De-Mail-G), akkreditieren lassen, um einen De-Mail-Dienst anbieten zu dürfen. Derzeit sind vier Anbieter für De-Mail akkreditiert, eine stets aktuelle Liste findet sich beim Bundesamt für Sicherheit in der Informationstechnik.[109]

Dem Konzept De-Mail wurde von verschiedenen Seiten Kritik entgegengebracht. Zum Teil wurde

105 *Fiebig*, BRAK-Magazin 02/2014, 4.
106 *egvp.de*, Änderungen zum 1.1.2016, Mitteilung auf der Startseite.
107 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 729; vgl. hierzu auch Abschnitt 3.1.5 unten.
108 Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften, BGBl I 666.
109 *Bundesamt für Sicherheit in der Informationstechnik*, Akkreditierte De-Mail Diensteanbieter.

kritisiert, dass damit eine parallele, zur normalen E-Mail inkompatible Infrastruktur geschaffen werde, was mit einer Verwechslungsgefahr zwischen normaler E-Mail und De-Mail beim Bürger einhergehen könne.[110] Auch sei die versprochene Sicherheit mangels verpflichtender Ende-zu-Ende-Verschlüsselung nicht gegeben, da sich wie bei der normalen E-Mail jeder Nutzer nach wie vor selbst um eine entsprechende Sicherung seiner versandten Inhalte kümmern müsse.[111] Hierzu ist jedoch anzumerken, dass zumindest die Verwaltung der privaten Schlüssel für ein entsprechendes Verschlüsselungsverfahren zwingend unter der individuellen Verwaltung der Nutzer bleiben müsste, da Nutzer nur so sicher gehen könnten, dass nur sie Zugriff zu ihren privaten Schlüsseln und somit auf die für diese verschlüsselten Klartextdaten hätten. Der kritisierte Mangel an einer sicheren Verschlüsselung kann insofern nur so interpretiert werden, dass keine Infrastruktur für eine Verschlüsselung durch die Anbieter zur Verfügung gestellt wird. Dennoch hat der Gesetzgeber sich im Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten entschieden, die De-Mail als eine zulässige Einreichungsart für Gerichte festzulegen (§ 130 a Abs. 4 ZPO n.F.[112]). Die Folge hiervon ist, dass die bisher notwendige qualifizierte elektronische Signatur nicht mehr zur Formwahrung erforderlich sein soll, wenn die Nachricht über ein De-Mail-Postfach versandt wurde, an dem der Absender zum Versendezeitpunkt sicher angemeldet gewesen ist.

2.3.6 E-Postbrief

Als Konkurrenzprodukt zur De-Mail hat die Deutsche Post AG ein Produkt namens E-Postbrief entwickelt. Dieser verwendet ähnlich wie die De-Mail eine Transportverschlüsselung (jedoch keine Ende-zu-Ende-Verschlüsselung) und eine sichere Authentifizierung. Ein Alleinstellungsmerkmal des E-Postbriefs ist, dass unter der Bezeichnung E-Postbrief mit klassischer Zustellung auch ein Ausdruck, Kuvertierung und Versand auf dem Postweg der beim Anbieter elektronisch eingegangenen Nachricht angeboten wird.[113] Hierfür ist es natürlich zwingend notwendig, dass die Nachricht beim Anbieter in unverschlüsselter Form vorliegt, was zumindest für die Dienstleistung E-Postbrief mit klassischer Zustellung eine Ende-zu-Ende-Verschlüsselung faktisch ausschließt.

Anfangs hatte die Deutsche Post AG angekündigt, eine Zertifizierung als De-Mail-Anbieter zu beantragen, war später jedoch von diesem Ziel wieder abgerückt. Die Begründung hierfür lautete, dass das für die Authentifizierung der Nutzer des E-Postbriefs verwendete Verfahren Postident nicht

110 *Welte*, 4.
111 *Welte*, 2.
112 Vgl. hierzu unten Abschnitt 3.1.7.
113 *Hoffmann/Luch/Schulz/Tallich u. a.*, 1.

mit den Vorschriften des De-Mail-Gesetzes zur Identitätsfeststellung vereinbar sei. Die Deutsche Post AG erklärte, auf dieses Verfahren jedoch nicht verzichten zu wollen, da es ein Kernstück der Sicherheit des E-Postbriefs darstellte. Zwischenzeitlich hat der Betreiber jedoch angekündigt, nunmehr doch eine Akkreditierung als De-Mail-Anbieter anzustreben.[114] Dies mag dem Umstand geschuldet sein, dass die De-Mail mit der Aufnahme ins Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten nunmehr nach § 130a ZPO n.F.[115] als offizielles Verfahren im elektronischen Rechtsverkehr gilt.

3 Die Geschichte des elektronischen Rechtsverkehrs

Um den elektronischen Rechtsverkehr in seiner jetzigen Gestalt zu verstehen, ist es zunächst erforderlich, seinen Werdegang zu kennen. Viele der Argumente sowohl von Befürwortern als auch Kritikern des elektronischen Rechtsverkehrs stützen sich auf die bisher mit dem elektronischen Rechtsverkehr gemachten Erfahrungen, die eng verknüpft sind mit der Entwicklung, die dieser genommen hat. Ein Verständnis und die Gewichtung der vorgebrachten Argumente setzen deshalb voraus, dass die wesentlichen Entwicklungsschritte hin zum elektronischen Rechtsverkehrs bekannt sind. Der folgende Abschnitt bietet deshalb einen Überblick über den Werdegang des elektronischen Rechtsverkehrs anhand einer chronologischen Darstellung, die ein Verständnis der Bedingungen des elektronischen Rechtsverkehrs vermitteln soll. Hierbei soll zunächst unter 3.1 auf die Entwicklung der rechtlichen und technischen Voraussetzungen eingegangen werden, die den elektronischen Rechtsverkehr erst ermöglicht haben. Unter Kapitel 3.2 wird mit einer Betrachtung des Datenschutzrechts ein Rechtsgebiet betrachtet, das zwar keine direkte Voraussetzung für den elektronischen Rechtsverkehr darstellt, jedoch einen rechtlichen Rahmen für bestimmte Gefahren technischer Entwicklungen schafft, in den sich auch der elektronischen Rechtsverkehr einfügen muss.

114 *Bünder*, FAZ.NET vom 11.12.2013, S.1.
115 vgl. hierzu unten unter Abschnitt 3.1.7.

3.1 Entwicklung der Voraussetzungen für den elektronischen Rechtsverkehr

3.1.1 Signaturgesetz und Signaturverordnung

In seiner ursprünglichen Fassung wurde das Signaturgesetz am 22. Juli 1997 als Teil des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz – IuKDG) veröffentlicht.[116] Ziel des Gesetzes war es, zur Ermöglichung eines elektronischen Rechts- und Geschäftsverkehrs die Rechtssicherheit in offenen Netzen zu erhöhen.[117] Das Signaturgesetz war weltweit das erste seiner Art.[118] In seiner ursprünglichen Fassung sah es dabei keine technischen Detailregelungen vor, sondern lediglich ein Gerüst, innerhalb dessen verschiedene technische Verfahren in Wettbewerb zueinander treten können.[119] Ein Bedarf für das Signaturgesetz wurde darin gesehen, dass digitale Signaturverfahren bis dato mangels einer Sicherheitsinfrastruktur mit zentralen Beglaubigungsinstanzen für die Zuordnung von Signaturschlüsseln zu natürlichen Personen nur innerhalb geschlossener Benutzergruppen eingesetzt würden.[120]

Kernbegriff des SigG 1997 war die digitale Signatur gemäß § 2 Abs. 1, die als „Siegel zu digitalen Daten“ mit einem privaten Signaturschlüssel erzeugt und mittels eines öffentlichen Signaturschlüssels den Inhaber des Signaturschlüssels und die Integrität der Daten bestätigen konnte. Der öffentliche Signaturschlüssel sollte dabei über ein Zertifikat im Sinne des § 2 Abs. 3 SigG 1997 verfügen, d.h. über eine „digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person“, die ihrerseits mit einer digitalen Signatur versehen sein musste. Diese Zertifikate sollten durch Zertifizierungsstellen im Sinne von § 2 Abs. 2 SigG 1997 erteilt werden, die gemäß § 4 Abs. 1 SigG 1997 für ihre Tätigkeit über eine Genehmigung von der nach § 3 SigG 1997 zuständigen Behörde sowie ein Zertifikat, das „zum Signieren von Zertifikaten eingesetzt“ werden kann, verfügen mussten. Der Gesetzeswortlaut war an dieser Stelle etwas missverständlich, da Zertifikate mit privaten Signaturschlüsseln und nicht mit Zertifikaten signiert werden. Ein Zertifikat war nach § 2 Abs. 3 SigG 1997 lediglich als eine digitale Bescheinigung der Zugehörigkeit eines Signaturschlüssels zu dessen Inhaber oder über Eigenschaften des Inhabers legaldefiniert. Gemeint dürfte mit dieser insoweit verkürzten

116 BGBl. I 1870, 1872 ff.
117 *Roßnagel*, DuD 1997, 75 ff., 76.
118 *Bergfelder*, 150.
119 Gesetzesbegründung Signaturgesetz 2001, BT-Drs. 13/7385, 17.
120 Gesetzesbegründung Signaturgesetz 2001, BT-Drs. 13/7385, 25.

Formulierung wohl gewesen sein, dass eine Zertifizierungsstelle nach § 3 SigG 1997 eines Zertifikats für jenen privaten Signaturschlüssel bedarf, mit dem sie beabsichtigt, selbst Zertifikate zu signieren.

Obwohl das Gesetz im amtlichen Titel als „Gesetz zur digitalen Signatur“ bezeichnet wurde, regelte es nicht die konkrete Ausgestaltung oder die dinglichen Rechtsfolgen digitaler Signaturen, sondern setzte den Rahmen für eine öffentliche Beglaubigungsinfrastruktur. Dies ist historisch zu begründen: Während anfangs noch ein zivilrechtlicher Ansatz verfolgt wurde, nach dem das Signaturgesetz die Rechtsfolgen digitaler Signaturen regeln sollte, wurde auf Grund von Kritik aus Forschung und Praxis hieran jedoch ein öffentlich-rechtlicher Ansatz gewählt.[121]

Gesetzgebungstechnisch sah das Signaturgesetz in dieser ursprünglichen Fassung vor, dass der Betrieb einer Zertifizierungsstelle genehmigungspflichtig sein sollte. Die Erteilung von Genehmigungen oblag nach § 3 SigG 1997 der Behörde nach § 66 TGK 1996, mithin nach der zu dieser Zeit gültigen Fassung des TKG der Regulierungsbehörde für Telekommunikation und Post (RegTP). Ihr oblag nach § 4 Abs. 5 SigG 1997 auch das Erteilen von Zertifikaten für jene Signaturschlüssel, mit denen Zertifizierungsstellen ihrerseits erteilte Zertifikate signierten. Damit war die RegTP als sogenannte Wurzel-Zertifizierungsstelle[122] gleichsam oberste Instanz in der Zertifikatskette. Dies führte zum Teil zu Kritik, da somit nur die Zertifikate einer Stelle kompromittiert werden müssten, um die ganze Zertifizierungsinsfrastruktur zu Fall zu bringen.[123] Obgleich der Bundesrat in seiner Stellungnahme zum Gesetzesentwurf des Signaturgesetzes von 1997 die fehlende Haftung der Zertifizierungsstellen gegenüber Dritten kritisierte[124], wurde eine solche Regelung in das Signaturgesetz in seiner ursprünglichen Fassung nicht aufgenommen. Auch konkrete Rechtswirkungen der elektronischen Signaturen wurden im Signaturgesetz selbst nicht geregelt. Stattdessen bestimmte das Gesetz als Rechtsfolge der Genehmigung von Zertifizierungsstellen, dass für von diesen ausgestellte Zertifikate eine Sicherheitsvermutung als Beweiserleichterung gelten sollte.[125] Der Gesetzgeber ging davon aus, dass die faktische Sicherheit von Signaturen, die von staatlich geprüften Stellen ausgegeben werden, von den Gerichten im Wege der freien Beweiswürdigung berücksichtigt werden würden.[126] Das Signaturgesetz trat in seiner ersten Fassung am 1. August 1997 in Kraft.

In § 16 SigG 1997 war der Erlass einer Rechtsverordnung durch die Bundesregierung vorgesehen,

121 *Roßnagel*, RDV 1998, 5 ff., 10.
122 Teilweise wird hierfür auch der englische Begriff *root-CA* (für root certificate authority) verwendet.
123 Vgl. *Roßnagel*, DuD 1997, 75 ff., 78.
124 *Roßnagel* in Telemediendienste, Einl. SigG Rn. 43.
125 *Roßnagel* in Telemediendienste, Einl. SigG Rn. 47.
126 Gesetzesbegründung Signaturgesetz 2001, BT-Drs. 13/7385, 26.

in der Details zur technischen und organisatorischen Ausgestaltung digitaler Signaturen geregelt werden sollten. Eine solche Verordnung wurde im gleichen Jahr in Form der Signaturverordnung[127] erlassen und trat am 1. November 1997 in Kraft. Diese konkretisierte die Vorgaben des Signaturgesetzes, indem sie die Verfahren der Beantragung und Erteilung von Signaturschlüsseln und Zertifikaten näher beschrieb und abstrakte Anforderungen hinsichtlich der Ausgestaltung und Sicherheit der erforderlichen technischen Komponenten aufstellte. Für die konkrete technische Umsetzung wie beispielsweise die Wahl von geeigneten Algorithmen zur digitalen Signatur sollte ebenfalls die RegTP zuständig sein, die gemäß § 17 Abs. 2 SigV 1997 für die digitale Signatur als geeignet anzusehende Algorithmen im Bundesanzeiger bekanntgeben sowie diese mindestens jährlich auf ihre fortgesetzte Eignung überprüfen sollte. Hierbei sollte sie sich nach den Angaben des Bundesamtes für Sicherheit in der Informationstechnik richten.

Der Gesetzgeber entschloss sich zudem, aufgrund der bis dahin noch nicht vollständig vorhandenen Voraussetzungen für elektronische Signaturen, das Gesetz nach spätestens zwei Jahren zu evaluieren.[128] Der Evaluierungsbericht der Bundesregierung wurde am 18. Juni 1999 veröffentlicht[129]. Er kam zu der Einschätzung, dass keine wesentlichen Änderungen am Signaturgesetz notwendig seien.[130] Dennoch wurden in dem Bericht als Reaktion auf Kritik aus Literatur und Praxis Änderungen zu einzelnen Aspekten des Signaturgesetzes erwogen. So wurde auf die Kritik aus der Rechtswissenschaft, die enge Definition von Zertifizierungsstellen in § 2 Abs. 2 SigG 1997 ermögliche keine Auslagerung einzelner Funktionen von Zertifizierungsstellen an andere Dienstleister, eingegangen und eine erneute Prüfung in Aussicht gestellt.[131] Auch wurde erwogen, dem Wunsch von Berufskammern entsprechend diesen eine Sperrung von Zertifikaten zu ermöglichen, wenn diese Zertifikate falsche Angaben über die Zulassung durch die jeweilige Kammer enthielten. Schließlich wurde im Hinblick auf die erwartete EU-Signaturrichtlinie davon ausgegangen, dass die Aufnahme von einfachen Signaturen und einer Haftungsregelung in ein neues Signaturgesetz erforderlich werden würde.[132]

3.1.2 EU-Signaturrichtlinie und Änderung des Signaturgesetzes

Ein weiterer Anlass, der eine Überarbeitung des Signaturgesetzes nötig machte, war die

127 BGBl. I 2498.
128 *Thomale*, 33 m.w.N.
129 BT-Drs. 14/1191.
130 *Thomale*, 33.
131 BT-Drs. 14/1191, 18.
132 BT-Drs. 14/1191, 20.

Verabschiedung der europäischen „Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“[133] (im Folgenden: RLeS).[134] Die Richtlinie war Ergebnis von Harmonisierungsbestrebungen bezüglich der nach Erlass des deutschen Signaturgesetzes begonnenen Regulierungsversuche zahlreicher EG-Mitgliedsstaaten im Hinblick auf digitale Signaturen.[135] Ziel der Richtlinie war die Beseitigung von Hindernissen für den Gemeinsamen Markt und die Förderung der Entwicklung elektronischer Märkte.[136]

Der Überarbeitungsbedarf liegt vor allem in der Systematik der Richtlinie begründet, die sich von der des Signaturgesetzes in seiner ursprünglichen Form deutlich unterschied: Anders als das Signaturgesetz in der Fassung von 1997 bestimmte die Signaturrichtlinie mehrere Klassen von Signaturen, an die unterschiedliche Rechtsfolgen geknüpft sein sollten. Die geringsten Anforderungen stellt danach die elektronische Signatur im Sinne von Artikel 2 Nr. 1 RLeS, die zugleich Oberbegriff für die folgenden, an engere Voraussetzungen geknüpften Signaturformen war. Für die elektronische Signatur reichten elektronische Daten aus, die mit anderen elektronischen Daten verknüpft oder diesen beigefügt sind und die zur Authentifizierung dienen. Aufgrund dieser weiten Voraussetzungen genügen hier auch die bereits oben unter 2.3.2 genannte eingescannte Unterschrift oder sogar eine bloße textuelle Repräsentation des Namens[137]. Dementsprechend knüpfte die Richtline außer dem Diskriminierungsverbot aus Art. 5 Abs. 2 RLeS auch keine Rechtsfolgen an die elektronische Signatur nach Art. 2 Nr. 1 RLeS.[138] Für die fortgeschrittene elektronische Signatur enthielt Art. 2 Nr. 2 RLeS als zusätzliche Voraussetzungen die ausschließliche Zuordnung zum Unterzeichner, die Identifizierungsmöglichkeit des Unterzeichners durch die Signatur, die Erstellung mit Mitteln unter der alleinigen Kontrolle des Unterzeichners sowie die Verknüpfung mit den signierten Daten in der Art, dass eine nachträgliche Veränderung der Daten erkennbar wird. Trotz der Bemühungen des Verordnungsgebers, die Richtlinie technikneutral zu gestalten, ließ sich nach dem aktuellen Stand der Technik unter den Wortlaut kein anderes Verfahren subsumieren als die Verschlüsselung eines Hash-Wertes der zu signierenden Daten mit einem dem Empfänger bekannten Schlüssel.[139]

Die anforderungsintensivste und sicherste Form der elektronischen Signatur war schließlich gemäß Art. 5 Abs. 1 RLeS die fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wurde. Für diese wählte

133 Richtlinie 1999/93/EG.
134 *Roßnagel* in Telemediendienste, Einl. SigG Rn. 77.
135 *Roßnagel* in Telemediendienste, Einl. SigG Rn. 48.
136 *Roßnagel* in Telemediendienste, Einl. SigG Rn. 48.
137 *Geis*, MMR 2000, 667 ff., 669.
138 *Roßnagel*, K&R 2000, 314 ff., 318.
139 So im Ergebnis auch *Roßnagel*, K&R 2000, 314 ff., 317.

die Richtlinie – im Bruch mit der vorher in Art. 1 aufgenommenen Systematik – jedoch keine gesonderte Bezeichnung. In der rechtswissenschaftlichen Diskussion wurde diese daher beispielsweise als „fortgeschrittene Signatur ‚plus'"[140] oder als „fortgeschrittene elektronische Signatur besonderer Qualität"[141] bezeichnet. Das Signaturgesetz in seiner Fassung von 2001 wählte hier in Anlehnung an die Terminologie der Richtlinie für die Zertifikate, die in „Zertifikate" und „qualifizierte Zertifikate" aufgeteilt sind, den Begriff „qualifizierte elektronische Signatur".[142]

Am 16. Mai 2001 wurde die Neufassung des Signaturgesetzes[143] erlassen. Diese folgte eng den Vorgaben der Signaturrichtlinie. Die qualifizierte elektronische Signatur, die an die Stelle der digitalen Signatur nach § 2 Abs. 1 Nr. 1 SigG 1997 trat, entsprach dabei der in Art. 5 Abs. 1 RLeS definierten Qualifikation der fortgeschrittenen elektronischen Signatur. Mit der einfachen elektronischen Signatur und der fortgeschrittenen elektronischen Signatur fanden sich auch die anderen Qualitätsstufen von elektronischen Signaturen aus der RLeS in § 2 SigG 2001. Dabei wurde entsprechend der Struktur der Richtlinie ein Stufenverhältnis geschaffen, in dem die größte Gruppe – elektronische Signaturen – den Oberbegriff und fortgeschrittene sowie qualifizierte elektronische Signaturen Qualifikationen darstellen. Da die einzige Voraussetzung für die elektronische Signatur nach § 2 Nr. 1 SigG die (bloße) Beifügung zu elektronischen Daten oder die Verknüpfung mit selbigen war, reicht hierfür wie auch nach der Signaturrichtlinie vorgesehen schon eine einfache textuelle Darstellung eines Namens oder der bloße Scan einer Unterschrift,[144] die jedoch keinerlei Aussagekraft über die Integrität oder Authentizität der so behandelten Daten traf. Die nächste Stufe, die fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG, enthielt mit den Anforderungen der ausschließlichen Zuordnung zum Signaturschlüsselinhaber, der Identifizierung des Inhabers, der Erzeugung mit Mitteln, die der Inhaber unter seiner alleinigen Kontrolle halten kann und der logischen Verknüpfung mit den zu signierenden Daten bereits alle technischen Voraussetzungen an eine rechtsverbindliche elektronische Signatur. Trotzdem hatte der Gesetzgeber auch der fortgeschrittenen elektronischen Signatur keine Rechtsverbindlichkeit zugestanden, diese war der qualifizierten elektronischen Signatur vorbehalten. Diese höchste Anforderungsstufe an die Signatur selbst war in § 2 Nr. 3 SigG geregelt. Die qualifizierte elektronische Signatur musste zusätzlich zu den Voraussetzungen einer fortgeschrittenen elektronischen Signatur auch noch auf einem qualifizierten Zertifikat gemäß § 2 Nr. 7 SigG beruhen und mit einer sicheren Signaturerstellungseinheit erstellt worden sein. Ein qualifiziertes Zertifikat war ein Zertifikat im

140 *Tettenborn*, CR 2000, 683 ff., 685.
141 *Geis*, MMR 2000, 667 ff., 668.
142 BR-Drs. 496/00, 25.
143 BGBl. I 876.
144 *Roßnagel* in Telemediendienste, § 2 SigG Rn. 11.

Sinne von § 2 Nr. 6 SigG, das die in § 7 SigG genannten Angaben enthielt, d.h. insbesondere mit einer qualifizierten elektronischen Signatur „unterzeichnet“ war, und von einem Anbieter stammte, der die Voraussetzungen nach §§ 4 – 14 bzw. § 23 SigG erfüllte. Hierzu zählte neben der für den Betrieb einer Zertifizierungsstelle erforderlichen Zuverlässigkeit und Fachkunde insbesondere eine Anzeige nach § 4 Abs. 3 SigG an die zuständige Behörde.

Als weitere wesentliche Änderung des Signaturgesetzes von 1997 war durch die Signaturrichtlinie die Einführung einer Haftungsregelung notwendig geworden. Im Signaturgesetz von 1997 war der Gesetzgeber davon ausgegangen, dass die im geltenden Recht bestehenden Haftungsmechanismen auch für Haftungsfälle bezüglich des Signaturgesetzes ausreichend seien.[145] Diese Auffassung wurde in der Literatur stark kritisiert, da sich insbesondere die bei einem Versagen des Zertifizierungsdiensteanbieters[146] häufigen Dreipersonenverhältnisse nur unzureichend mit dem bestehenden Instrumentarium lösen ließen.[147] Diskutierte Konstruktionen wie die Betrachtung des Signaturgesetzes als Schutzgesetz im Sinne von § 823 Abs. 2 BGB, die Lösung von Dreipersonenverhältnissen über die Prinzipien des Vertrags mit Schutzwirkung zu Gunsten Dritter oder über das Produkthaftungsgesetz verursachten große Rechtsunsicherheit.[148] Die Signaturrichtlinie sah demgegenüber in Art. 6 eine Gefährdungshaftung der Zertifizierungsdiensteanbieter mit Beweislastumkehr zu deren Lasten vor.[149] Eine Exkulpationsmöglichkeit für den Fall, dass der Anbieter ein nicht fahrlässiges Handeln nachweisen konnte, war ebenfalls vorgesehen, Art. 6 Abs. 1 und Abs. 2 RLeS. Von diesem Haftungsrisiko sollten Anbieter sich befreien können, indem Sie bei der Ausstellung von Zertifikaten von vornherein deren Anwendungsbereich begrenzten, Art. 6 Abs. 3 RLeS, oder nach Art. 6 Abs. 4 RLeS eine maximale Transaktionssumme für Geschäfte mit einem so zertifizierten Signaturschlüssel festlegen konnten. Der deutsche Gesetzgeber hatte dies in § 11 Signaturgesetz 2001 umgesetzt, aber durch eine Verpflichtung der Zertifizierungsanbieter zum Treffen einer Deckungsvorsorge in Höhe von mindestens 250.000 € pro Schaden abgesichert (§ 12 SigG 2001).

Schließlich war auch die bisher erforderliche Genehmigung von Zertifizierungsdiensteanbietern einer freiwilligen Akkreditierung gewichen.[150] Der Betrieb eines Zertifizierungsdiensteanbieters, der befugt war, Zertifikate für die qualifizierte elektronische Signatur auszustellen, bedurfte nicht einmal der Akkreditierung sondern lediglich der Erfüllung der gesetzlichen Voraussetzungen und

145 Entwurf IuKDG, BT-Drs. 13/7385, 27.
146 Seit dem Signaturgesetz von 2001 ersetzt dieser Begriff den im Signaturgesetz 1997 verwendeten Begriff der Zertifizierungsstelle.
147 *Geis*, MMR 2000, 667 ff., 671.
148 *Leier* in IuKDG-Komm, 6 SigG Vorb. Rn. 80.
149 *Schumacher*, CR 1999, 473 ff., 474.
150 *Thomale*, 51.

einer Anzeige an die zuständige Behörde. Dies entsprach der in Art. 3 Abs. 1 RLeS vorgesehenen Genehmigungsfreiheit für den Betrieb von Zertifizierungsstellen. Von der Möglichkeit in Art. 3 Abs. 2 RLeS, optional freiwillige Akkreditierungssysteme mit engeren Voraussetzungen einzuführen, hatte der deutsche Gesetzgeber mit § 15 SigG Gebrauch gemacht. Nach diesem konnten Zertifizierungsdiensteanbieter eine freiwillige Akkreditierung beantragen, die sie berechtigte, Zertifikate für eine vierte Sicherheitsstufe von elektronischen Signaturen, die „qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung“ (§ 15 Abs. 1 S. 4 SigG), zu erteilen. Voraussetzung hierfür war neben der Erfüllung der allgemeinen Voraussetzungen für den Betrieb eines Zertifizierungsdiensteanbieters eine externe Prüfung des Sicherheitskonzepts nach § 4 Abs. 2 S. 4 SigG durch eine Prüf- und Bestätigungsstelle im Sinne des § 18 SigG.

Eine Regelung, die sich in der Signaturrichtlinie nicht fand, jedoch im Signaturgesetz Bestand hatte, war jene zu elektronischen Zeitstempeln. Während diese in § 2 Abs. 4 SigG 1997 noch an relativ prominenter Stelle platziert war, war sie – systematisch allerdings gleich aufgehängt – durch die Neuregelung des Signaturgesetzes 2001 in § 2 S. 1 Nr. 14 SigG gewandert und ihre rechtlichen Anforderungen wurden konkretisiert.

Zur Konkretisierung der Vorgaben des Signaturgesetzes wurde gemäß § 24 SigG am 16. November 2001 zudem eine Neufassung der Signaturverordnung[151] erlassen. In dieser wurde den Änderungen durch das Signaturgesetz 2001 und die Ergebnissen der Evaluierung des Informations- und Kommunikationsdienstegesetzes Rechnung getragen, im Übrigen blieben Inhalt und Struktur der Signaturverordnung jedoch erhalten.[152]

3.1.3 E-Commerce-Richtlinie und Formanpassungsgesetz 2001

Da das Signaturgesetz auch in seiner neuen Fassung nur den Rahmen für elektronische Signaturen festlegte, ohne an diese jedoch materiellrechtliche oder prozessuale Folgen zu knüpfen, bedurfte es neben dem Signaturgesetz weiterer rechtlicher Regelungen, um den elektronischen Rechtsverkehr zu eröffnen. Auch die Signaturrichtlinie enthielt in Erwägungsgrund 17 die Aussage, dass das nationale Vertragsrecht bezogen auf den Abschluss und die Erfüllung von Verträgen durch die Richtlinie nicht verändert werden und auch außervertragliche Formvorschriften für Unterschriften nicht harmonisiert werden sollten. Dies stieß insbesondere in Verbindung mit Art. 5 Abs. 1 RLeS

151 BGBl. I, 3074.
152 *Roßnagel* in Telemediendienste, Einl. SigV Rn. 14.

vielfach auf Unverständnis, da hierin zum Teil ein Widerspruch gesehen wurde.[153] Nach herrschender Meinung ist dies dahingehend aufzulösen, dass die Signaturrichtlinie nur die Gleichstellung von (bestimmten) elektronischen Signaturen mit handschriftlichen Unterschriften regelt, aber offen lässt, ob Rechtsgeschäfte nach nationalem Recht überhaupt auf elektronischem Wege geschlossen werden können.[154]

Eine Harmonisierung der materiellen Wirkungen elektronischer Signaturen erfolgte jedoch durch die Europäische Richtlinie vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtline über den elektronischen Geschäftsverkehr“[155], im Folgenden RLeG). Diese auch als E-Commerce-Richtlinie bezeichnete Richtlinie sah in Art. 9 Abs. 1 vor, dass Mitgliedsstaaten Vertragsschlüsse auf elektronischem Wege ermöglichen sollten. In Erwägungsgrund 18 der Richtline über den elektronischen Geschäftsverkehr wurde klargestellt, dass der in der Richtlinie zentrale Begriff der „Dienste der Informationsgesellschaft“ nicht nur auf Online-Vertragsschlüsse beschränke, sondern auch auf von den Empfängern nicht vergütete Dienste, etwa Informations- oder Kommunikationsdienste, soweit es sich bei der Nutzung jener um eine wirtschaftliche Tätigkeit handelte. Darüber hinaus wurde in Erwägungsgrund 34 klargestellt, dass die Mitgliedsstaaten solche Vorschriften zu ändern hätten, die ein Hindernis für die Verwendung elektronischer Dienste darstellen könnten. Dies solle sich ausdrücklich auch auf (nationalstaatliche) Formerfordernisse beziehen und dem Zweck dienen, die Verwendung elektronisch geschlossener Verträge zu ermöglichen. Schließlich wird in Erwägungsgrund 52 auch angeregt, dass die Mitgliedsstaaten prüfen, ob ein Bedürfnis für die Bereitstellung elektronischer Zugänge zu den Gerichten bestünde. Die Richtlinie beschränkte sich jedoch in Art. 1 Abs. 5 d) dahingehend, dass sie keine Anwendung auf die Vertretung eines Mandanten und die Verteidigung seiner Interessen vor Gericht finden sollte. In Art. 9 Abs. 1 RLeG findet sich schließlich die Vorschrift, nach der die Mitgliedstaaten elektronische Vertragsschlüsse ermöglichen und dafür sorgen sollen, dass der Anerkennung elektronisch geschlossener Verträge keine Hindernisse im Wege stehen. Diese Vorschrift erforderte damit das, was die Signaturrichtlinie gerade vermied – eine Pflicht der Mitgliedsstaaten, ihre nationalen Formvorschriften dahingehend zu ändern, dass auch elektronisch geschlossene Verträge diese erfüllten. Nicht von der Norm verlangt wurde jedoch, dass jede beliebige Art des elektronischen Vertragsschlusses gleichermaßen anerkannt würde, was die Einbindung der elektronischen Signatur im Sinne der Signaturrichtlinie in die Formvorschriften ermöglichte. Mithin

153 Siehe z.B. *Redeker*, CR 2000, 455 ff., 458, *Roßnagel*, K&R 2000, 314 ff., 320.
154 *Borges*, 635 m.w.N.
155 RL 2000/31/EG.

stellt sich das Verhältnis zwischen Signaturrichtlinie und E-Commerce-Richtline so dar, dass die E-Commerce-Richtlinie die Mitgliedsstaaten verpflichtet, elektronische Vertragsschlüsse zu ermöglichen, den Mitgliedsstaaten aber freistellte, ob und unter welchen Voraussetzungen sie die elektronische Signatur als notwendige Form des Vertragsschlusses vorsehen.

Am 13. Juli 2001 wurde das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr[156] (Formanpassungsgesetz – FormAnpG) erlassen. Es diente sowohl zur Umsetzung der Richtline über den elektronischen Geschäftsverkehr als auch zur Anpassung des deutschen Privatrechts an den modernen Rechtsverkehr.[157] Dabei geht die Vorgeschichte des Formanpassungsgesetzes weiter zurück als bis zur Richtline über den elektronischen Geschäftsverkehr, da bereits mit dem Entwurf des Signaturgesetzes von 1996 von der Bundesregierung beschlossen worden war, einen Gesetzentwurf zur Anpassung von Formvorschriften an den elektronischen Rechtsverkehr zu erstellen.[158] Dementsprechend nennt die Begründung des Gesetzesentwurfs auch nicht die Richtline über den elektronischen Geschäftsverkehr als treibende Kraft hinter dem Gesetzgebungsvorhaben, sondern stellt lediglich fest, der Gesetzesentwurf setze die Verpflichtung von EU-Mitgliedsstaaten, elektronische Vertragsschlüsse qua Gesetzes zu ermöglichen, „bereits weitgehend um“.[159]

Dem Gesetzentwurf des Formanpassungsgesetzes war eine lebhafte Diskussion zwischen Bundestag und Bundesrat über die Inhalte des Gesetzes vorangegangen, welche in einem Einberufen des Vermittlungsausschusses gipfelte. Die finale Gesetzesfassung wurde schließlich am 13. Juli 2001 erlassen und trat mit Wirkung zum 1. August 2001 in Kraft. Das Gesetz definierte erstmals neben der bisherigen Schriftform in § 126a BGB eine elektronische Form, die mit einer qualifizierten elektronischen Signatur im Sinne des Signaturgesetzes versehen sein und in bestimmten Fällen die Schriftform ersetzen können sollte. Hiermit war die Grundlage für eine Nutzung der qualifizierten elektronischen Signatur im elektronischen Geschäftsverkehr gelegt. Zudem wurde in § 126b BGB eine Textform definiert. Für diese war jedoch lediglich eine Wiedergabe des Namens in Form einer „Nachbildung der Namensunterschrift“ oder anderweitig gefordert, was letztendlich den Voraussetzungen an eine einfache elektronische Signatur entspricht, die nach dem Signaturgesetz keine Privilegierung erfährt.

Eine deutliche Änderung brachte das Formanpassungsgesetz auch im Bereich des Prozessrechts mit

156 BGBl. I 1542.
157 *Borges*, 117.
158 *Roßnagel*, NJW 2001, 1817, 1818 m.w.N.
159 BT-Drs. 14/4987, 11.

sich. Es erlaubte durch die Änderung diverser Fachgerichtsordnungen die Einreichung von Schriftsätzen auch als elektronische Dokumente. Betroffen hiervon waren unter anderem das Zivilprozessrecht, die Verwaltungsgerichtsbarkeit, die Sozialgerichtsbarkeit und die Arbeitsgerichtsbarkeit.

Mit dem neuen § 130a ZPO hielt die qualifizierte elektronische Signatur auch Einzug in das Zivilprozessrecht. Die praktische Relevanz war hier jedoch zunächst gering.[160] Zudem stellten sich im Zusammenhang mit dem Gesetzeswortlaut einige rechtliche Probleme. So war zunächst ungeklärt, ob das Erfordernis einer qualifizierten elektronischen Signatur in § 130a Abs. 1 S. 2 ZPO zwingend ist, da es sich um eine Sollvorschrift handelte („Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen."). Während Teile der Literatur hierin eine bloße Ordnungsvorschrift sahen, betrachteten andere diese Vorschrift als zwingend.[161] Der Wortlaut der Gesetzesbegründung ist insoweit nicht sehr ergiebig, da er zwar einerseits § 130a Abs. 1 S. 2 ZPO als Ordnungsvorschrift bezeichnet, andererseits jedoch feststellt, dass Satz zwei „verlangt […], dass der Absender das elektronische Dokument mit seiner qualifizierten elektronischen Signatur versieht".[162] In ihrer Erwiderung auf die Stellungnahme des Bundesrates zu § 130a Abs. 1 S. 2 ZPO erklärte die Bundesregierung jedoch, eine zwingende Nutzung der elektronischen Form würde zu Wertungswidersprüchen mit der bisherigen Rechtsprechung zur Formwirksamkeit von anderen Medien wie Telegramm, Fernschreiben und Telefax führen.[163] Zum Teil wird allerdings auch darauf hingewiesen, es in der Praxis letztlich nicht auf den Wortlaut von § 130a Abs. 1 S. 2 ZPO ankomme, sondern auf die nach § 130a Abs. 2 S.1 ZPO vorgesehene Rechtsverordnung, die Formanforderungen an Schriftsätze festlegt.[164]

Das Formanpassungsgesetz erkannte zudem an, dass eine Eröffnung des elektronischen Rechtsverkehrs den Aufbau einer Infrastruktur erforderte, der Zeit in Anspruch nehmen würde, und sah deswegen in § 130a Abs. 2 ZPO vor, dass Bund und Länder mittels Rechtsverordnung den Zeitpunkt und die Art der Einreichung elektronischer Schriftsätze – auch nur für einzelne Verfahrensarten oder Schriftstücke – bestimmen können sollten.[165] Ungeachtet der Unsicherheiten, die mit den zivilprozessualen Änderungen durch das Formanpassungsgesetz einhergingen, legte dieses Gesetz damit den Grundstein für den – zunächst rein optionalen – elektronischen Rechtsverkehr mit den Gerichten.

160 *Stadler* in *Musielak*/*Voit*, § 130a Rn. 1.
161 *Fritsche* in MüKo-ZPO Band 1, § 130a Rn. 4.
162 BT-Drs. 14/4987, 24.
163 BT-Drs. 14/4987, 43 f.
164 *Schmieszek* in *Scherf*/*Schmieszek*/*Viefhues*, B II § 130a ZPO Rn. 14.
165 BT-Drs. 14/4987, 24.

3.1.4 Zustellungsreformgesetz 2001 und Justizkommunikationsgesetz 2005

Durch das Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren vom 25. Juni 2001[166] (Zustellungsreformgesetz – ZustRG) sollte das Zustellungsrecht entsprechend häufiger Forderungen aus den Ländern und der Literatur vereinfacht und die Palette an möglichen Zustellungsformen für die Geschäftsstellen erweitert werden.[167] Während das Formanpassungsgesetz mit Einführung des § 130a ZPO die elektronische Einreichung bestimmender Schriftsätze im Zivilprozess erlaubte, wurde durch das Zustellungsreformgesetz mit § 174 Abs. 3 ZPO die elektronische Zustellung von Gerichtsentscheidungen ermöglicht.[168] Damit einhergehend wurde eine Zustellmöglichkeit per Telefax und E-Mail gesetzlich normiert.[169] Die durch das Gesetz geschaffene Regelung für die Zustellmöglichkeit per E-Mail für bestimmte Berufsgruppen findet sich in § 174 Abs. 3 ZPO. Danach kann auch nach § 174 Abs. 3 ZPO an andere Verfahrensbeteiligte als die in § 174 Abs. 1 ZPO genannten Personen elektronisch zugestellt werden, sofern diese vorher der Übermittlung elektronischer Dokumente zugestimmt haben. Zum Teil wird hierin ein Wertungswiderspruch gesehen, sofern nicht für diese Gruppe ebenfalls die erhöhte Zuverlässigkeit wie in § 174 Abs. 1 ZPO verlangt wird.[170] Dem wird jedoch von anderen unter Hinblick auf die Entstehungsgeschichte der Norm und die Gesetzesbegründung widersprochen, jedoch nicht ohne den Hinweis, dass die Folge hieraus eine in sich unstimmige Regelung sei.[171] Hierdurch ergebe sich eine ungerechtfertigte Privilegierung der elektronischen Amtszustellung.[172] Zwar hat der Gesetzgeber mit dem Gesetz zur Änderung der Vertretung durch Rechtsanwälte vor den Oberlandesgerichten (OLGVertrÄndG) vom 23. Juli 2002[173] Nachbesserungen an den Änderungen durch das Zustellungsreformgesetz vorgenommen, der Unklarheit hinsichtlich den Anforderungen an den Personenkreis, an den mittels Empfangsbekenntnis zugestellt werden kann, hat er jedoch nicht abgeholfen. Im November 2001 eröffnete der BGH den elektronischen Rechtsverkehr in Zivilsachen, indem die Einreichung von Schriftsätzen per E-Mail mit qualifizierter elektronischer Signatur erlaubt wurde.[174]

Auf den Neuerungen durch das Zustellungsreformgesetzes baute das Justizkommunikationsgesetz

166 BGBl. I 1206.
167 BT-Drs. 14/4554, 13.
168 *Viefhues*, NJW 2005, 1009, 1010.
169 BT-Drs. 14/4554, 13.
170 *Hartmann* in *Baumbach*/*Lauterbach*/*Albers*/*Hartmann*, § 174 Rn. 10.
171 *Häublein* in MüKo-ZPO Band 1, § 174 Rn. 19.
172 *Häublein*, MDR 2002, 563.
173 BGBl I, 2850.
174 *Berlit*, JurPC Web-Dok. 13/2006, Abs. 11.

vom 22. März 2005[175] auf, indem es den durch Formanpassungsgesetz und Zustellungsreformgesetz normierten Möglichkeiten der Gerichte, auf elektronischem Weg Eingänge entgegenzunehmen und Zustellungen zu bewirken, die Möglichkeit zur elektronischen Aktenführung gegenüberstellte.[176] Hiervon erhoffte man sich diverse, auf einen schnelleren, kostengünstigeren und effizienteren Gerichtsablauf abzielende Effekte wie beispielsweise eine schnellere Kommunikation zwischen Gerichten und Verfahrensbeteiligten, eine dezentrale und kooperative Aktenbearbeitung, Verbesserungen in der Handhabung der Akten sowie eine vereinfachte Logistik.[177] Dabei sollte die elektronische Aktenführung- und Bearbeitung nicht die Papierakte sofort ersetzen, sondern als gleichberechtigt neben diese treten.[178] Um die vorher geltenden Formvorschriften nicht antasten zu müssen, wurde für die Abbildung der Anforderungen an schriftliche Dokumente für elektronische Dokumente auf elektronische Signaturen nach dem Signaturgesetz verwiesen. Die unterschiedlichen Hürden der „Papierwelt“ wurden dabei durch die verschiedenen Abstufungen der elektronischen Signatur abgebildet.[179] Die umfangreichsten Änderungen wurden durch das Justizkommunikationsgesetz an der Zivilprozessordnung vorgenommen, was sich aufgrund der zahlreichen Verweise anderer Prozessordnungen auf die Zivilprozessordnung erklären lässt.[180] Dabei wurden zunächst zahlreiche terminologische Änderungen eingeführt, wie beispielsweise der Wechsel vom analog geprägten Begriff „Schriftstück“ hin zu dem auch die digitale Welt umfassenden „Dokument“ oder auch vom Begriff „Vordruck“ zum universellen Begriff „Formular“. Eine Kernvorschrift des Justizkommunikationsgesetzes ist die in Art. 1 Nr. 7 JKommG vorgesehene Einfügung eines § 130b ZPO. Dieser ermöglicht dem Gericht – konkret den Richtern, Rechtspflegern, Urkundsbeamten der Geschäftsstelle sowie Gerichtsvollziehern – statt eines handschriftlich unterschriebenen Schriftstücks ein gerichtliches elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist, zu erstellen. Der Zeitpunkt soll sich hierbei nach den Rechtsverordnungen gemäß § 130a Abs. 2 ZPO, der durch das Formanpassungsgesetz eingefügt wurde, richten.[181] Dies mag verwundern, da § 130a Abs. 2 ZPO dem Wortlaut nach nur die Einreichung von elektronischen Dokumenten nennt, wenngleich es natürlich sinnvoll erscheint, neben der Einreichung elektronischer Dokumente und den Formatanforderungen hierfür auch zugleich den Versand elektronischer Dokumente mitzuregeln.

Anders als bei analogen Schriftstücken besteht bei elektronischen Dokumenten nicht ohne Weiteres

175 BGBl. I 837.
176 *Viefhues*, NJW 2005, 1009, 1010.
177 Gesetzesentwurf zum Justizkommunikationsgesetz vom 28.10.2004, BT-Drs. 15/4067, 24.
178 BT-Drs. 15/4067, 24.
179 BT-Drs. 15/4067, 24.
180 So im Ergebnis auch *Viefhues*, NJW 2005, 1009, 1011.
181 *Hartmann* in *Baumbach*/*Lauterbach*/*Albers*/*Hartmann*, § 130b Rn. 1.

die Möglichkeit, Vermerke auf den Dokumenten anzubringen. Eine Veränderung eines einmal elektronisch signierten Dokuments würde dazu führen, dass die Signaturprüfung kein positives Ergebnis ausgibt, da sich der Inhalt des Dokuments hierdurch ja im Vergleich zum Zeitpunkt der Signatur verändern würde.[182] Um dieses Problem zu lösen, sieht das Justizkommunikationsgesetz an verschiedenen Stellen vor, Vermerke stattdessen durch ein separates elektronisches Dokument zu erstellen, und dieses mit dem Ursprungsdokument „untrennbar zu verbinden“ (z.B. §§ 105 Abs. 1, 164 Abs. 4, 315 Abs. 3, 319 Abs. 2, 320 Abs. 4 ZPO). Ausweislich der Gesetzesbegründung soll dies durch eine Containersignatur als „elektronische Klammer“ erfolgen.[183] Aufgrund der Natur des Signaturgesetzes, Signaturschlüssel stets an natürliche Personen zu binden, ist diese Containersignatur entsprechend mit dem Schlüssel einer natürlichen Person wie etwa des Urkundsbeamten der Geschäftsstelle zu versehen, und nicht etwa mit einem (nach dem Signaturgesetz nicht möglichen) „Gerichtssignaturschlüssel“. Dies wurde im Schrifttum zum Teil bedauert und mit dem Ruf nach einer „Behördensignatur“ verbunden.[184]

Durch eine Hinzufügung zu § 130a ZPO in Form des § 130a Abs. 1 S. 3 ZPO kann das Gericht auf nicht lesbare oder nicht bearbeitbare eingehende Dokumente reagieren, indem es dem Absender unverzüglich die mangelnde Eignung des Dokuments und die geltenden technischen Rahmenbedingungen mitteilt. Eine weitere wesentliche Neuerung ist der § 298 ZPO, der den Transfer von einem elektronischen Dokument in ein Papierdokument durch das Gericht regelt, nicht jedoch durch einen Anwalt.[185] Durch § 298a ZPO schließlich wird die Führung einer elektronischen Akte erlaubt. Eingehende Dokumente in Papierform werden dabei nach § 298a Abs. 2 ZPO durch Einscannen in elektronische Dokumente überführt, die Ursprungsdokumente müssen jedoch danach bis zum rechtskräftigen Verfahrensabschluss aufbewahrt werden, „sofern sie in Papierform weiter benötigt werden“. Damit hatte sich das Justizkommunikationsgesetz für die Lösung entschieden, bei beweisrechtlichen Fragen im Zweifel auf das Originaldokument abzustellen.[186]

Eine Gleichstellung der Beweiskraft von privaten elektronischen Dokumenten mit qualifizierter elektronische Signatur mit jener von Privaturkunden sowie eine Gleichstellung der Beweiskraft von öffentlichen elektronischen Dokumenten mit jener der öffentlichen Urkunde findet sich in § 371a ZPO.

In der Literatur wurde das Justizkommunikationsgesetz im Allgemeinen als Schritt in die richtige Richtung angesehen, Kritik daran bezog sich vor allem auf die als zu hoch wahrgenommenen

182 So auch *Viefhues*, NJW 2005, 1009, 1010.
183 BT-Drs. 15/4067 30.
184 *Viefhues*, NJW 2005, 1009, 1011.
185 *Viefhues*, NJW 2005, 1009, 1012 Fn. 49.
186 *Viefhues*, NJW 2005, 1009, 1013.

Sicherheitsanforderungen, die geeignet seien, die Fortentwicklung des elektronischen Rechtsverkehrs eher zu behindern als zu befördern.[187] Weiterhin wurden das wegen nötiger Investitionen fragliche Kosten-Nutzen-Verhältnis sowie das ungelöste Problem der Archivierung kritisiert.[188]

3.1.5 De-Mail-Gesetz

Eine weitere wesentliche gesetzliche Neuerung zur sicheren Kommunikation war neben dem Signaturgesetz das Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 28. April 2011[189]. Dem De-Mail-Gesetz von 2011 vorausgegangen war ein Gesetzesentwurf der Bundesregierung vom 8. April 2009 zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften[190]. Dieser Entwurf, in dem allerdings schon punktuell der Begriff „De-Mail“ für den neu zu schaffenen Kommunikationsweg verwendet wurde,[191] fiel jedoch dem Grundsatz der Diskontinuität des Bundestages zum Opfer.[192] Die nach dem De-Mail-Gesetz angebotenen Dienste sollten dabei die Infrastruktur für elektronische Kommunikation mit gewährleisteter Sicherheit, Vertraulichkeit und Authentizität schaffen, um die Qualität von Diensten im Internet zu steigern und zu höherer Rechtssicherheit zu führen.[193] Die über diese Infrastruktur versandten Nachrichten sind technisch normalen E-Mails nachgebildet. Dabei sind sie allerdings nicht direkt mit dieser kompatibel – ein Versenden von E-Mails an De-Mail-Adressen oder von De-Mails an E-Mail-Adressen scheidet deswegen aus.[194] Für eine solche Übersetzung zwischen den Standards notwendige Gatewaysysteme wären zwar denkbar, waren jedoch vom Gesetzgeber nicht erwünscht.[195] Die Nutzung des De-Mail-Versanddienstes soll dabei sowohl über ein Webinterface möglich sein, was die nach dem Gesetz geforderte Mindestvariante darstellt, als auch über ein E-Mail-Programm wie Microsoft Outlook oder Mozilla Thunderbird, sofern der jeweilige De-Mail-Anbieter diese Variante unterstützt.[196]

187 *Fischer*, 48; weiter geht der Autor noch in *Fischer*, DRIZ 2005, 90, 95, indem er eine hinderliche Wirkung des Justizkommunikationsgesetzes aus der Fixierung des Gesetzes auf die Form statt auf den Inhalt des Gerichtsverfahrens ableitet.
188 *Hähnchen*, NJW 2005, 2257, 2259.
189 BGBl. I, 666.
190 BT-Drs. 16/12598.
191 BT-Drs. 16/12598 21 f.
192 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 729.
193 BT-Drs. 16/12598, 14.
194 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 731.
195 *Werner/Wegener*, CR 2009, 310, 312.
196 *Bundesamt für Sicherheit in der Informationstechnik*, De-Mail-Broschüre, 12

Die De-Mail-Dienste werden nach dem Gesetz von privaten Unternehmen betrieben, die sich einer freiwilligen Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik unterworfen haben (§ 17 i.V.m. § 2 De-Mail-G). Zwar ist ein Betreiben von Diensten mit einem Leistungsspektrum gleich dem von De-Mail jedermann ohne Erlaubnis möglich, jedoch entstehen die rechtlichen Wirkungen von über solche Dienste versandten und empfangenen Nachrichten und die Befugnis, als akkreditierter Anbieter im Rechtsverkehr aufzutreten, erst mit erfolgter Akkreditierung.[197] Zu den durch die Akkreditierung eintretenden Rechtsfolgen gehört für den Diensteanbieter die Berechtigung, ein Gütezeichen zu führen, sich auf die nachgewiesene Sicherheit des Dienstes zu berufen und sich als akkreditierter Diensteanbieter zu bezeichnen (§ 17 Abs. 1 De-Mail-G). Mit der Akkreditierung unterwirft sich der Diensteanbieter zugleich der Aufsicht durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) (§ 20 Abs. 1 S. 2 i.V.m. § 2 De-Mail-G). Schließlich ist auch die rechtliche Qualifikation als De-Mail-Dienst im Sinne von § 1 De-Mail-G an die Akkreditierung geknüpft, da nach § 1 Abs. 2 S. 2 De-Mail-G ein De-Mail-Dienst von einem nach dem De-Mail-Gesetz akkreditierten Diensteanbieter betrieben wird. Damit sind auch die in anderen Gesetzen angeordneten Rechtsfolgen wie die elektronische Zustellung im Zivilprozess (§ 174 Abs. 3 ZPO) oder im Verwaltungsverfahren (§§ 2, 5 Abs. 5 VwZG) nur durch akkreditierte Diensteanbieter möglich, die für die Zustellung als beliehene Unternehmer agieren (§ 5 Abs. 6 S. 2 De-Mail-G).

Der Akkreditierung des Diensteanbieters steht auf Nutzerseite eine Identitätsprüfung gegenüber. Hierdurch soll sichergestellt werden, dass die Identität des Nutzer fest mit dem De-Mail-Postfach verknüpft ist, um die Rechtssicherheit von Kommunikation über De-Mail zu steigern. Hinzu kommt das Erfordernis einer sicheren Anmeldungsmöglichkeit am Postfach, die den Regelfall der Anmeldung bei einem De-Mail-Account darstellen soll. Diese sichere Anmeldung erfordert anders als die sonst oft im Internet gängige Authentifizierung mittels Benutzername und Passwort eine sogenannte Zwei-Faktor-Authentifizierung mit zwei voneinander unabhängigen Sicherungsmitteln (§ 4 Abs. 1 De-Mail-G). Als Sicherungsmittel (die oft unter der Bezeichnung „Besitz und Wissen“ zusammengefasst werden) kommen zum Beispiel eine Chipkarte (Besitz) mit PIN-Schutz (Wissen) in Frage. Auch die Identitätsnachweisfunktion des elektronischen Personalausweises (die ebenfalls über eine PIN freigeschaltet werden muss[198]) ist als Spezialfall einer Chipkarte mit PIN-Schutz in § 4 Abs. 2 De-Mail-G als in jedem Fall vom Diensteanbieter bereitzustellende Anmeldeoption vorgesehen. Eine weniger sichere Anmeldeart wie jene mit Benutzernamen und Passwort kann gemäß § 4 Abs. 1 S. 7 De-Mail-G angeboten werden, dann muss jedoch eine Belehrung des Nutzers

197 BT-Drs. 17/3630, 20.
198 *Roßnagel/Hornung/Schnabel*, DuD 2008, 168.

über die geringere Sicherheit dieser Anmeldung erfolgen. Der Absender einer De-Mail-Nachricht kann verlangen, dass der Empfänger nur bei sicherer Anmeldung Zugriff auf diese erhält (§ 5 Abs. 4 De-Mail-G). Umgekehrt kann der Empfänger nach § 5 Abs. 5 De-Mail-G auf Verlangen des Absenders eine Bestätigung darüber erhalten, dass der Absender zum Versandzeitpunkt sicher angemeldet war. Diese Maßnahmen sollen die Sicherheit im Rechtsverkehr dadurch erhöhen, dass sie den Beteiligten an der Kommunikation eine Bescheinigung über die Identität des jeweils Anderen erteilen. An die sichere Anmeldung ist auch die förmliche Zustellung per De-Mail geknüpft, da gemäß § 5 Abs. 9 De-Mail-G eine zur förmlichen Zustellung berechtigte öffentliche Stelle eine Abholbestätigung über die Zustellung verlangen kann, aus der sich auch die sichere Anmeldung des Empfängers der Zustellung ergibt. Gemäß § 5 Abs. 10 De-Mail-G kann eine derart zugestellte De-Mail-Nachricht ohne sichere Anmeldung erst 90 Tage nach Empfang gelöscht werden, was eine Zugangsvereitelung durch Dritte erschweren soll.[199] Sowohl die Sende- und Empfangsbestätigung als auch die Abholbestätigung sind durch den Diensteanbieter jeweils mit einer qualifizierten elektronischen Signatur zu sichern, um Fälschungen zu verhindern.

Um über die Identitätssicherung hinaus auch eine technische Sicherheit zu gewährleisten, ist in § 5 Abs. 3 S. 2 Nr. 1 De-Mail-G eine zwingende Transportverschlüsselung der De-Mail-Nachrichten zwischen den Anbietern vorgesehen. In § 5 Abs. 3 S. 2 Nr. 2 De-Mail-G wird darüber hinaus eine Verschlüsselung des Inhalts der De-Mail-Nachrichten bei der Übertragung zwischen den akkreditierten Anbietern verlangt. Demgegenüber stellt § 5 Abs. 3 S. 3 De-Mail-G jedoch klar, dass hierunter keine Ende-zu-Ende-Verschlüsselung im Sinne einer Verschlüsselung zwischen ursprünglichem Absender und letztendlichem Empfänger der Nachricht zu verstehen ist, das Gesetz aber einer solchen nicht entgegensteht. Dieser Punkt hat verschiedentlich zu Kritik am De-Mail-Gesetz geführt, da die verwendete Verschlüsselung somit nicht vor einer Kenntnisnahme vom Inhalt der Nachrichten durch die akkreditierten Diensteanbieter selbst oder böswillige Dritter, die sich Zugang zu den Rechnern der Diensteanbieter verschaffen, schütze.[200] Als ein Grund für den Verzicht auf eine verpflichtende Ende-zu-Ende-Verschlüsselung wurde angeführt, dass durch eine solche zu hohe technische Zugangshürden für den Versand von Nachrichten geschaffen werden könnten.[201] In diesem Zusammenhang wurde auch kritisiert, dass das Gesetz explizit eine kurzzeitige Entschlüsselung der Nachrichten bei den De-Mail-Anbietern vorsieht, damit die Nachrichten auf Schadsoftware geprüft werden können.[202] Als Reaktion auf die Kritik an der fehlenden Ende-zu-Ende-Verschlüsselung stellte die vom Bundesinnenministerium im Rahmen des 8. Nationalen IT-

199 BT-Drs. 17/3630, 31.
200 *Lapp*, DuD 2011, 651, 653; siehe hierzu bereits oben unter 2.3.5.
201 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 730.
202 *Neumann*, Stellungnahme EGovG, 5.

Gipfels gegründete Arbeitsgemeinschaft De-Mail Anfang März 2015 ein Verschlüsselungsplugin für die Webbrowser Mozilla Firefox und Google Chrome vor, mit dem die Verschlüsselungssoftware PGP komfortabel mit den webbasierten Benutzeroberflächen der De-Mail-Anbieter benutzbar sein soll.[203]

Ein Kernanliegen des De-Mail-Gesetzes war es, Einsparpotentiale insbesondere in der Verwaltung durch Digitalisierung eines Teils der bisher über Briefpost abgewickelten Vorgänge zu realisieren. Nach den im Entwurf des Bürgerportalgesetzes angestellten Berechnungen sollten in der Verwaltung so über vier Jahre gemittelt jährlich 50 bis 80 Millionen Euro eingespart werden, ab dem fünften Jahr nach Erlass des Gesetzes sogar 100 bis 150 Millionen Euro[204]. Für diese Zahlen ging der Entwurf des Bürgerportalgesetzes allerdings davon aus, dass die Kosten für den Versand einer Bürgerportalnachricht (in einer Analogie zur Briefpost als Porto bezeichnet) auf lediglich einen Bruchteil des Briefportos belaufen werde. Im Entwurf des De-Mail-Gesetzes wurden die Einsparerwartungen demgegenüber deutlich nach unten korrigiert, so ging man hier lediglich noch von einer Einsparmöglichkeit von jährlich durchschnittlich 20 – 40 Millionen Euro während der ersten 4 Jahre und 40 – 80 Millionen Euro ab dems fünften Jahr aus.[205] Dies dürfte darauf zurückzuführen sein, dass man in diesem Entwurf schon deutlich vorsichtiger im Bezug auf die „Portokosten“ für De-Mail-Nachrichten war, für die nach diesem Entwurf lediglich „nicht auszuschließen“ war, dass sie unter dem zu dieser Zeit üblichen Briefporto lagen.[206] Die tatsächlichen Kosten für die Nutzung von De-Mail variieren in der Praxis – so ist beim Anbieter GMX der Versand einer normalen De-Mail ohne Versand- oder Empfangsbestätigung kostenlos,[207] beim Anbieter T-Online kostet eine solche De-Mail 39 Cent.[208] Zusatzleistungen wie Versand- und Empfangsbestätigung lassen sich die Anbieter jeweils zusätzlich vergüten, hierfür werden bei den obengenannten Anbietern jeweils 12 Cent zusätzlich erhoben.

Bisher haben sich vier De-Mail-Anbieter (namentlich die 1&1 De-Mail-GmbH, die Mentana Claimsoft GmbH, die Telekom Deutschland GmbH sowie die T-Systems International GmbH) akkreditieren lassen.[209] Nach dem Zwischenbericht der Bundesregierung über den Stand der Einführung von De-Mail vom 16.2.2015 setzt sich deren Kundenstamm aus ca. einer Million Privatnutzer und einer Anzahl von Unternehmenskunden einschließlich Verwaltung im hohen

203 *Borchers/Wilkens*, Heise-Newsticker 9.3.2015.
204 BT-Drs. 16/12598 2.
205 BT-Drs. 17/3630, 3.
206 BT-Drs. 17/3630, 3.
207 *1&1 Mail & Media GmbH*, GMX-Preisliste.
208 *Telekom*, T-Online: De-Mail-Preisliste, 2.
209 *Bundesamt für Sicherheit in der Informationstechnik*, Akkreditierte De-Mail Diensteanbieter.

fünfstelligen Bereich zusammen.[210] Gleichwohl sei die kritische Masse bei den Nutzerzahlen noch nicht erreicht, was mit der verzögerten Einführung von De-Mail-Diensten begründet wird.[211]

3.1.6 EGVP, OSCI und SAFE

Parallel zu den oben genannten gesetzlichen Vorstößen in Richtung elektronischer Rechtsverkehr hat sich bereits 2004 mit dem elektronischen Gerichts- und Verwaltungspostfach (EGVP) ein System etabliert, das die sichere, vertrauliche und beweisbare Kommunikation zwischen Gerichten und Behörden auf der einen Seite und Bürgern auf der anderen Seite ermöglichen sollte. Das EGVP bestand zunächst als freiwilliges Angebot des Bundesverwaltungsgerichts und des Bundesfinanzhofs. Mit diesem gingen sie einen anderen Weg als der BGH, für den bereits im November 2001 der elektronische Rechtsverkehr per E-Mail mit qualifizierter elektronischer Signatur durch die Verodnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof (ERVVOBGH)[212] eröffnet wurde.[213]

Rechtsgrundlage dieses freiwilligen elektronischen Gerichtsverkehrs war der durch das Formanpassungsgesetz von 2001 eingefügte § 86a VwGO für das Bundesverwaltungsgericht sowie § 77a FGO für den Bundesfinanzhof. Nach diesen Vorschriften (die ihrerseits durch das Justizkommunikationsgesetz von 2005 aufgehoben und durch die neuen § 55a VwGO und § 52a FGO ersetzt wurden) war eine freiwillige Einreichung von vorbereitenden Schriftsätzen sowie Anträgen und Erklärungen der Parteien möglich. Voraussetzung hierfür war nach § 86a Abs. 1 S. 1 VwGO bzw. § 77a Abs. 1 S. 1 FGO, dass das Dokument „für die Bearbeitung durch das Gericht geeignet ist“. Nach § 86a Abs. 1 S. 2 VwGO bzw. § 77a Abs. 1 S. 2 FGO musste das Dokument überdies mit einer qualifizierten elektronischen Signatur versehen sein.[214] Schließlich war nach § 86a Abs. 2 S. 1 VwGO bzw. § 77a Abs. 2 S. 1 FGO per Rechtsverordnung der Bundes- oder Landesregierung eine Bestimmung des Zeitpunktes, ab dem Dokumente elektronisch eingereicht werden können, erforderlich. Diese Rechtsverordnung erging in Form der Verordnung über den elektronischen Rechtsverkehr beim Bundesverwaltungsgericht und beim Bundesfinanzhof

210 BT-Drs. 18/4042, 2.
211 BT-Drs. 18/4042, 2.
212 BGBl. I 3225.
213 *Berlit*, JurPC Web-Dok. 13/2006, Abs. 11.
214 Zur insoweit missverständlichen Formulierung „Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen“, vgl. die Ausführungen oben unter Abschnitt 3.1.3 zu § 130a ZPO.

(ERVVBVerwGBFH) vom 26. November 2004[215] und eröffnete den freiwilligen elektronischen Rechtsverkehr mit dem Bundesverwaltungsgericht und Bundesfinanzhof zum 1. Dezember 2004. Die Rechtsverordnung regelte die Formanforderungen an den elektronischen Rechtsverkehr mit Bundesverwaltungsgericht und Bundesfinanzhof und bestimmte zugleich als einzig zulässigen Übertragungsweg die Nutzung des OSCI-Protokolls mittels des von den teilnehmenden Gerichten zur Verfügung gestellten EGVP-Clients. Da dieser auch die qualifizierte elektronische Signatur von ausgehenden Nachrichten beherrschte, waren somit die Voraussetzungen für den elektronischen Rechtsverkehr mit diesen Gerichten geschaffen.

Weitere Bundesgerichte boten in der Folgezeit ebenfalls den fakultativen elektronischen Rechtsverkehr mit ihnen an – so eröffneten das Bundesarbeitsgericht mit Rechtsverordnung vom 9. März 2006[216] und das Bundessozialgericht mit Rechtsverordnung vom 18. Dezember 2006[217] den elektronischen Rechtsverkehr, der Bundesgerichtshof und das Bundespatentgericht folgten mit Rechtsverordnung vom 24. August 2007[218]. Auch zahlreiche Gerichte der Länder eröffneten nach und nach den freiwilligen elektronischen Rechtsverkehr mittels qualifizierter elektronischer Signatur und EGVP.

Das System EGVP basiert auf dem Standard OSCI, dessen erste Version 1.0 im November 2000 veröffentlicht wurde.[219] Bei OSCI handelt es sich um eine Bündelung von insbesondere für das E-Government geeigneten technologischen Standards zur Klassifizierung von Daten sowie zur vertraulichen und authentifizierten Kommunikation. Die Entwicklung von OSCI wurde vom Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA ADV[220]) in Auftrag gegeben. Der Standard ist in zwei Teile aufgegliedert, wobei Teil A (auch als OSCI-Transport bezeichnet) sich mit Transport- und Sicherheitsfunktionen befasst und Teil B (auch XÖV[221]-Standards genannt) Datenformate für die übertragenen Inhalte auf Basis des XML-Formates[222] beschreibt.[223] Bei OSCI-Transport werden insbesondere auch die rechtlichen Vorgaben des Signaturgesetzes berücksichtigt, um eine rechtssichere Kommunikation zu ermöglichen. Auch eine Ende-zu-Ende-Verschlüsselung dergestalt, dass der verwendete

215 BGBl I, 3091.
216 Verordnung über den elektronischen Rechtsverkehr beim Bundesarbeitsgericht, BGBl. I 519.
217 Verordnung über den elektronischen Rechtsverkehr beim Bundessozialgericht (ERVVOBSG), BGBl. I 3219.
218 Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof und Bundespatentgericht (BGH/BPatGERVV), BGBl. I 2130.
219 *OSCI Leitstelle*, Projektauftrag OSCI Transport 1.2, 1; vgl. hierzu bereits oben unter 2.3.3.
220 Rechtsnachfolger des nunmehr aufgelösten KoopA ADV ist der IT-Planungsrat, der mit dem Gesetz zum Vertrag über die Errichtung des IT-Planungsrats gegründet wurde; vgl. BT-Drs. 17/427, 6.
221 XML in der Öffentlichen Verwaltung.
222 XML steht dabei für eXtensible Markup Language und beschreibt ein Format, mit dem strukturierte Informationen in einer für Menschen noch lesbaren, aber für Maschinen gut auswertbaren Form gespeichert werden können.
223 *Die Beauftragte der Bundesregierung für Informationstechnik (BfIT)*, XÖV-Handbuch 1.0, 8.

Postfachserver (der sogenannte Intermediär) ihm vorliegende verschlüsselte Nachrichten an Dritte nicht entschlüsseln kann, ist Bestandteil des Standards.[224] Der OSCI-Standard gehört in seiner Version 1.2 zu den im SAGA-Modul technische Spezifikationen zu den empfohlenen Standards bei Anwendungsprotokollen zur Kommunikation.[225] Da die SAGA-Standardisierung für die Bundesverwaltung verbindlich ist, ist hiermit eine starke Präferenz zur Nutzung von OSCI vorgegeben.

Eine wesentliche Inhaltliche Erweiterung des EGVP-Systems erfolgte schließlich in EGVP-Version 2.6.0 vom 20.6.2011 mit Anbindung von EGVP an das SAFE-System.[226] Während bei früheren EGVP-Versionen die Benutzerverwaltung zentralisiert war, ermöglichte SAFE nunmehr eine dezentrale (hierfür steht der Begriff *federated* im Akronym SAFE) Verwaltung von Benutzern und Rollen.

Dies ermöglicht es, dass einzelne Benutzergruppen ihre eigene Identifizierungs- und Authentifizierungsinfrastruktur nutzen können. Den Anfang machte hierbei die Bundesnotarkammer, die für das von ihr geführte Zentrale Testamentsregister sowie das Zentrale Vorsorgeregister als Identifizierungslösung SAFE benutzt.[227] Diese Neuerung ermöglichte auch die vom Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vorgesehene Einrichtung des besonderen elektronischen Anwaltspostfaches (beA) bei der Bundesrechtsanwaltskammer. Eine weitere Anpassung an unterschiedliche Trusted Domains schließlich erfolgte mit EGVP-Version 2.9 vom 16. Juni 2014, womit eine Kompatibilität mit dem besonderen elektronischen Anwaltspostfach, das ursprünglich ab 1.1.2016 von der Bundesrechtsanwaltskammer zur Verfügung gestellt werden sollte, ermöglicht wird.[228] SAFE ermöglicht überdies die Verwaltung von Rollen, die wiederum aufgeteilt sind in Rollentyp (z.B. EGVP oder Vollstreckungsportal) und Rollenwert (z.B. Bürger oder Behörde), und aus denen sich die zugreifbaren Verzeichnisinhalte und -funktionen ergeben.[229]

3.1.7 Das Gesetz zur Förderung des elektronischen Rechtsverkehrs

Als Resultat aus den bisherigen Erfahrungen mit dem elektronischen Rechtsverkehr wurde am 8.

224 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 9.
225 *Die Beauftragte der Bundesregierung für Informationstechnik (BfIT)*, SAGA-Modul Technische Spezifikationen Version de.bund 5.0.0, 61.
226 *egvp.de*, Hinweise Hardwarezertifikate, 1.
227 *Arbeitsgruppe „IT-Standards in der Justiz“ der Bund-Länder-Kommission*, SAFE-Übersicht, 5.
228 *egvp.de*, Neuerungen EGVP 2.9.
229 *Arbeitsgruppe „IT-Standards in der Justiz“ der Bund-Länder-Kommission*, SAFE-Rollenmodell, 1.

Januar 2012 durch die Länder Hessen, Baden-Württemberg und Sachsen ein Diskussionsentwurf für ein Gesetz zur Förderung des elektronischen Rechtsverkehrs in der Justiz veröffentlicht. Ausgangspunkt war die bis zu diesem Zeitpunkt geringe Nutzung der elektronischen Angebote für Justizkommunikation, der man durch eine Neugestaltung des elektronischen Rechtsverkehrs einschließlich einer Nutzungspflicht für „professionelle Einreicher" begegnen wollte.[230] Dem Diskussionsentwurf folgten Stellungnahmen diverser Interessenvertretungen wie beispielsweise dem Deutschen Richterbund,[231] der Bundesrechtsanwaltskammer,[232] dem deutschen Anwaltverein[233] sowie dem BITKOM,[234] die grundsätzlich dem Ziel einer Förderung der Digitalisierung in der Justiz aufgeschlossen gegenüberstanden, aber im Detail verschiedene Regelungen kritisierten.[235] Dieser Diskussionsentwurf wurde von den genannten Ländern und unter Beteiligung der Länder Berlin, Bayern, Niedersachsen und Schleswig-Holstein am 30. August 2012 als Länderentwurf in den Bundesrat eingebracht.[236]

Dem Länderentwurf folgte ein Gegenentwurf der Bundesregierung, der am 21.12.2012 in den Bundesrat eingebracht wurde.[237] Auch dieser Entwurf wurde wieder kritisch von diversen Verbänden, insbesondere jenen, die sich bereits zum Diskussionsentwurf der Länder geäußert hatten, begleitet. Die stärkste Kritik entzündete sich an der Verpflichtung der Anwaltschaft zur Nutzung des elektronischen Rechtsverkehrs,[238] an den Plänen eines automatischen Empfangsbekenntnisses, das ohne Handeln oder auch nur Kenntnisnahme des Anwalts versandt werden sollte,[239] sowie an der befürchteten Absenkung des Sicherheitsniveaus durch Verzicht auf die qualifizierte elektronische Signatur[240] und die Zulassung von De-Mail als sicheren

230 Diskussionsentwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs in der Justiz, abrufbar unter https://edvgt.de/wp-content/uploads/2016/02/E-Justice_Bundesratsinitiative_-_Diskussionsentwurf_Stand_8_Januar_2012.pdf, zuletzt abgerufen am 18.12.2017, 1 f.; vgl. hierzu bereits oben unter 1.

231 *Scholz*, DRB Stellungnahme Nr. 04/12.

232 *Backs/Kühnelt/Sandkühler/Schmid u. a.*, BRAK-Stellungnahme Nr. 6/2012.

233 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 14/2012.

234 *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Stellungnahme Diskussionsentwurf ERVG.

235 Exemplarisch seien hier die Stellungnahmen durch die Neue Richtervereinigung (https://www.neuerichter.de/details/artikel/article/stellungnahme-zum-diskussionsentwurf-eines-gesetzes-zur-foerderung-des-elektronischen-rechtsverkehrs-in-der-justiz-374.html), den Deutschen Notarverein (http://www.dnotv.de/stellungnahmen/diskussionsentwurf-einer-bundesratsinitiative-fuer-ein-gesetz-zur-foerderung-des-elektronischen-rechtsverkehrs-in-der-justiz/), die Bundesrechtsanwaltskammer (http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2012/februar/stellungnahme-der-brak-2012-06.pdf), alle zuletzt abgerufen am 18.12.2017.

236 BR-Drs. 503/12.

237 BR-Drs. 818/12.

238 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 14/2012, 6 f.; *Volk/Burianski/Feil/Redeker u. a.*, DAV-Stellungnahme 87/2012, 4; a.A. z.B. *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Stellungnahme Diskussionsentwurf ERVG, 4.

239 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 14/2012, 7 ff.

240 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 3.

Einreichungsweg.[241] Befürchtet wurden zudem unkalkulierbare Haftungsrisiken durch mögliche Ausfälle des elektronischen Übermittlungssystems, insbesondere im Hinblick auf den als ambitioniert wahrgenommenen Zeitplan zur Umsetzung und der Abweichungsmöglichkeiten für die Länder.[242]

Dieser Kritik wurde in dem schließlich am 16.10.2013 verkündeten Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten[243] zum Teil abgeholfen. Zwar blieb es bei dem generellen Anschluss- und Benutzungszwang für professionelle Einreicher, also insbesondere für Rechtsanwälte. Das automatische Empfangsbekenntnis wurde jedoch fallen gelassen zu Gunsten eines nur auf Betreiben des Postfachinhabers versandten elektronischen Empfangsbekenntnisses.[244] Für Systemausfälle wurde zudem eine Rückfallregelung auf analoge Kommunikation ins Gesetz aufgenommen.[245] Auch der angesetzte Zeitrahmen wurde durch eine Verlängerung des Umsetzungszeitraums und eine gestufte Einführung, die eine Verpflichtung zur Nutzung in den Bundesländern nur vorsah, wenn zuvor ein mindestens einjähriger Erprobungszeitraum, in dem die Nutzung des elektronischen Rechtsverkehrs schon fakultativ möglich war, absolviert wurde.[246] Keine Abweichung erfolgte jedoch vom generellen Prinzip, dass die Länder von den Einführungszeitpunkten für die Eröffnung des elektronischen Rechtsverkehrs und die Verpflichtung zum elektronischen Rechtsverkehr abweichen können, wenngleich bereits im Regierungsentwurf vom 6.3.2013 der Zeitrahmen innerhalb dessen die Länder die Einführung des elektronischen Rechtsverkehr hinauszögern können (Opt-Out-Lösung) gegenüber dem Diskussionsentwurf der Länder halbiert wurde.[247]

Schlüsselnormen des ERV-Gesetzes, bei dem es sich um ein Artikelgesetz handelt, sind die Änderungen der Zivilprozessordnung (Art. 1 ERVG) und entsprechende Normen anderer Prozessordnungen (FamFG, ArbGG, SGG, VwGO und FGO). Diese Änderungen betreffen in erster Linie die Anforderungen an ein elektronisches Dokument und die hierfür zulässigen Einreichungswege (z.B. § 130a ZPO n.F.).[248] Gemäß § 130a Abs. 3 ZPO n.F. muss ein

241 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 4 f.
242 *Volk/Burianski/Feil/Redeker u. a.*, DAV-Stellungnahme 87/2012, 4 f.
243 BGBl. I 3786.
244 Vgl. z.B. § 174 Abs. 4 S. 3 ZPO n.F.; die vorherige Formulierung „Die Zustellung nach Absatz 3 wird durch die automatisierte Empfangsbestätigung nachgewiesen." aus dem Regierungsentwurf vom 6.3.2013 (BT-Drs. 17/12634) wurde ersetzt durch die Formulierung „Die Zustellung nach Absatz 3 wird durch ein elektronisches Empfangsbekenntnis nachgewiesen.". Auch die im Regierungsentwurf noch enthaltene Drei-Tages-Fiktion in § 174 Abs. 4 S. 4 ZPO-E ist entfallen.
245 Vgl. z.B. § 130d S. 2, 3 ZPO n.F.
246 Vgl. Art. 24 Abs. 1 ERVG.
247 BT-Drs. 17/12634, 50.
248 Da die Normen in den anderen genannten Prozessordnungen alle nach dem gleichen Schema aufgebaut sind, wird im Folgenden der Aufbau nur am Beispiel der Zivilprozessordnung in der neuen Fassung dargestellt. Für die anderen betroffenen Prozessordnungen gelten die Ausführungen jedoch analog.

elektronisches Dokument entweder mit einer qualifizierten elektronischen Signatur eingereicht werden – dann über einen beliebigen Einreichungsweg – oder von der verantwortenden Person (lediglich einfach) signiert und auf einem der in § 130a Abs. 4 Nr. 1 – 4 ZPO n.F. genannten sicheren Übermittlungswege übermittelt werden. Die Übermittlungswege sind der Postfach- und Versanddienst eines De-Mail-Kontos mit sicherer Anmeldung und Anmeldebestätigung (§ 130a Abs. 4 Nr. 1 ZPO n.F.), das neu einzurichtende besondere elektronische Anwaltspostfach (§ 130a Abs. 4 Nr. 2 ZPO n.F.), die Kommunikation über ein Behördenpostfach oder das Postfach einer juristischen Person des öffentlichen Rechts nach Identifizierung (§ 130a Abs. 4 Nr. 3 ZPO n.F. i.V.m. der Rechtsverordnung nach § 130a Abs. 2 S. 2 ZPO n.F.) sowie sonstige bundeseinheitliche Übermittlungswege nach Rechtsverordnung der Bundesregierung (§ 130a Abs. 4 Nr. 4 ZPO). Für Professionelle Einreicher enthält das Gesetz zudem mit dem neu eingefügten § 130d ZPO n.F. eine Nutzungspflicht der elektronischen Einreichung, die allerdings eine Ausnahme für vorübergehende technische Störungen enthält. § 174 ZPO n.F. verlangt schließlich für die elektronische Zustellung an den Anwalt ebenfalls die Nutzung eines sicheren Übermittlungsweges sowie die Eröffnung eines entsprechenden Zugangs durch den Anwalt. Der Nachweis der elektronischen Zustellung wird nach § 174 Abs. 4 ZPO n.F. durch ein elektronisches Empfangsbekenntnis erbracht, das gemäß § 182 Abs. 3 ZPO n.F. allerdings durch einen Willensakt des Empfängers versandt werden muss.

Für die Digitalisierung eingehender Papierdokumente wurde ein neuer § 371b ZPO eingefügt, der die Beweiskraft gescannter öffentlicher Urkunden regelt. Die Vorschrift gilt nur für öffentliche Urkunden, da sich nur für diese eine Echtheitsvermutung aus dem Gesetz[249] ergibt.[250] Durch § 371b ZPO wird die Echtheitvermutung für (inländische) öffentliche Urkunden entsprechend auf einen Scan dieser Urkunde angewandt, solange der Scan nach dem Stand der Technik von einer öffentlichen Behörde oder von einer mit öffentlichem Glauben versehenen Person vorgenommen wurde und die bildliche und inhaltliche Übereinstimmung zwischen Urkunde und Scan bestätigt sowie die Bestätigung qualifiziert elektronisch signiert wurde. Wenngleich § 371b ZPO den erforderlichen Stand der Technik sowie die Form der Bestätigung nicht näher ausführt, enthält die Gesetzesbegründung hierfür einen Verweis auf die Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnik.[251] Auch andere Scanmethoden seien zulässig, um einen Scan nach dem Stand der Technik zu erzeugen, allerdings trage der der Beweisführer im Bestreitensfall die volle Beweislast für die Einhaltung des Standes der Technik.[252] Diese Begründung überrascht, da nach dem Wortlaut der Norm gerade keine der

249 Vgl. § 437 Abs. 1 ZPO.
250 BT-Drs. 17/12634, 34.
251 *Bundesamt für Sicherheit in der Informationstechnik*, TR RESISCAN.
252 BT-Drs. 17/12634, 34.

Parteien die Art der Übertragung in ein Scanprodukt unter ihrer Kontrolle hat, sondern vielmehr ein Träger öffentlicher Gewalt den Scanvorgang durchführen muss. In der Praxis wird gleichwohl zu erwarten sein, dass die Gerichte sich an den Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik in der TR-RESISCAN orientieren werden.

Die prozessualen Vorschriften werden ergänzt durch Änderungen in der Bundesrechtsanwaltsordnung. Insbesondere wird die Bundesrechtsanwaltskammer im neu eingefügten § 31a BRAO n.F. verpflichtet, für jeden eingetragenen Rechtsanwalt ein besonderes elektronisches Anwaltspostfach einzurichten, das überdies barrierefrei sein soll, und zu dem der Zugang nur durch zwei getrennte Sicherungsmittel gewährt werden soll (§ 31a Abs. 2 BRAO n.F.). Hierzu enthält § 31b BRAO n.F. eine Verordnungsermächtigung für das Bundesministerium der Justiz, nach der die nähere Ausgestaltung des beA geregelt werden kann. § 49c BRAO n.F. enthält schließlich eine Verpflichtung, Schutzschriften nur noch an das (einzurichtende) elektronische Schutzschriftenregister nach dem neu eingefügten § 945a ZPO n.F. zu richten.

Die Umsetzungsmodalitäten sind in Art. 26 ERVG geregelt. Hiernach tritt das Gesetz grundsätzlich am 1. Januar 2018 in Kraft. Vorverlagert sind demgegenüber unter anderem die Verordnungsermächtigung für das Bundesjustizministerium bezüglich des besonderen elektronischen Anwaltspostfachs mit Inkrafttreten ab 1.1.2014 (Art. 26 Abs. 4 ERVG) und die Verpflichtung zur Nutzung des elektronischen Schutzschriftenregisters ab 1.1.2017 (Art. 26 Abs. 6 ERGV). Nachgelagert sind die Regelungen zur Nutzungspflicht wie in § 130d ZPO n.F. (Art. 26 Abs. 7 ERVG), diese treten erst mit dem 1.1.2022 in Kraft.

Für die prozessualen Änderungen, um Dokumente wie in § 130a ZPO n.F. elektronisch einzureichen, können die Länder nach Art. 24 Abs. 1 ERVG durch Rechtsverordnung jeweils den Termin für das Inkrafttreten der neuen Fassung ein oder zwei Jahre (auf den 1.1.2019 oder 2020) nach hinten verschieben. Die (aus Anwaltssicht aktive) Nutzungspflicht können die Länder hingegen durch Rechtsverordnung um ein oder zwei Jahre vorverlagern (auf den 1.1.2020 oder 2021). Bei bei einer Vorverlagerung nach Art. 24 Abs. 1 ERVG ein Inkrafttreten der Nutzungsverpflichtung ab 1.1.2021 in Betracht kommt, Art. 24 Abs. 2 ERVG. Hiermit soll sichergestellt werden, dass in jedem Land eine Nutzung des elektronischen Rechtsverkehrs mindestens ein Jahr lang möglich war, bevor eine Nutzungsverpflichtung in Kraft tritt.

Flankierend zu den neuen Vorschriften in der BRAO ist zudem am 28.9.2016 die Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (Rechtsanwaltsverzeichnis- und Postfachverordnung – RAVPV)[253] in Kraft getreten. In dieser wird

253 BGBl I, 2167.

die Ausgestaltung des besonderen elektronischen Anwaltspostfachs konkretisiert. Insbesondere wird auf die Kritik an der nach der anfänglichen Auffassung der Bundesrechtsanwaltskammer bestehenden Obliegenheit zur Überwachung des beA bereits ab dem Ersteinrichtungsdatum eingegangen. Diese Auffassung hatte auf Antrag zweier Rechtsanwälte zu einer einstweiligen Anordnung des Anwaltsgerichtshofs Berlin geführt, die die Eröffnung des beA für die Betroffenen verbot. Nach Erlass der Rechtsanwaltsverzeichnis- und Postfachverordnung, die in § 31 klarstellt, dass eine Empfangsbereitschaft erst ab dem 1.1.2018 auch ohne eigene diesbezügliche Erklärung verlangt werden kann, wies der AGH Berlin allerdings einen weiteren Antrag eines Kölner Antragstellers unter Hinweis auf die neue neue Rechtslage ab.[254]

3.1.8 Die eIDAS-Verordnung und das Vertrauensdienstegesetz

Eine Änderung des europäischen Signaturrechts und verwandter Vertrauensdienste wie elektronischer Einschreiben und Website-Zertifikaten wurde mit der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung - eIDAS-VO) vollzogen.[255] Ziel der Verordnung ist die Vereinheitlichung einer im Rahmen der Evaluierung der EU-Signaturrichtlinie als heterogen wahrgenommenen Umsetzung in den Mitgliedsstaaten, die einer weiteren Verbreitung elektronischer Signaturen im Weg stünde.[256]

Die Vorbereitungen für die Verordnung gehen dabei bereits auf das Jahr 2008 zurück, in dem die Kommission einen „Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzüberschreitender öffentlicher Dienste im Binnenmarkt“ erstellte, der nach einer Konsultation und mehreren Studien zu dem Thema in einem am 4. Juni 2012 vorgelegten ersten Vorschlag für eine eIDAS-Verordnung mündete.[257] Die am 28. August 2014 im Amtsblatt verkündete[258] Verordnung trat mit dem 1. Juli 2016 in den Mitgliedsstaaten in Kraft (Art. 52 Abs. 2 eIDAS-VO) und ist seit diesem Zeitpunkt in den Mitgliedsstaaten unmittelbar geltendes Recht. Einzelne Vorschriften, die in erster Linie Ermächtigungen für die EU-Kommission enthalten, wurden bereits zu früheren Zeitpunkten wirksam (Art. 52 Abs. 2 a), einige Vorschriften gelten erst

254 *Bundesrechtsanwaltskammer*, Presseerklärung 12/2016.
255 Vgl. hierzu bereits oben unter 2.3.2.
256 Erwägungsgrund 9 eIDAS-VO; vgl. hierzu auch *Lapp* in *Auer-Reinsdorff/Conrad*, § 30 Rn. 93.
257 *Roßnagel*, Vertrauensdienste, 16.
258 Abl. L 257/73.

ab späteren Zeitpunkten, die an den Erlass der Durchführungsrechtsakte gekoppelt sind (Art. 52 Abs. 2 b, c). Mit dem 1. Juli 2016 wurde nach Art. 50 Abs. 1 eIDAS-VO durch die Verordnung auch die EU-Signaturrichtlinie (RL 1999/93/EG) aufgehoben, wobei alle Verweise auf die Signaturrichtlinie ab diesem Zeitpunkt nach Art. 50 Abs. 2 eIDAS-VO als solche auf die eIDAS-VO gelten sollen.

Die Verordnung bedient sich an zahlreichen Stellen sogenannter delegierter Durchführungsrechtsakte, zu denen die Kommission ermächtigt wird. Diese Konstruktion wurde teilweise in der Literatur kritisiert.[259] Neben Vorschriften zu elektronischen Signaturen, die die Regelungen im Signaturgesetz ersetzen, enthält die eIDAS-Verordnung auch Regeln für weitere Techniken, die der Sicherheit elektronischer Kommunikation dienen. So führt es analog zu elektronischen Signaturen mit Art. 35 – 38 eIDAS-VO auch „elektronische Siegel“ ein, die die Regelungen zu qualifizierten elektronischen Signaturen auch für juristische Personen anwendbar machen, indem bei diesen auf den notwendigen Personenbezug verzichtet wird. Auch wird eine Technik für die die Eingangsbestätigung elektronischer Kommunikation – „elektronische Einschreiben“, Art. 3 Nr. 36 eIDAS-VO – geregelt und in Art. 3 Nr. 16a eIDAS-VO als eine mögliche Dienstleistung von Vertrauensdiensteanbietern genannt, jedoch ohne technische oder rechtliche Rahmenbedingungen für diese weiter auszuführen. Art. 43 f. eIDAS-VO enthalten lediglich rudimentäre rechtliche Regelungen für elektronische Einschreiben, sie sehen in Art. 43 Abs. 1 eIDAS-VO ein Benachteiligungsverbot sowie eine Vermutung der Unversehrtheit der Daten, der richtigen Identität von Absender und Empfänger und die Korrektheit von Datum und Uhrzeit von Versendung und Empfang vor (Art. 43 Abs. 2), sofern das elektronische Einschreiben nach Art. 44 eIDAS-VO durch einen qualifizierten Diensteanbieter übermittelt wurde.

Beinahe systemfremd wirken die Ausführungen zur Website-Authentifizierung in Art. 45 i.V.m. Anhang IV eIDAS-VO, da hierbei abstrakte Anforderungen an entsprechende Zertifikate aufgestellt werden, ohne sich zum Verhältnis zu bereits existierenden Techniken wie SSL/TLS[260] oder zu Fragen der technischen Realisierbarkeit und der Akzeptanz durch die Nutzer einzulassen. Derlei Erwägungen wären jedoch gerade für ein – im Gegensatz zu elektronischen Signaturen – völlig neues Regelungsfeld wie Website-Authentifizierung unerlässlich gewesen.

Schließlich enthält die eIDAS-VO in Art. 41 und 42 auch Vorschriften für elektronische Zeitstempel. Hier besteht insoweit eine Überschneidung mit dem Signaturgesetz, als dass elektronische Zeitstempel zwar im Signaturgesetz, nicht jedoch in der zugrundeliegenden EU-

259 So z.B. *Spindler/Rockenbauch*, MMR 2013, 139, 140; *Roßnagel/Johannes*, ZD 2013, 65.
260 Vgl. hierzu oben unter 2.3.1.2.

Signaturrichtlinie geregelt waren.[261] Für qualifizierte Zeitstempel gilt nach Art. 41 Abs. 2 eIDAS-VO die Vermutung der Richtigkeit des Datums und der Zeit sowie der Unversehrtheit der mit dem Zeitstempel versehenen Daten. Qualifizierte Zeitstempel müssen hierfür nach Art. 42 Abs. 1 eIDAS-VO Datum und Zeit mit den „gestempelten" Daten verknüpfen sowie auf einer mit der koordinierten Weltzeit verknüpften Zeitquelle beruhen und durch eine fortgeschrittene elektronische Signatur, ein fortgeschrittenes elektronisches Siegel oder einem gleichwertigen Verfahren unterzeichnet sein. Im Vergleich zum Signaturgesetz ist hiermit eine Konkretisierung der Anforderungen an elektronische Zeitstempel erfolgt. Insbesondere die Anforderung ein einen Abgleich mit der koordinierten Weltzeit erscheint zielführend, da eine Zeitangabe überhaupt nur in Verbindung mit der Zeitquelle und (gegebenenfalls) Begleitinformationen wie der betreffenden Zeitzone eine klärende Wirkung haben kann. Der Verweis auf eine einheitlich geltende Universalzeit ist deswegen zu begrüßen, da er eventuelle Auslegungsschwierigkeiten bei der Würdigung von Zeitstempeln beseitigen kann.

Durch die unmittelbare Anwendbarkeit und die gleichzeitige Aufhebung der EU-Signaturrichtlinie ergab sich das Problem, dass Umsetzungen der Signaturrichtlinie im nationalen Recht, wie sie beispielsweise das deutsche Signaturgesetz darstellt, in Teilen unanwendbar wurde. Aufgrund einer zum Teil an der Verordnung kritisierten Unterkomplexität[262] blieben jedoch viele Lücken bestehen, die durch nationales Recht gefüllt werden konnten und mussten.

Um die durch die Unanwendbarkeit bestimmter nationaler Regelungen in Verbindung mit der Allgemeinheit der eIDAS-Verordnung entstandenen Regelungslücken zu füllen, wurde am 18. Juli 2016 das eIDAS-Durchführungsgesetz erlassen, das als wesentlichen Bestandteil das Vertrauensdienstegesetz enthält.[263] DasVertrauensdienstegesetz beschränkt sich darauf, in der eIDAS-Verordnung wahrgenommene Lücken zu ergänzen. Er enthält selbst keine Einschränkungen hinsichtlich seines Anwendungsbereichs, wodurch hierfür die gleichen Beschränken wie bei der eIDAS-VO selbst gelten.[264] Durch das eIDAS-Durchführungsgesetz traten zudem ab dem Zeitpunkt seines Inkrafttretens das Signaturgesetz und die Signaturverordnung außer Kraft.[265] Hiermit setzt das eIDAS-Durchführungsgesetz faktisch eine seitens der Wissenschaft vorgeschlagene Gestaltungsmöglichkeit um, bei der auch nicht durch die eIDAS-Verordnung unanwendbar gewordene Vorschriften aus Signaturgesetz und Signaturverordnung durch ein dann in Verbindung mit der eIDAS-Verordnung einheitlich geltendes Vertrauensdienstegesetz und eine dieses

261 *Roßnagel*, Vertrauensdienste, 25.
262 So beispielsweise *Roßnagel*, Vertrauensdienste, 18 f.
263 Vgl. hierzu bereits oben unter 2.3.2.
264 Vgl. hierzu auch *Bundesministerium für Wirtschaft und Energie*, Referentenentwurf VDG, 39 zu § 1 Abs. 1.
265 Vgl. zu dieser Thematik anhand des Referentenentwurfs bereits Johannes, ZD-Aktuell 2016, 05423, Abschnitt 2.

flankierende Rechtsverordnung ersetzt werden. Eine solche Gestaltung hat den deutlichen Vorteil, dass eine saubere, einheitliche Rechtsgrundlage ohne nationale Sonderwege geschaffen wird.[266]

3.2 Datenschutzrecht

Zum Verständnis des rechtlichen Rahmens, in dem sich der elektronische Rechtsverkehr bewegt, ist zudem die Kenntnis des Datenschutzrechts hilfreich. Da dieses geschaffen wurde, um der gesteigerten Bedrohung durch automatisierte Datenverarbeitung zu begegnen, ist eine Auseinandersetzung mit der Geschichte und den Auswirkungen des Datenschutzrechts sinnvoll, um den elektronischen Rechtsverkehr richtig einordnen zu können.

3.2.1 Völker- und Europarecht

Zunächst sollen die europarechtlichen Vorgaben im Bezug auf den Datenschutz untersucht werden. Zwar hat Deutschland mit dem Datenschutzgesetz des Landes Hessen (HDSG) vom 7.10.1970[267] das erste Datenschutzgesetz der Welt erlassen[268] – noch dazu in einer Zeit, in der das Thema Datenschutz anders als heute noch keinen großen Raum in der öffentlichen Wahrnehmung einnahm.[269] In der Zwischenzeit sind durch europäische und (sonstige) völkerrechtliche Rechtsakte jedoch zusätzliche Vorgaben entstanden. Diese haben zum einen das nationale Datenschutzrecht beeinflusst, machen zum anderen jedoch teilweise auch direkte Vorgaben für Datenschutz im weiteren Sinne. Die folgenden Rechtsquellen unterliegen keiner historischen Sortierung, sondern sind anhand ihrer Stellung in der Normenpyramide gegliedert.

3.2.1.1 Die Europäische Menschenrechtskonvention

Die Konvention zum Schutze der Menschenrechte und Grundfreiheiten (auch Europäische Menschenrechtskonvention oder EMRK genannt) normiert ein Recht auf Datenschutz zwar nicht ausdrücklich, ein solches wird aber als Bestandteil des Grundrechts auf Achtung des Privat- und Familienlebens gemäß Art. 8 Abs. 1 EMRK gesehen.[270] Zudem enthält Art. 8 Abs. 1 EMRK auch

266 *Roßnagel*, Vertrauensdienste, 128.
267 GVBl. I 625.
268 *Weichert* in *Däubler*/*Klebe*/*Wedde*/*Weichert*, Einleitung Rn. 4.
269 *Lewinski* in *Auernhammer*, Einleitung Rn. 20 f.
270 *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rn. 10.

einen Schutz der Kommunikation, der sich sowohl auf private als auch berufliche Betätigung erstreckt, beispielsweise auch auf Anwaltsakten.[271] Im Einzelnen ist umstritten, ob der Schutz von Kommunikation dem Begriff des Privatlebens oder dem Begriff der Korrespondenz zuzuordnen ist, was letztlich aufgrund des gleichen Schutzbereiches jedoch in der Praxis keine große Bedeutung haben dürfte.[272] Wenngleich ein Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention in Art. 6 Abs. 2 S. 1 EUV vorgesehen ist, ist ein solcher bislang noch nicht erfolgt, was insbesondere auf das Gutachten 2/13 des Europäischen Gerichtshofs[273] zurückzuführen sein dürfte, in dem dieser den Entwurf eines Beitrittsvertrags für mit dem Unionsrecht unvereinbar erklärt.[274] Als völkerrechtlicher Vertrag genießt die Europäische Menschenrechtskonvention in Deutschland jedoch gemäß Art. 59 Abs. 2 GG (einfachen) Gesetzesrang.[275] Gleichwohl berücksichtigt das Bundesverfassungsgericht in seiner Rechtsprechung bei der Auslegung von Grundrechten zum Teil auch die Europäische Menschenrechtskonvention und die dazu ergangene Rechtsprechung, wobei es einen diesbezüglichen Automatismus ablehnt.[276] In jedem Fall erlangen die Wertungen der Europäischen Menschenrechtskonvention damit auf der einfachgesetzlichen Ebene Bedeutung für den elektronischen Rechtsverkehr. Diese dürften jedoch angesichts konkreterer Regelungen mit Bezug zum Datenschutz in anderen Rechtsquellen, die im Folgenden dargestellt werden, eher gering sein.

3.2.1.2 Die EU-Grundrechtecharta

Mit Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 erlangte auch die Charta der Grundrechte der Europäischen Union verkündet (EU-Grundrechtecharta – GRCh) Rechtskraft.[277] Der durch den Vertrag von Lissabon neu gefasste Art. 6 Abs. 1 EUV erkennt die in der EU-Grundrechtecharta festgehaltenen „Rechte, Freiheiten und Grundsätze“ an und stellt die Grundrechtecharta auf eine Ebene mit den Verträgen.[278] Die Grundrechtecharta enthält im Gegensatz zur Europäischen Menschenrechtskonvention in Art. 8 Abs. 1 ein eigenes Grundrecht auf Schutz personenbezogener Daten. Ausweislich der offiziellen Begründung stützt sich der Artikel

271 *Uerpmann-Wittzack* in *Ehlers*, § 3 Rn. 5.
272 *Uerpmann-Wittzack* in *Ehlers*, § 3 Rn. 6.
273 Veröffentlicht in DÖV 2016, 36.
274 *Terhechte* in *Groeben*/*Schwarze*/*Hatje*, Vorbemerkung GRC, Rn. 13.
275 *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 3 Rn. 6.
276 *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 3 Rn. 8.
277 *Huber*, NJW 2011, 2385.
278 Diese ungewöhnliche Konstruktion erklärt sich aus dem vorangegangenen Versuch, zu einem europäischen Verfassungsvertrag zu gelangen, der letztlich scheiterte (*Terhechte* in *Groeben*/*Schwarze*/*Hatje*, Vorbemerkung GRC, Rn. 11).

dabei auf Art. 286 EGV, der mittlerweile durch Art. 16 AEUV und Art. 39 EUV ersetzt wurde.[279]

Schutzgut ist hierbei jedoch nicht nur eine Schutzpflicht der Mitgliedsstaaten, sondern zugleich ein Anspruch auf die Gewährleistung des freien Datenverkehrs.[280] Anknüpfungspunkt für den Schutz des Grundrechts aus Art. 8 Abs. 1 GRCh ist der Begriff der personenbezogenen Daten, der alle über eine (mindestens) bestimmbare natürliche Person existierenden Informationen erfasst, ohne allerdings Daten zu rein geschäftlichen Angelegenheiten ohne Personenbeziehbarkeit zu schützen.[281] Ob juristische Personen auch erfasst werden sollen, ist streitig.[282] Nach der neueren Rechtsprechung des EuGH sollen jedoch juristische Personen sich jedenfalls in soweit auf den Schutz des Art. 8 GRCh berufen können, wenn ihr Name eine oder mehrere natürliche Personen bestimmt.[283] Dieser Streit tangiert jedoch im Ergebnis den Datenschutz im elektronischen Rechtsverkehr im Hinblick auf Art. 8 GRCh nicht, da jedenfalls regelmäßig auch personenbezogene Daten von natürlichen Personen erfasst und übermittelt werden müssen, um am elektronischen Rechtsverkehr teilnehmen zu können. Jedenfalls für Daten von Mandanten und Zeugen stellt sich somit die Frage des wirksamen Datenschutzes. Aus der unmittelbaren Anwendung des Grundrechts ergibt sich zunächst ein Abwehranspruch gegenüber Datenerhebungen durch staatliche Stellen, im Wege der Drittwirkung des Grundrechts jedoch auch eine Einwirkung ins Privatrecht.[284] Große Beachtung fand die mittelbare Drittwirkung von (zumindest auch) Art. 8 GRCh durch das Urteil des Europäischen Gerichtshofs zum sogenannten „Recht auf Vergessenwerden“[285] anlässlich von Suchtreffern in der Internet-Suchmaschine Google.[286] Eine Anforderung an die Ausgestaltung des Datenschutzes findet sich in Art. 8 Abs. 2 GRCh, nach dem Daten nur für festgelegte Zwecke und mit Einwilligung des Betroffenen oder aufgrund einer gesetzlichen Grundlage erhoben werden dürfen. Für den elektronischen Rechtsverkehr ergibt sich aus dieser Konstruktion jedenfalls für unfreiwillige Betroffene einer Datenerhebung wie Zeugen oder Sachverständige keine generelle erlaubnis der Dantenerhebung- und Verarbeitung, da bei diesen Personen von einer Einwilligung jedenfalls nicht immer ausgegangen werden kann. Etwas anderes kann jedoch für die gesetzliche Grundlage gelten, auf der die Datenverarbeitung basiert. Unmittelbar verpflichtet aus der Grundrechtecharta sind gemäß Art. 51 Abs. 1 2. Hs. GRCh nur Organe und Einrichtungen der Europäischen Union, eine Verpflichtung der Mitgliedsstaaten ergibt sich „ausschließlich bei der

279 Abl. EU 2007 C 303/17, 20.
280 *Augsberg* in *Groeben*/*Schwarze*/*Hatje*, Art. 8 GRC Rn. 3.
281 Kingreen in Calliess/Ruffert, EU-GRCharta Art. 8 Rn. 11; *Augsberg* in *Groeben*/*Schwarze*/*Hatje*, Art. 8 GRC Rn. 6.
282 *Jarass in Jarass*, *Augsberg* in *Groeben*/*Schwarze*/*Hatje*, Art. 8 GRC Rn. 7.
283 EuGH, Urteil vom 9. 11. 2010, C-92, 93/09 = EuZW 2010, 939, 941 Rn. 53.
284 *Augsberg* in *Groeben*/*Schwarze*/*Hatje*, Art. 8 GRC Rn. 10.
285 EuGH, Urteil vom 13.5.2014, C-131/12 = NJW 2014, 2257.
286 *Augsberg* in *Groeben*/*Schwarze*/*Hatje*, Art. 8 GRC Rn. 10; zum Recht auf Vergessenwerden vgl. auch die Berichterstattung von *Wilkens*, Heise-Newsticker 13.5.2014.

Durchführung des Rechts der Union“. Zwar hat der Europäische Gerichtshof in der Vergangenheit dazu tendiert, den Anwendungsbereich weit auszulegen. So hat er beispielsweise im Urteil Åkerberg-Fransson[287] festgestellt, dass die in der Unionsrechtsordnung garantierten Grundrechte „in allen unionsrechtlicht geregelten Fragestellungen“ Anwendung fänden. Jedoch stehen dem eine restriktivere Interpretation durch den Europäischen Gerichtshof in jüngerer Zeit sowie Vorbehalte mitgliedsstaatlicher Gerichte wie des BVerfG[288] entgegen.[289] Für die Anwendbarkeit auf den elektronischen Rechtsverkehr ist deshalb zu beachten, dass eine Verletzung von Rechten aus der Grundrechtecharta grundsätzlich nur dann in Betracht kommt, wenn und soweit Gemeinschaftsrecht angewandt wird. Auf die Grundrechtecharta wird zwar ausdrücklich in der Datenschutzrichtlinie für Justiz und Inneres sowie im dritten Abschnitt der Neufassung des Bundesdatenschutzgesetzes[290] Bezug genommen. Die Regelungsmaterie dieser Vorschriften fällt jedoch nicht in den Betrachtungsbereich dieser Arbeit, weshalb sie hier keine Berücksichtigung finden kann. Außer in Fällen, in denen die Ausgestaltung nach europäischen Vorgaben erfolgt, wie es beispielsweise bei der qualifizierten elektronischen Signatur nach dem Signaturgesetz der Fall ist, dürfte somit eine Beurteilung nach der Grundrechtecharta nicht in Betracht kommen.

3.2.1.3 EG-Datenschutzrichtline

Schließlich war das Datenschutzrecht auf europäischer Ebene geprägt durch eine Reihe von Unions-Richtlinien. Da solche Richtlinien grundsätzlich keine unmittelbare Wirkung entfalten (Art. 288 Abs. 3 AEUV), bedurften diese jedoch der Umsetzung durch die Mitgliedsstaaten. Zu nennen ist hier zunächst die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie – DSRL).[291] Diese nahm bereits in den Mitgliedsstaaten existierende Regelungen zum Datenschutz auf, worunter auch solche des deutschen Bundesdatenschutzgesetzes in der Fassung von 1990 fielen, ohne dass man jedoch von einer Dominanz der deutschen Regelungen in der Richtlinie sprechen könnte.[292] Wesentliche Inhalte der

287 EuGH, Urteil vom 26.2.2013, ECLI:EU:C:2013:105.
288 Vgl. hierzu insbesondere BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/07 = BVerfGE 133, 277, in dem das Bundesverfassungsgericht die nach der Åkerberg-Fransson-Enscheidung bestehende weite Anwendung der EU-Grundrechte dahingehend einschränkt, dass rein sachliche Bezüge oder rein tatsächliche Auswirkungen auf das Unionsrecht als Anknüpfungspunkt nicht ausreichen sollen, vgl. Orientierungssatz 2b, Rn. 91.
289 Terhechte in Groeben/Schwarze/Hatje, GRC Vorbemerkung Rn. 16.
290 Dazu sogleich unter 3.2.1.6.
291 ABl. L 281 vom 23.11.1995, 31 – 50.
292 *Lewinski* in *Auernhammer*, Einleitung Rn. 32.

Datenschutzrichtlinie waren der Grundsatz der Zweckbindung sowie das Erfordernis von Transparenz im Hinblick auf Erhebung und Verarbeitung von Daten.[293] Die Richtlinie differenziert hinsichtlich der Datenverarbeitung – anders als das deutsche Bundesdatenschutzgesetz – nicht zwischen öffentlichen und privaten Stellen.[294] Der Begriff der Datenverarbeitung der Richtlinie ist weit zu verstehen, er umfasste auch die Erhebung und Nutzung von Daten (Art. 2 lit. b DSRL).[295] Darüber hinaus enthielt Art. 18 f. DSRL Meldepflichten gegenüber staatlichen Kontrollstellen und Art. 14 DSRL Gewährleistungen, dass auch bei rechtmäßigen Datenerhebungen und -verarbeitungen durch Betroffene Widerspruch eingelegt werden konnte, sofern hierfür überwiegend schutzwürdige Belange sprachen.[296] Schließlich verlangte Art. 17 DSRL geeignete technische und organisatorische Sicherheitsvorkehrungen für die Verarbeitung von Daten, wobei keine absolute Sicherheit gefordert wurde, sondern eine solche, die – unter Berücksichtigung des Standes der Technik und der hierdurch entstehenden Kosten – zum Risiko der Datenverarbeitung in einem angemessenen Verhältnis stand. Die Datenübertragung ins Ausland wurde in Art. 25 DSRL derart geregelt, dass eine Übermittlung in ein Drittland ohne hinreichendes („angemessenes“) Datenschutzniveau nicht zulässig war. Ausnahmen hierzu fanden sich in Art. 26 DSRL, insbesondere bei vorliegender Einwilligung des Betroffenen in die Datenverarbeitung oder mit Genehmigung des Mitgliedsstaates, wenn die verarbeitende Stelle in dem Drittland Garantien hinsichtlich des Grundrechts- und Datenschutzes des Betroffenen abgegeben hatte.

Die Richtlinie sah in Art. 32 Abs. 1 eine Umsetzung binnen drei Jahren vor, was ausgehend von dem Unterzeichnungstermin am 24.10.1995 als spätesten Umsetzungstermin in den Mitgliedsstaaten den 24.10.1998 bedeutete. Die Umsetzung durch den deutschen Gesetzgeber zögerte sich jedoch hinaus, die Neufassung des Bundesdatenschutzgesetzes trat erst am 22.5.2001 in Kraft.[297] Die Umsetzung im Bundesdatenschutzgesetz wurde zum Teil scharf kritisiert, da sie nur auf das nötigste beschränkt sei und zudem gegen Grundsätze wie Normenklarheit und Lesbarkeit verstoße.[298] Zudem war die Umsetzung der Richtlinie Gegenstand einer Rüge durch die Kommission sowie eines darauf folgenden Vertragsverletzungsverfahrens gegen Deutschland im Juli 2005. In diesem wurde die mangelnde Unabhängigkeit der in Art. 28 Abs. 1 S. 2 der Richtlinie vorgesehenen Kontrollstellen gerügt. Im März 2010 urteilte der Europäische Gerichtshof, dass Deutschland die Richtlinie falsch umgesetzt habe, da die in Deutschland eingerichteten

293 *Gola/Klug*, 18.
294 *Taeger/Schmidt* in *Taeger*/*Gabel*, Einführung Rn. 53.
295 *Taeger/Schmidt* in *Taeger*/*Gabel*, Einführung Rn. 53.
296 Vgl. hierzu auch Erwägungsgrund 45 der Richtlinie.
297 *Simitis* in *Simitis*, Einleitung Rn. 98.
298 *Simitis* in *Simitis*, Einleitung Rn. 91, Rn 100.

Kontrollstellen ihrerseits einer staatlichen Aufsicht unterworfen waren.[299]

Für die abstrakten Anforderungen an den elektronischen Rechtsverkehr trat die Bedeutung der Richtlinie wegen der nur mittelbaren Wirkung von EU-Richtlinien hinter den konkreten einfachgesetzlichen Umsetzungen wie dem Bundesdatenschutzgesetz zurück. Durch den Erlass der Datenschutzgrundverordnung wurde die Datenschutzrichtlinie mit Wirkung ab dem 25. Mai 2018 aufgehoben.[300] Die datenschutzrechtliche Beurteilung des elektronischen Rechtsverkehrs richtet sich damit nunmehr nicht mehr nach der Datenschutzrichtlinie und deren einfachgesetzlichen Umsetzungen, sondern vielmehr nach der Datenschutzgrundverordnung und der Neufassung des Bundesdatenschutzgesetzes als deren Konkretisierung.

3.2.1.4 EG-Datenschutzrichtlinie für elektronische Kommunikation

Eine weitere für einen Teilbereich des Datenschutzes relevante Richtlinie ist die 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 (Datenschutzrichtlinie für elektronische Kommunikation – TK-DatenschutzRL)[301], welche die vorher für diese Bereich erlassene und technisch überholte Richtlinie 97/66/EG[302] ersetzt.[303] Die Richtlinie regelt für den Telekommunikationsverkehr spezifische datenschutzrechtliche Fragestellungen wie die Gewährleistung von Betriebssicherheit von elektronischen Kommunikationsdiensten, die Vertraulichkeit elektronischer Kommunikation und Erhebung und Löschung von Verkehrsdaten. Sie ergänzt damit die EG-Datenschutzrichtline um bereichsspezifische Regelungen für elektronische Telekommunikation.[304] Anders als die EG-Datenschutzrichtlinie, die nur die Grundrechte natürlicher Personen schützt, zielt die Datenschutzrichtlinie für elektronische Kommunikation auch auf den Schutz berechtigter Interessen von juristischen Personen ab, soweit diese Teilnehmer elektronischer Kommunikation sind (Art. 1 Abs. 2 der Richtlinie). Eine Verpflichtung der Mitgliedsstaaten, den Schutz der Datenschutzrichtlinie auch auf juristische Personen zu erstrecken, soll hierin jedoch gerade nicht liegen.[305]

299 Urteil vom 9. März 2010, Az. C-518/07, ECLI:EU:C:2010:125.
300 Vgl. hierzu sogleich unter 3.2.1.6.
301 ABl. L 201 vom 31.7.2002, 37 – 47.
302 ABl. L 24 vom 30.1.1998, 1 – 8.
303 *Comans*, 96.
304 *Bodenschatz*, 238.
305 Erwägungsgrund 12 der Richtlinie.

Die Richlinie ist technikneutral formuliert, um eine möglichst hohe Zukunftssicherheit zu erzielen.[306] Kernbegriff der Richtlinie ist der des öffentlich zugänglichen elektronischen Kommunikationsdienstes, vgl. Art. 3 Abs. 1 TK-DatenschutzRL. Art. 4 Abs. 1 der TK-DatenschutzRL verpflichtet die Mitgliedsstaaten zu einer Gesetzgebung zur organisatorischen Sicherung dieser Dienste. Darüber hinaus enthält sie in Art. 5 Abs. 1 eine Verpflichtung für die Mitgliedstaaten zur Gewährleistung der Vertraulichkeit der über solche Dienste übertragenen Daten und verlangt in Art. 6 Abs. 1 die Anonymisierung oder Pseudonymisierung von sogenannten Verkehrsdaten, lässt hiervon jedoch Ausnahmen zu. Zu den Ausnahmen bestimmt Art. 13 Abs. 1 TK-DatenschutzRL, dass diese gemäß Art. 13 Abs. 1 der EG-Datenschutzrichtlinie „für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen“ geboten sein müssen. Hiermit eröffnet die TK-DatenschutzRL die Möglichkeit für Mitgliedsstaaten, eine Vorratsdatenspeicherung von Verkehrsdaten einzuführen.[307] Als konsequente Fortsetzung dieser rechtspolitischen Richtungsentscheidung wurde schließlich 2006 eine gesonderte EG-Richtlinie zur Vorratsdatenspeicherung erlassen, die jedoch keinen Bestand hatte.[308]

Die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation in nationales Recht erfolgte mit der Neufassung des Telekommunikationsgesetzes von 2004.[309]

Für den elektronischen Rechtsverkehr ist wie bei den Erwägungen zur Datenschutzrichtlinie oben zunächst festzustellen, dass mangels unmittelbarer Wirkung von Richtlinien in erster Linie die einfachgesetzlichen Umsetzungen der Richtlinie zu betrachten sind. In zweiter Linie kann dann geprüft werden, ob diese nationalen Umsetzungen möglicherweise gegen Regelungen der Richtlinie verstoßen. Inhaltlich ergibt sich die Relevanz der Richtlinie für den elektronischen Rechtsverkehr daraus, dass für diesen elektronische Kommunikationsdienste erforderlich sind. Da die Richtlinie nach Art. 3 Abs. 1 nur für Datenverarbeitung „in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen der Gemeinschaft“ gilt, stellt sich die Frage, ob die für den elektronischen Rechtsverkehr genutzten Dienste sich unter diese Gruppe subsumieren lassen. Dies ist unproblematisch gegeben, da die Abwicklung des elektronischen Rechtsverkehrs mit den Gerichten unabhängig von der verwendeten Technik jedenfalls auf die Nutzung des Internets und damit auch der Dienste der Internet Service Provider (ISPs) angewiesen ist. Diese fallen unstreitig in den Anwendungsbereich der Richtlinie, da

306 *Bodenschatz*, 239, ebenso *Gola/Klug*, 26.
307 *Gola/Klug*, 27.
308 Vgl. dazu unten unter 3.2.1.5.
309 BGBl I 1190.

sie öffentliche zugängliche Kommunikationsdienste sind, die in den öffentlichen Kommunikationsnetzen der Gemeinschaft bereitgestellt werden. Der Begriff der Kommunikationsdienste ist dabei weit zu verstehen, er erstreckt sich auf jedwede Art elektronischer Kommunikation.[310] Auch das Kriterium der Öffentlichkeit ist gegeben. Unschädlich ist hierbei, dass bestimmte Techniken für den elektronischen Rechtsverkehr selbst nur für eingeschränkte Benutzerkreise konzipiert sind.[311] Denn jedenfalls die Kommunikationsdienste, die auch das beA nutzt, sind öffentlich zugängliche Kommunikationsdienste.

Damit ist die Datenschutzrichtlinie für Telekommunikation auch bei Beurteilung des elektronischen Rechtsverkehrs zu berücksichtigen. Zwar treffen deren Vorschriften nicht direkt die Techniken für den elektronischen Rechtsverkehr, sie regulieren jedoch die für diesen Notwendigen Internetzugänge und damit die Anforderungen, die die Anbieter dieser Zugänge erfüllen müssen.

Zu Berücksichtigen ist, dass die Datenschutzrichtlinie für Telekommunikation durch die neue Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation – ePrivacy-VO)[312] ersetzt werden soll. Diese soll unter anderem die Regelungen der Datenschutzrichtlinie für elektronische Kommunikation an die neue Datenschutzgrundverordnung anpassen, Ziffer 1.1 des Kommissionsentwurfs.

3.2.1.5 EG-Richtlinie zur Vorratsdatenspeicherung

Am 15. März 2006 wurde die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates 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[313] (auch als Richtlinie über die Vorratsdatenspeicherung bezeichnet) unterzeichnet. Diese verpflichtete die Mitgliedsstaaten, eine gesetzliche Pflicht zur Speicherung von Verkehrsdaten und Standortdaten durch Anbieter öffentlicher elektronischer Kommunikationsdienste oder Betreiber von öffentlichen

310 *Büttgen* in *Hoeren*/*Sieber*/*Holznagel*, Teil 16.3, Rn. 23.
311 Ein Beispiel hierfür ist das besondere elektronische Anwaltspostfach, das nach dem durch das ERV-Gesetz neu eingefügten § 31a BRAO nur für eingetragene Rechtsanwälte eingerichtet werden soll.
312 Kommissionsentwurf vom 10. Januar 2017, COM/2017/010 final - 2017/03 (COD), abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017PC0010, zuletzt abgerufen am 18.12.2017.
313 ABl. L 105 vom 13.4.2006, 54 – 63.

Kommunikationsnetzen einzuführen. Dies stellte insofern einen Bruch mit der bisherigen Regelungsrichtung für den Datenschutz auf europäischer Ebene dar, als die bis dahin vorherrschenden Prinzipien der Datensparsamkeit, Datenvermeidung und Zweckbindung einer verdachtsunabhängigen pauschalen Speicherung weichen sollten.[314] Die Speicherfrist betrug dabei gemäß Art. 6 der Richtlinie zwischen sechs Monaten und zwei Jahren. Die Daten sollten gemäß Art. 4 der Richtlinie unter bestimmten Umständen an die zuständigen nationalen Behörden weitergegeben werden dürfen. Gegen die Richtlinie wurden – wie bereits gegen dieser vorangegangene nationale Vorstöße in Richtung einer Vorratsdatenspeicherung in Deutschland – sowohl auf deutscher als auch europäischer Ebene aus diversen Richtungen Kritik laut. In der Literatur wurde zunächst konstatiert, die Richtlinie sei formell rechtswidrig, da sie sich auf Art. 95 a.F. EGV stützte, der sich mit der Rechtsangleichung zu Gunsten der Errichtung und der Funktionsfähigkeit des Binnenmarkts befasst, statt auf die eigentlich einschlägigen Art. 29 ff. a.F. EUV, die die justizielle und polizeiliche Zusammenarbeit regeln.[315] Auch materiellrechtlich wurde die Richtlinie kritisiert. So wurde befürchtet, dass die vorgesehenen Beschränkungen auf Metadaten wie beispielsweise Standortdaten und Verkehrsdaten keine wesentliche Reduzierung der Eingriffsintensität mit sich brächten, da auch mit Metadaten umfangreiche Bewegungs- und Kommunikationsprofile der von der Vorratsdatenspeicherung erfassten Personen erstellt werden könnten.[316] Zudem wurde der grundsätzliche Ansatz, dass die erfassten Daten überwiegend von Personen stammen, die keinerlei Anlass für einen Grundrechtseingriff gegen Sie gegeben haben, scharf angegriffen.[317] Bedenken betrafen weiterhin Möglichkeiten zum Schutz der gespeicherten Daten vor Missbrauch und die Sicherung von Zeugnisverweigerungsrechten und anderen besonders geschützten Rechtspositionen wie z.B. der Pressefreiheit.[318] Befürworter der Richtlinie gaben an, diese stelle ein alternativloses Instrument zur Terrorismus- und Kriminalitätsbekämpfung dar.[319]

Auf Vorlagen des irischen High Court sowie des österreichischen Verfassungsgerichtshofs erklärte der Europäische Gerichtshof die Richtline mit Urteil vom 8. April 2014[320] für ungültig. In der Urteilsbegründung erkannte der Europäische Gerichtshof zwar an, dass die Ziele der Richtlinie (öffentliche Sicherheit und Bekämpfung von Terrorismus) als zulässige Ziele des Gemeinswohls in Frage kämen, jedoch einen so schwerwiegenden Eingriff in das Recht auf Schutz personenbezogener Daten gemäß Art. 8 Abs. 1 GRC wie er von der Richlinie vorgenommen werde

314 *Comans*, 101.
315 *Comans*, 112.
316 *Schmittmann/Kempermann*, AfP 2005, 254, 256; so im Ergebnis auch *Braum*, ZRP 2009, 174, 176.
317 *Leutheusser-Schnarrenberger*, ZRP 2007, 9, 11; ebenso *Puschke/Singelnstein*, NJW 2008, 113, 118.
318 *Gola/Klug/Reif*, NJW 2007, 2599, 2602.
319 *Schmittmann/Kempermann*, AfP 2005, 254.
320 EuGH, Urteil vom 8.4.2014, C-293/12, C-594/12, ECLI:EU:C:2014:238.

nicht rechtfertigen können. Durch die Erfassung aller elektronischen Kommunikationsmittel werde in die Grundrechte „fast der gesamten europäischen Bevölkerung“ eingegriffen. Die fehlende Differenzierung nach betroffenen Personen oder Kommunikationsvorgängen, das Fehlen von Ausnahmen und die fehlenden Beschränkungen der Zugriffsmöglichkeiten von ersuchenden Behörden auf die Daten und die pauschale Erfassung von Daten ohne Unterscheidung nach (erwartbarem) Nutzen mache diesen Eingriff so schwerwiegend, dass die Zielsetzung ihn nicht rechtfertigen könne.

Die Ungültigkeitserklärung entfaltete dabei eine Rückwirkung auf den Zeitpunkt des Inkrafttretens der Richtlinie, mithin den 3. Mai 2006. Für den elektronischen Rechtsverkehr hat die Richtlinie damit ebenfalls keine unmittelbare Bedeutung mehr.

Ungeachtet der Ungültigkeitserklärung der Richtlinie durch den EuGH hatte der deutsche Gesetzgeber im Dezember 2015 ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Vorratsdatenspeicherungs-Gesetz, VDS-G) erlassen.[321] Das Gesetz sieht in Artikel 2 Nr. 2 unter anderem die Ersetzung von §§ 113a und b TKG durch die Einfügung der neuen §§ 113a - 113g TKG-neu vor. Diese verpflichten Anbieter von Telefon- und Internetdiensten, Verkehrsdaten wie Rufnummern und Verbindungszeiten von Telefonierenden sowie IP-Adressen und zugewiesene Benutzerkennungen nach § 113b Abs. 1 Nr. 1 TKG-neu für zehn Wochen sowie Standortdaten, die sich aus der Funkzellennutzung von Mobiltelefonen ergeben, nach § 113b Abs. 1 Nr. 2 TKG-neu für vier Wochen zu speichern. Das Gesetz begegnete gerade im Hinblick auf die gegenläufige Rechtsprechung des EuGH starker Kritik.[322]

Nach § 150 Abs. 13 TKG-neu sollte die Speicherverpflichtung für die Adressaten der §§ 113b ff. TKG-neu ab dem 1. Juli 2017 greifen. Hiergegen hatte jedoch ein Internetprovider vor dem Verwaltungsgericht Köln geklagt. Nach Ablehnung des Erlasses einer einstweiligen Anordnung durch das Verwaltungsgericht Köln hatte die Klägerin Beschwerde vor dem Oberverwaltungsgericht Nordrhein-Westfalen eingelegt. Dieses gab der Beschwerde statt und stellte vorläufig fest, dass die Klägerin bis zum rechtskräftigen Abschluss des Haupsacheverfahrens nicht verpflichtet sei, die Telekommunikationsdaten Ihrer Kunden zu speichern.[323] Zur Begründung führte das Gericht aus, dass die in § 113a Abs. 1 i.V.m. § 113b enthaltenen Regelungen reichten im Hinblick auf die Rechtsprechung des EuGH zu Tele2 Servige AB und Watson (C-203/15 und C-698/15) nicht aus,

321 BGBl I, 2218.

322 So sieht *Roßnagel*, NJW 2017, 696, 697 die Vorratsdatenspeicherung in der derzeitigen Form endgültig als gescheitert an; ähnlich Ziebarth, ZUM 2017, 398, 405; anders jedoch *Sandhu*, EuR 2017, 453, 469, die einen erneuten Anlauf für eine Vorratsdatenspeicherung für möglich hält.

323 OVG Münster, Beschluss vom 22. Juni 2017, 13 B 238/17, abrufbar unter http://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2017/13_B_238_17_Beschluss_20170622.html, zuletzt abgerufen am 18.12.2017.

um den Eingriff durch die Datenspeicherung auf Personen zu beschränken, deren Daten geeignet sind, um zumindest einen mittelbaren Zusammenhang zu schweren Straftaten aufzuzeigen. Die Regelungen würden im Gegenteil eine allgemeine und unterschiedslose Speicherung sämtlicher Verkehrs- und Standortddaten nahezu aller Nutzer und für nahezu alle Kommunikationsmittel vorsehen.[324] Wenngleich das Urteil in der Hauptsache abzuwarten bleibt, ist auch für dieses zu erwarten, dass die Europarechtswidrigkeit der Regelungen erkannt und eine Umsetzungsverpflichtung dementsprechend verneint werden wird.

Dennoch besteht grundsätzlich die Möglichkeit, dass in Zukunft auf europäischer oder nationaler Ebene erneute Vorstöße in Richtung einer Vorratsdatenspeicherung erfolgen. Im Gespräch waren bisher schon Verfahren wie das sogenannte Quick Freeze, bei dem an sich flüchtige (d.h. vom TK-Anbieter zu löschende) Daten in einem konkreten Verdachtsfall auf Anordnung der Strafverfolgungsbehörden gespeichert und dann – ggf. durch Richtervorbehalt abgesichert – in die weiteren Ermittlungen einbezogen werden können.[325] Von solchen weiteren Vorstößen wäre möglicherweise auch der elektronische Rechtsverkehr betroffen, bei dem sich dann insbesondere die Frage stellen würde, wie zufällig miterfasste Daten von Unbeteiligten geschützt werden könnten und Zeugnisverweigerungsrechte und berufliche Verschwiegenheitspflichten beachtet werden können. Auch im Hinblick auf die ins Blickfeld der Öffentlichkeit geratene umfassende Ausspähung elektronischer Kommunikation durch Geheimdienste wie den US-Auslandsgeheimdienst NSA dürfte eine Neubewertung der Risiken einer Vorratsdatenspeicherung erforderlich sein, zumal die Schaffung zusätzlicher Datensammlungen weitere Ansatzpunkte für verdeckte Datenerhebungen durch solche Geheimdienste liefern würde.

3.2.1.6 Datenschutz-Grundverordnung

In Weiterentwicklung der bisherigen EU-Regelungen zum Datenschutz hat die EU-Kommission den Vorschlag einer EU-Datenschutz-Grundverordnung vorgelegt, der nach umfassenden Trilog-Verhandlungen in der am 27. April 2016 erlassenen Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-

324 OVG Münster, Beschluss vom 22. Juni 2017, 13 B 238/17, Rn. 80.

325 Dieses Verfahren wurde beispielsweise auch vom EU-Generalanwalt in seinen Schlussanträgen im Verfahren gegen die Richtlinie zur Vorratsdatenspeicherung als eine Alternative genannt; vgl. Schlussanträge des Generalanwalts Pedro Cruz Villalón vom 12. Dezember 2003, Rechtssache C-293/12, Rn. 142., abrufbar unter http://curia.europa.eu/juris/celex.jsf?celex=62012CC0293&lang1=de&type=TXT&ancre=, zuletzt abgerufen am 18.12.2017.

Grundverordnung – DSGVO)[326] mündete. Ausweislich der Erwägungsgründe 6 und 7 DSGVO soll diese Verordnung das europäische Datenschutzrecht an moderne Technologien und Verhältnisse anpassen. Anders als bei den bisherigen europäischen Rechtsakten zum Datenschutz, die als Richtlinien erlassen wurden, wurde hierfür das Rechtsinstrument der Verordnung gewählt, was die unmittelbare Geltung der Normen in jedem Mitgliedsstaat zur Folge hat, ohne dass noch nationale Umsetzungsakte erforderlich wären (Art. 288 Abs. 2 AEUV).

Die Entwicklung der Verordnung wurde von verschiedenen Interessengruppen intensiv begleitet, nicht zuletzt aufgrund des zeitlichen Zusammentreffens mit der öffentlichen Diskussion des Themas Datenschutz anlässlich diverser Datenschutzskandale.[327] Kritisiert wurden an den verschiedenen Verordnungsentwürfen unter anderem die auch bei der eIDAS-Verordnung anzutreffende Benutzung von delegierten Rechtsakten und Durchführungsrechtsakten,[328] das Festhalten am Erfordernis gesetzlicher Erlaubnistatbestände oder der Einwilligung für Datenverarbeitungen[329] sowie die beanspruchte weite räumliche Geltung der Verordnung.[330] Zum Teil wurde diesen Bedenken im Rahmen des Trilogs abgeholfen, beispielsweise durch die Reduzierung der Anzahl der delegierten Rechtsakte und Durchführungsrechtsakte.[331] Wesentliche Inhalte der nunmehr abgestimmten Datenschutz-Grundverordnung sind das wie das bereits in der EU-Datenschutzrichtlinie enthaltene Prinzip der Zulässigkeit einer Datenverarbeitung nur bei Einwilligung oder gesetzlichem Erlaubnistatbestand (Art. 6 Abs. 1 DSGVO),[332] das Marktortprinzip (Art. 3 Abs. 2 DSGVO), ein System von Sanktionen und abgestimmtem Vorgehen der einzelnen mitgliedsstaatlichen Aufsichtsbehörden[333] sowie ein Recht auf Übertragbarkeit der eigenen, bei einem Anbieter gespeicherten personenbezogenen Daten (Art. 20 DSGVO).[334] Auch ist in der Datenschutzgrundverordnung ein umfangreicheres Widerspruchsrecht gegen Datenverarbeitungen im Rahmen von Profiling normiert, das als Voraussetzung eine bloße Beeinträchtigung durch eine Datenverarbeitung mit rechtlichen oder wirtschaftlichen Folgen für den Einzelnen genügen lässt.[335]

Das EU-Parlament hat die Verordnung am 14. April 2016 beschlossen.[336] Gemäß Art. 99 DSGVO

326 Abl. L 119 vom 4.5.2016, 1.
327 *Albrecht*, CR 2016, 88, 89.
328 *Jaspers*, DuD 2012, 571; ebenso *Hornung*, ZD 2012, 99, 105.
329 *Härting*, BB 2012, 459, 466, der allerdings vom „Verbotsprinzip" spricht; Grundsätzliche Kritik an dieser Konstruktion im Datenschutzrecht findet sich beispielsweise bei *Bull*, Netzpolitik, 136 und *Schneider/Härting*, ZD 2016, 63, 64.
330 *Härting*, BB 2012, 459, 462; lobend hingegen äußert sich *Buchner*, DuD 2016, 155, 156, der durch das Marktortprinzip eine erhöhte Rechtssicherheit erwartet.
331 *Albrecht*, CR 2016, 88, 97.
332 *Roßnagel/Kroschwald*, ZD 2014, 495, 497.
333 *Albrecht*, CR 2016, 88, 95.
334 *Roßnagel*, DuD 2017, 561, 562.
335 *Albrecht*, CR 2016, 88, 93.
336 *Wybitul*, BB 2016, 1077.

treten die Regelungen in der Verordnung ab dem 20. Tag nach ihrer Veröffentlichung in Kraft. Da die Veröffentlichung im Amtsblatt der EU am 4. Mai 2016 erfolgte, tritt die Verordnung somit am 24. Mai 2016 in Kraft. Nach Art. 99 Abs. 2 DSGVO gilt sie jedoch erst ab dem 25. Mai 2018.

Die Datenschutzgrundverordnung beansprucht ab ihrem Inkrafttreten zum 25. Mai 2018 umfassende Geltung. Insbesondere ist der Bereich der Justiz nicht von ihren Wirkungen ausgenommen. Nach Art. 2 Abs. 2 DSGVO sind lediglich bestimmte Arten von Datenverarbeitungen ausgeschlossen, in die der elektronische Rechtsverkehr jedoch nicht fällt. Insbesondere lässt sich aus Art. 2 Abs. 2 lit. a DSGVO, nach dem Datenverarbeitungen im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, ausgenommen sein sollen, nicht herleiten, dass der Bereich der Justiz damit nicht erfasst ist. Nach Art. 4 Abs. 2 lit. j AEUV erstreckt sich der Bereich der geteilten Zuständigkeit der Union auf den Bereich des „Raum[s] der Freiheit, der Sicherheit und des Rechts“. Hierin enthalten ist auch eine Zuständigkeit für den Bereich des Zivilprozesses in Form der justiziellen Zusammenarbeit in Zivilsachen, Art. 81 ff. AEUV.[337] Hiervon geht erkennbar auch der europäische Verordnungsgeber aus, indem er in Erwägungsgrund 20 DSGVO die Tätigkeiten von Gerichten und anderen Justizbehörden ausdrücklich in den Anwendungsbereich der Datenschutzgrundverordnung einschließt.[338] Nichts anderes gilt durch die in Art. 55 Abs. 3 DSGVO enthaltene Bereichsausnahme von der Zuständigkeit der Aufsichtsbehörden für die Justiz „im Rahmen ihrer justiziellen Tätigkeit“. Hierin soll gerade keine Unanwendbarkeit der Datenschutzgrundverordnung für den Bereich der Justiz liegen, sondern lediglich die Ermöglichung einer Datenschutzrechtlichen Selbstkontrolle der Justiz.[339]

Damit gilt der Anwendungsvorrang der Datenschutzgrundverordnung auch für datenschutzrechtliche Regelungen, die den elektronischen Rechtsverkehr betreffen. Eine Beurteilung der Datenschutzkonformität des elektronischen Rechtsverkehrs muss somit nach dem 25. Mai 2018 zumindest auch anhand der Datenschutzgrundverordnung erfolgen.

Während durch die Datenschutzgrundverordnung die Vorschriften der EU-Datenschutzrichtlinie aufgehoben werden[340], gilt die Telekommunikations-Datenschutzrichtlinie gleichwohl als *lex specialis* weiter (Art. 95 DSGVO).[341] Für den Bereich des elektronischen Rechtsverkehrs ist damit zumindest hinsichtlich der Internetprovider, auf deren Diensten die elektronische Kommunikation

337 *Obwexer* in *Groeben*/*Schwarze*/*Hatje*, Art. 4 AEUV Rn. 28.
338 *Selmayr* in *Ehmann*/*Selmayr*, Art. 55 DSGVO Rn. 13.
339 *Selmayr* in *Ehmann*/*Selmayr*, Art. 55 DSGVO Rn. 13, ebenso *Eichler* in *Wolff*/*Brink*, Art. 55 DSGVO Rn. 11, *Boehm* in *Kühling*/*Buchner*, Art. 55 DSGVO Rn. 15.
340 Vgl. Art. 94 Abs. 1 DSGVO.
341 *Albrecht*, CR 2016, 88, 93, ebenso *Buchner*, DuD 2016, 155, 161.

aufbaut,[342] weiterhin die TK-Datenschutzrichtlinie bzw. deren einfachgesetzliche Umsetzung maßgeblich. Zudem wird die Datenschutzgrundverordnung von der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI[343] (Datenschutzrichtlinie für Justiz und Inneres) flankiert, die Datenschutzrechtliche Anforderungen für den Bereich des Sicherheitsrechts normiert. Zwar gilt diese Richtlinie auch für Gerichte, jedoch nur, soweit sie im Sicherheitsbereich tätig sind, mithin für den Bereich der Prävention und Repression.[344] Diese Richtlinie fällt somit nicht unter den in der vorliegenden Arbeit betrachteten Bereich.

Als ungünstig dürfte sich hinsichtlich des elektronischen Rechtsverkehrs der Zeitpunkt des Inkrafttretens der Datenschutzgrundverordnung erweisen, da dieser annähernd mit dem Zeitpunkt der verpflichtenden Einführung des elektronischen Rechtsverkehrs nach dem ERV-Gesetz zusammenfällt. Es ist deswegen zu erwarten, dass die Praxis des elektronischen Rechtsverkehrs in einer Zeit beginnt, in der gleichsam ein judikatives Vakuum herrscht, da es noch keine Rechtsprechung zu den neu in Kraft getretenen datenschutzrechtlichen Regelungen geben wird. Aufgrund der teilweisen Überschneidung mit bereits bestehenden Datenschutzregelungen können zwar gewisse Prognosen über Gerichtsentscheidungen hinsichtlich offener Datenschutzfragen getroffen werden, sicher ist die zukünftige Entwicklung deswegen jedoch keineswegs. Im Gegenteil ist davon auszugehen, dass die deutsche Rechtsprechung zu datenschutzrechtlichen Grundsätzen eben nicht einfach auf die Datenschutzgrundverordnung bzw. die kommende Neufassung der Datenschutzrichtlinie für elektronische Kommunikation übertragbar ist.[345] Aufgrund dieser Unsicherheiten ist anzuraten, dass die Länder von den Möglichkeiten, die Einführung des verpflichtenden elektronischen Rechtsverkehrs mit den Gerichten hinauszuzögern, regen Gebrauch machen. Auf der anderen Seite dürfte dies die unerwünschte Folge haben, dass sich die bereits erheblichen Investitionen der öffentlichen Hand in den elektronischen Rechtsverkehr durch die erwarteten Einspareffekte erst später realisieren lassen. Hier muss seitens der Länder eine umfassende Abwägung getroffen werden, die keinesfalls Folgekosten durch eventuelle datenschutzrechtlich notwendig werdende Änderungen an der ERV-Infrastruktur außer Acht lassen darf.

342 Vgl. hierzu oben unter 3.2.1.4.
343 RL (EU) 2016/680.
344 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-RL; vgl. hierzu auch *Bäcker/Hornung*, ZD 2012, 147, 149.
345 So zum Entwurf der Datenschutzgrundverordnung *Kramer*, DuD 2013, 380, 381.

3.2.2 Deutsches Verfassungsrecht

Das Grundgesetz kennt kein ausdrückliches Grundrecht auf Datenschutz.[346] Das Bundesverfassungsgericht hat jedoch in seiner Rechtsprechung verschiedene Grundrechte herausgearbeitet, die ein subjektives Recht auf den Schutz der eigenen personenbezogenen Daten verleihen. Durch die Datenschutzgrundverordnung ist der Bereich des Datenschutzes jedoch noch weiter in den Bereich europäischen Rechts gerückt, was im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts seit der Solange II-Entscheidung[347], die in der Folgezeit konkretisiert[348] wurde, die grundrechtliche Prüfungskompetenz des Bundesverfassungsgerichts in diesem Bereich stark begrenzt.[349] Die (verfassungsrechtliche) Geschichte des Datenschutzrechts aus deutscher Perspektive hilft jedoch dabei, die grundsätzlichen Erwägungen hinter bestimmten Ausformungen des einfachen Rechts zu verstehen. Aus diesem Grunde soll im Folgenden die grundrechtliche Entwicklung des Datenschutzes kurz vorgestellt werden.

3.2.2.1 Das Grundrecht auf Informationelle Selbstbestimmung

Ein solches, nicht ausdrücklich im Grundgesetz enthaltenes Grundrecht ist das Grundrecht auf Informationelle Selbstbestimmung. Dieses Grundrecht wurde vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil als Bestandteil des allgemeinen Persönlichkeitsrechts gemäß Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG herausgearbeitet. Sein wesentlicher Inhalt ist ein „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“[350]. Anlass des Urteils waren Verfassungsbeschwerden gegen das Volkszählungsgesetz von 1983. Das Bundesverfassungsgericht stellte im Urteil zunächst fest, dass die Befugnis des Einzelnen, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“[351], durch die moderne automatische Datenverarbeitung besonderen Schutzes bedarf.[352] Das Gericht leitete dies aus der (technisch) unbegrenzten Speicherdauer und schnellen Abrufbarkeit von personenbezogenen Daten sowie den Gefahren, die sich aus der Verknüpfung verschiedener Datensammlung ergeben, ab.[353] Dies sei

346 *Klink*, 56; ebenso *Ambs* in *Erbs/Kohlhaas*, § 1 BDSG Rn. 4.
347 BVerfG, Beschluss vom 22. Oktober 1986 = BVerfGE 73, 339 – Solange II.
348 BVerfG, Urteil vom 30. Juni 2009 = BVerfGE 123, 267 – Lissabon.
349 Vgl. hierzu ausführlich *Hoidn* in Europäische Datenschutz-Grundverordnung, § 2 Rn. 106.
350 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 3, Leitsatz 1.
351 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 41 f., Rn. 152.
352 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 42, Rn. 153.
353 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 42, Rn. 153.

insbesondere deswegen wichtig, da die Ausübung der Selbstbestimmung durch die Befürchtung, Daten hierüber könnten ohne Kontrolle durch den Betroffenen gesammelt und später gegebenenfalls gegen diesen verwendet werden, eingeschränkt sei.[354] Hierzu führte das Bundesverfassungsgericht aus: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[355] Zu den wesentlichen Erkenntnissen des Urteils gehört ebenfalls, dass es im Hinblick auf Verknüpfungsmöglichkeiten von Daten durch automatisierte (Weiter-)Verarbeitung von Daten keine von sich aus belanglosen Daten mehr gibt.[356]

Diese Erkenntnisse spiegeln sich ebenfalls im Bundesdatenschutzgesetz wieder. Darüber hinaus strahlt das Recht auf informationelle Selbstbestimmung auch in das einfache Recht aus, indem es die Anwendung und Auslegung einfachgesetzlicher Normen beeinflusst.[357] Auch einfachgesetzliche Regelungen für den elektronischen Rechtsverkehr müssen damit im Lichte der informationellen Selbstbestimmung ausgelegt und angewendet werden. Dies gilt umso mehr, da die Regelungen im Bundesdatenschutzgesetz und in den Datenschutzgesetzen der Länder Datenerhebungen und -verarbeitungen jedenfalls dann zulassen, wenn eine gesetzliche Erlaubnis hierfür vorliegt. Eine solche Erlaubnis, die sich auch aus den Regelungen zum elektronischen Rechtsverkehr ergeben kann, muss sich jedoch mindestens am Grundrecht auf informationelle Selbstbestimmung messen lassen.[358] Eine besondere Bedeutung ergibt sich bezüglich der informationellen Selbstbestimmung insbesondere für Daten Dritter, die nicht selbst Prozesspartei sind (beispielsweise Zeugen) und daher nur eingeschränkt oder gar nicht über ihr Recht auf informationelle Selbstbestimmung disponieren können.

3.2.2.2 Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Ebenfalls der Rechtsprechung des Bundesverfassungsgerichts entspringt das Grundrecht auf

354 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 42, Rn. 153.
355 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 41 f., Rn. 152.
356 BVerfG, Urteil vom 15. Dezember 1983 = BVerfGE 65, 44 f., Rn. 158.
357 *Jarass* in *Jarass*/*Pieroth*, Art. 2 Rn. 57.
358 Zu den einfachgesetzlichen Regelungen des Datenschutzes vgl. im Übrigen unten Abschnitt 3.2.3.1.

Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, das im Urteil des Bundesverfassungsgerichts vom 27. Februar 2008[359] herausgearbeitet wurde. Hintergrund waren Verfassungsbeschwerden gegen mehrere Vorschriften des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen in der Fassung vom 20. Dezember 2006, das in der gerügten Fassung unter anderem einen heimlichen Zugriff auf informationstechnische Systeme (sog. „Online-Durchsuchung“) erlaubte. Das Bundesverfassungsgericht stellte zunächst fest, dass informationstechnische Systeme mittlerweile allgegenwärtig sind und eine zentrale Stelle im Leben vieler Personen einnehmen, was umso mehr gilt, wenn diese Systeme vernetzt sind.[360] Auch die Verlagerung anderer Kommunikationsmedien in das Internet führt zu einer steigenden Bedeutung dieser Systeme.[361] Dem gegenüber steht jedoch eine große Komplexität solcher Systeme, die den Einzelnen beinahe schutzlos gegenüber Ausspähungs- und Manipulationsversuchen Dritter lässt. Hieraus folgt laut BVerfG ein erhebliches grundrechtliches Schutzbedürfnis, dem andere Grundrechte nur unzureichend Rechnung tragen.[362] So schützt Art. 10 GG zwar auch die (Tele)Kommunikation mittels informationstechnischer Systeme, nicht jedoch die Ergebnisse bereits abgeschlossener Kommunikation, soweit eigene Schutzmaßnahmen durch den Betroffenen möglich sind.[363] Art. 13 GG hingegen schützt zwar vor einem physischen Zugriff auf die Wohnung, nicht jedoch vor unkörperlichen Zugriffen auf informationstechnische Systeme in der Wohnung.[364] Schließlich ist auch das Recht auf informationelle Selbstbestimmung nicht ausreichend, da dieses nur vor einzelnen Datenerhebungen schützt, nicht jedoch vor dem Zugriff auf informationstechnische Systeme, der gleichwohl auf das Persönlichkeitsrecht des Betroffenen einen viel größeren Einfluss haben kann.[365]

Wichtig für die folgenden Betrachtungen ist insbesondere, welche Bedeutung das Bundesverfassungsgericht in diesem Kontext dem technischen Selbstschutz der Betroffenen beimisst. So erklärt es, dass sich das Gewicht des Grundrechtseingriffs durch die angegriffenen Normen dadurch erhöht, dass diese „unter anderem darauf angelegt und dazu geeignet [sind], den Einsatz von Verschlüsselungstechnologie zu umgehen“.[366] Das Bundesverfassungsgericht benennt damit die Nutzung von Verschlüsselung ausdrücklich als eine grundrechtsrelevante Maßnahme zum technischen Selbstschutz, deren Umgehung durch staatliche Stellen die Intensität des Grundrechtseingriffs noch erhöht. Hieraus ergibt sich allerdings nicht für alle Fälle bereits ein

359 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274.
360 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 178 ff.
361 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 181.
362 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 185 f.
363 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 190.
364 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 199 f.
365 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 205.
366 BVerfG, Urteil vom 27. Februar 2008 = BVerfGE 120, 274, Rn. 241.

subjektiver einklagbarer Anspruch auf staatliche Bereitstellung oder Förderung von Verschlüsselungstechnologien, da ein solcher jedenfalls an einer staatlichen Einschätzungsprärogative scheitern dürfte.[367]

Zudem kann das Grundrecht auf Gewährleistung auf Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts auch Verkehrssicherungspflichten Dritter eröffnen.[368] So müssen sich die Maßnahmen von Hard- und Softwareherstellern daran messen lassen, welche Maßnahmen sie zum Schutz der informationstechnischen Systeme Dritter sie ergreifen.[369] Für Hard- und Softwarelösungen für den elektronischen Rechtsverkehr bedeutet das insbesondere, Gestaltungsvarianten zu wählen, die Dritten kein Eindringen in jene Computersysteme, die zum Zugriff auf den elektronischen Rechtsverkehr genutzt werden, erleichtern oder ermöglichen.

Zu beachten ist allerdings, dass das Bundesverfassungsgericht die Nutzung als eigenes System voraussetzt, mithin – losgelöst von der sachenrechtlichen Beurteilung – auf die *Nutzung* eines Systems als eigenes abstellt.[370] Fraglich ist, ob hierdurch eine Beschränkung auf die private (im Gegensatz zur beruflichen) Nutzung des Systems beabsichtigt ist. Richtigerweise kann es hier jedoch nicht auf die beispielsweise im Steuerrecht nach § 3 Nr. 45 EStG anzutreffende Differenzierung zwischen privater und beruflicher Nutzung eines informationstechnischen Systems ankommen. Das Bundesverfassungsgericht stellte in der genannten Entscheidung vielmehr auf ein schutzwürdiges Vertrauen darauf ab, dass die im Betrieb eines informationstechnischen Systems anfallenden aussagekräftigen Nutzerdaten nicht in fremde Hände gelangen. Ein solches Vertrauen kann zwar in solchen Fällen nicht bestehen, in denen der Nutzer ein fremdes System nutzt, das (in einer für ihn mindestens erkennbaren Weise) auch derartige Informationen ohne sein Zutun überträgt. Eine solche Konstellation findet sich beispielsweise in Anstellungsverhältnissen, wenn der Arbeitgeber den Datenverkehr und die Nutzung eines informationstechnischen Systems wie beispielsweise eines Personalcomputers oder eines Diensthandys überwacht (eine solche Überwachung durch den Arbeitgeber kann jedenfalls dann zulässig sein, wenn dem Arbeitnehmer eine Privatnutzung des Anschlusses nicht oder nur eingeschränkt gestattet wird, da in einem solchen Fall statt der strengeren Vorschriften des Telekommunikationsgesetzes jene des Bundesdatenschutzgesetzes einschlägig sind[371]). Diese Konstellationen betreffen jedoch keinesfalls

367 *Gerhards*, 365 f.; Die Autorin weist jedoch auch darauf hin, dass im Hinblick auf verpflichtende staatliche Kommunikationstechnologien eine verfassungskonforme Ausgestaltung notwendig und eine klageweise Durchsetzung dieser im Einzelfall möglich sein dürfte (*Gerhards*, 366).
368 *Roßnagel/Schnabel*, NJW 2008, 3534, 3536.
369 *Roßnagel/Schnabel*, NJW 2008, 3534, 3536.
370 *Hornung*, CR 2008, 299, 303.
371 *Kruchen*, 140; zum ebenfalls zulässigen Zugriff auf nicht eindeutig als privat erkennbare Dateien des

alle Teilnehmer am elektronischen Rechtsverkehr, sondern allein angestellte Anwälte, und diese auch regelmäßig nur in größeren Sozietäten mit entsprechend fortgeschrittenen IT-Systemen und -prozessen und dort natürlich auch nur Eingriffe durch den Arbeitgeber selbst. Für Andere wie zum Beispiel Einzelanwälte dürfte bei Nutzung eines informationstechnischen Systems regelmäßig ein schutzwürdiges Vertrauen in dessen Vertraulichkeit und Integrität bestehen, zumal eine strikte Trennung zwischen beruflicher Nutzung und einer solchen Nutzung, die zur Erstellung eines umfassenden Persönlichkeitsprofils geeignete Daten anfallen lässt, regelmäßig nicht möglich sein wird. Der Schutzbereich des Grundrechts kann somit auch für professionelle Teilnehmer am elektronischen Rechtsverkehr eröffnet sein. Jedenfalls über eine Verkehrssicherungspflicht nach § 823 Abs. 1 BGB ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme somit zu berücksichtigen.

3.2.2.3 Das Telekommunikationsgeheimnis

Schließlich gibt es als Grundrecht mit Bezug zum Datenschutz noch das Telekommunikationsgeheimnis gemäß Art. 10 GG. Dieses wird in Art. 10 Abs. 1 Alt. 3 GG als Fernmeldegeheimnis bezeichnet, in der neueren Rechtsprechung des Bundesverfassungsgerichts jedoch in Anpassung an die veränderten technischen Gegebenheiten nunmehr Telekommunikationsgeheimnis genannt.[372] Das Grundrecht besteht dem Wortlaut nach aus den drei Bestandteilen Briefgeheimnis, Postgeheimnis, Fernmeldegeheimnis, stellt aber dennoch ein einheitliches Grundrecht dar.[373] Dabei erstreckt sich der Schutzbereich auf Nachrichten während des Kommunikationsvorgangs, sowie auf „ruhende“ Nachrichten, sofern sie sich außerhalb des Herrschaftsbereichs der Kommunikationspartner befinden (also beispielsweise E-Mails, die noch auf dem Server eines E-Mail-Anbieters gespeichert sind).[374] Der Schutzbereich von Art. 10 Abs. 1 Alt. 3 GG ist auch nicht auf bestimmte festgelegte oder gar nur auf die zur Zeit des Inkrafttreten des Grundgesetzes verfügbare Technologien beschränkt, sondern folgt einem für technische Weiterentwicklungen offenen Verständnis.[375] Damit ist nicht nur eine Anwendung auf bisher bereits

Arbeitnehmers auf einem Dienst-PC durch den Arbeitgeber vgl. LAG Hamm, Urteil vom 4. Februar 2004, Az. 9 Sa 502/03 = openJur 2011, 30913.

372 *Guckelberger* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 10 Rn. 21.

373 *Jarass* in *Jarass*/*Pieroth*, Art. 10 Rn. 1; vorsichtig bejahend auch *Schenke* in *Stern*/*Becker*, Art. 10 Rn. 20; ablehnend hingegen *Ogorek* in *Epping*/*Hillgruber*, Art. 10 Rn. 6, ebenso *Guckelberger* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 10 Rn. 6.

374 *Jarass* in *Jarass*/*Pieroth*, Art. 10 Rn. 7.

375 *Ogorek* in in *Epping*/*Hillgruber*, Art. 10 Rn. 38; *Guckelberger* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 10 Rn. 21.

unter den Schutzbereich des Grundrechts subsumierte Technologien wie die Telefonübertragung oder die E-Mail gewährleistet, sondern auch auf neue Technologien. Auch Dienste wie das elektronische Gerichts- und Verwaltungspostfach, dessen Ausprägung als besonderes elektronisches Anwaltspostfach oder die E-Mail-Alternative De-Mail lassen sich somit unter den Begriff der Telekommunikation im Sinne des Art. 10 GG subsumieren. Zwar unterfällt Kommunikation, die sich an einen nicht näher bestimmten Empfängerkreis richtet, nicht dem Grundrecht aus Art. 10 GG, geschützt ist nur die sogenannte Individualkommunikation.[376] Für den Bereich des elektronischen Rechtsverkehrs stellt dies jedoch keine Einschränkung dar, da bei diesem regelmäßig mit einzelnen, jedenfalls bestimmbaren Empfängern kommuniziert wird. Insoweit erfasst der Schutzbereich des Telekommunikationsgeheimnisses auch die Kommunikation im Rahmen des elektronischen Rechtsverkehrs.

Soweit der Schutzbereich des Art. 10 Abs. 1 GG reicht, geht dieser als lex specialis dem Grundrecht auf Schutz der informationellen Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor.[377] Art. 10 Abs. 1 GG schützt insbesondere im Gegensatz zum Recht auf informationelle Selbstbestimmung die Kommunikation über die von ihm erfassten Medien ohne Rücksicht auf die tatsächlichen Kommunikationsinhalte.[378] Auch der Anwendungsbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme tritt hinter der Anwendung von Art. 10 Abs. 1 GG zurück, soweit dessen Schutzbereich eröffnet ist.[379] Ein Verzicht auf den Schutz des Art. 10 Abs. 1 GG ist zwar möglich, allerdings erst dann wirksam, wenn dieser von allen Kommunikationsbeteiligten geteilt wird.[380] Geschützt werden vom Fernmeldegeheimnis sowohl die Inhalte der Kommunikation als auch die Vertraulichkeit sämtlicher äußeren Umstände dieser, beispielsweise Zeit, Häufigkeit und beteiligte Personen.[381] Genau wie die vorgenannten Grundrechte kann auch das Fernmeldegeheimnis Relevanz für den elektronischen Rechtsverkehr erlangen. Eine Beschränkung auf etwa private Nutzung oder Kommunikation, die die höchstpersönlichen Lebensbereich betrifft, gibt es für dieses gerade nicht. Eingriffe in dieses Grundrecht stehen unter Gesetzesvorbehalt, Art. 10 Abs. 2 GG. Für die Frage der Einsichtnahmemöglichkeit in Kommunikation, wie dies zum Beispiel durch die kurzzeitige Entschlüsselung von De-Mails zur Überprüfung auf Schadsoftware der Fall ist, kann zudem die Frage des (insoweit punktuellen) Grundrechtsverzichts Bedeutung erlangen. Zu beachten ist hierbei jedoch abermals, dass dieser von allen Kommunikationsbeteiligten ausgeübt werden muss, nicht

376 *Durner* in *Maunz*/*Dürig*, Art. 10 GG Rn. 92.
377 *Jarass* in *Jarass*/*Pieroth*, Art. 10 Rn. 2.
378 *Pagenkopf* in *Sachs*/*Battis*, Art. 10 Rn. 14a.
379 *Guckelberger* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 10 Rn. 6.
380 *Groß* in *Friauf*/*Höfling*, Art. 10 Rn. 32.
381 *Durner* in *Maunz*/*Dürig*, Art. 10 GG Rn. 86.

etwa nur von einer Partei. Darüber hinaus enthält Art. 10 GG auch eine staatliche Schutzpflicht gegen unbefugte Kenntnisnahme Dritter.[382] Hier kann für den elektronischen Rechtsverkehr deswegen eine staatliche Pflicht entstehen, für Schnittstellen und gegebenenfalls auch staatlich angebotene oder zertifizierte Produkte zur Nutzung des elektronischen Rechtsverkehrs möglichst sichere Standards zu setzen, um beispielsweise eine Spionage durch ausländische Geheimdienste oder nichtstaatliche Akteure mindestens zu erschweren.

Wie andere Grundrechte auch wirkt Art. 10 GG zudem im Wege einer Ausstrahlungswirkung auf die gesamte Rechtsordnung und beeinflusst so im Wege der verfassungskonformen Auslegung einfaches Gesetzesrecht, das das Grundrecht aus Art. 10 GG einschränken könnte.[383] Mithin ist der Schutz des Telekommunikationsgeheimnisses auch bei der Auslegung der Normen über den elektronischen Rechtsverkehr zu berücksichtigen.

3.2.3 Einfachgesetzliche Datenschutzregelungen

Der einfachgesetzlich ausgestaltete Datenschutz richtet sich zum einen nach dem Bundesdatenschutzgesetz und den jeweiligen Landesdatenschutzgesetzen, zum anderen aufgrund der Subsidiarität der Bundes- und Landesdatenschutzgesetze nach einer Vielzahl anderer Gesetze wie beispielsweise dem Telekommunikationsgesetz und dem Telemediengesetz. Datenschutzrechtliche Vorschriften finden sich zudem für den Bereich der Justiz auch in Prozessordnungen wie beispielsweise der Zivilprozessordnung[384] oder der Strafprozessordnung.[385] Auch können andere Gesetze Erlaubnisse zur Datenweitergabe oder -verarbeitung enthalten und insoweit den Anwendungsbereich des Bundesdatenschutzgesetzes verdrängen. Solche Regelungen finden sich beispielsweise für den elektronischen Rechtsverkehr im Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten. Im Folgenden soll auf die für den elektronischen Rechtsverkehr relevanten datenschutzrechtlichen Regelungen auf der Ebene des einfachen Rechts eingegangen werden. Hierbei ist zu beachten, dass durch das Inkrafttreten der Datenschutgrundverordnung mit dem 25. Mai 2018[386] durch den Anwendungsvorrang dieser das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze nur noch insoweit angewandt werden können, wie sie nicht im Widerspruch zur Datenschutzgrundverordnung stehen. Gleichwohl ist eine

382 *Guckelberger* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 10 Rn. 30; kritisch hingegen *Pagenkopf* in *Sachs*/*Battis*, Art. 10 Rn. 21.
383 *Schenke* in *Stern*/*Becker*, Art. 10 Rn. 59.
384 *Wullweber* in *Abel*, § 9 Rn. 3.
385 *Kesten* in *Abel*, § 10 Rn. 19.
386 Vgl. hierzu oben unter 3.2.1.6.

Darstellung des nationalen Datenschutzrechts hier unerlässlich. Denn zum einen fand die gesamte Entwicklung des elektronischen Rechtsverkehrs innerhalb dieses rechtlichen Rahmens statt, weshalb dieser zum Verständnis bestimmter Gestaltungsentscheidungen hilfreich ist. Zum anderen ist aufgrund der Neuheit der Datenschutzgrundverordnung zu erwarten, dass die Rechtsgrundsätze die zu den (auf der europäischen Datenschutzrichtlinie basierenden) deutschen Datenschutzgesetzen aufgestellt worden sind, in der ein oder anderen Form auch für die Auslegung der Datenschutzgrundverordnung herangezogen werden können, und sei es auch nur in Form historischer Rechtsauslegung.

3.2.3.1 Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Der Anwendungsbereich des Bundesdatenschutzgesetzes ist nach § 1 Abs. 2 Nr. 1, 2 BDSG bei jeder (d.h. nicht nur der automatisierten) Verarbeitung personenbezogener Daten durch eine öffentliche Stelle eröffnet. Zu öffentlichen Stellen im Sinne des § 1 Abs. 2 Nr. 1, 2 BDSG gehören gemäß § 2 Abs. 1 und § 2 Abs. 2 BDSG auch Organe der Rechtspflege und damit auch Gerichte, soweit sie Justizverwaltungsaufgaben oder Rechtsprechungsaufgaben wahrnehmen.[387] Das Bundesdatenschutzgesetz erfasst jedoch nur öffentliche Stellen des Bundes, für öffentliche Stellen der Länder ist es gemäß § 1 Abs. 2 Nr. 2 BDSG nur einschlägig, soweit die Landesdatenschutzgesetze keine diesbezüglichen Regelungen treffen. Die Länder haben von der Möglichkeit, für Organe der Rechtspflege vom BDSG abweichende Regelungen zu treffen, in unterschiedlichem Maße Gebrauch gemacht. Während die meisten Länder Organe der Rechtspflege vollständig in den Anwendungsbereich ihres jeweiligen Landesdatenschutzgesetzes aufgenommen haben, bestehen in den Landesdatenschutzgesetzen der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Saarland Einschränkungen dahingehend, dass das Landesdatenschutzgesetz nur auf den Bereich der Justizverwaltung Anwendung finden soll. Zum Teil sind in den Landesdatenschutzgesetzen nur einzelne Vorschriften für den Bereich der Rechtsprechung ausgeklammert. Eine Übersicht der jeweiligen landesrechtlichen Regelungen findet sich in der folgenden Tabelle:

Land	**Anwendbarkeit des LDSG auf Organe der Rechtspflege**	**Anwendbarkeit gemäß**	**Stand des Gesetzes**
Baden-Württemberg	Ja; §§ 10, 11, 27 – 32 nur für Gerichte in Verwaltungsangelegenheiten	§ 2 Abs. 3 LDSG	18. September 2000, zuletzt geändert durch Gesetz vom 3. Dezember 2013

387 *Schreiber* in *Plath*, § 2 BDSG Rn. 9.

Land	Anwendbarkeit des LDSG auf Organe der Rechtspflege	Anwendbarkeit gemäß	Stand des Gesetzes
Bayern	Ja; Abschnitt 4 + 5, Art. 9 nur in Verwaltungsangelegenheiten	Art. 2 Abs. 6 BayDSG	23. Juli 1993, zuletzt geändert durch Gesetz vom 22. Juli 2014
Berlin	Ja	§ 2 Abs. 1 BlnDSG	17. Dezember 1990, zuletzt geändert durch Gesetz vom 16. Mai 2012
Brandenburg	Soweit sie Verwaltungsaufgaben wahrnehmen; für Staatsanwaltschaften außer in Verwaltungsaufgaben nur Abschnitt 2 des Gesetzes	§ 2 Abs. 1 S. 2 BbgDSG	15. Mai 2008, zuletzt geändert durch Gesetz vom 27. Juli 2015
Bremen	Nur, soweit sie Verwaltungsaufgaben erfüllen	§ 1 Abs. 4 S. 1 BremDSG	4. März 2003, zuletzt geändert durch Gesetz vom 1.7.2013
Hamburg	Ja; keine Anwendung von §§ 5, 6 Abs. 1 Nr. 1 – 9, §§ 12 – 19 auf Gerichte im Rahmen der Rechtspflege	§ 2 Abs. 1 S. 1 Nr. 1, Abs. 5 S. 1 Nr. 1 HmbDSG	5. Juli 1990, zuletzt geändert durch Gesetz vom 5. April 2013
Hessen	Ja	§ 3 Abs. 1 HDSG	7. Januar 1999, zuletzt geändert durch Gesetz vom 20. Mai 2011
Mecklenburg-Vorpommern	Nur, soweit sie Verwaltungsaufgaben wahrnehmen; für Staatsanwaltschaften außer in Verwaltungsaufgaben nur eingeschränkt	§ 2 Abs. 4 S. 2 DSG M-V	28. März 2002, zuletzt geändert durch Gesetz vom 20. Mai 2011
Niedersachsen	Ja	§ 2 Abs. 1 S. 1 NSDG	29. Januar 2002, zuletzt geändert durch Gesetz vom 12. Dezember 2012
Nordrhein-Westfalen	Soweit sie Verwaltungsaufgaben wahrnehmen; für Staatsanwaltschaften außer in Verwaltungsaufgaben nur Abschnitt 2 des Gesetzes	§ 2 Abs. 1 S. 2 DSG NRW	9. Mai 2000, zuletzt geändert durch Gesetz vom 2. Juni 2015
Rheinland-Pfalz	Ja	§ 2 Abs. 1 S. 1 Nr. 2 LDSG	5. Juli 1994, zuletzt geändert durch Gesetz vom 20. Dezember 2011
Saarland	Nur, soweit sie Verwaltungsaufgaben wahrnehmen; für Staatsanwaltschaften außer in Verwaltungsaufgaben nur Abschnitt 2 des Gesetzes	§ 2 Abs. 1 S. 4 SDSG	24. März 1993, zuletzt geändert durch das Gesetz vom 18. Mai 2011
Sachsen	Ja	§ 2 Abs. 1 S. 1 SächsDSG	10. Juli 2003, zuletzt geändert durch Gesetz vom 9. Mai 2015
Sachsen-Anhalt	Ja	§ 3 Abs. 1 S. 1 DSG LSA	18. Februar 2002, zuletzt geändert durch Gesetz vom 21. Juli 2015
Schleswig-Holstein	Ja	§ 3 Abs. 1 LDSG	9. Februar 2000, zuletzt

Land	Anwendbarkeit des LDSG auf Organe der Rechtspflege	Anwendbarkeit gemäß	Stand des Gesetzes
			geändert durch Gesetz vom 16. März 2015
Thüringen	Ja	§ 2 Abs. 1 ThürDSG	10. Oktober 2001, zuletzt geändert durch Gesetz vom 30. November 2011

Tabelle: Übersicht der Anwendbarkeit der Landesdatenschutzgesetze auf Organe der Rechtspflege (eigene Darstellung)

Trotz der unterschiedlichen Rechtsquellen wird im Folgenden schwerpunktmäßig auf die Anforderungen nach Bundesdatenschutzgesetz eingegangen, da die Landesdatenschutzgesetze – die wie das Bundesdatenschutzgesetz durch die EG-Datenschutzrichtlinie beeinflusst worden sind – materiellrechtlich im wesentlichen mit dem Bundesdatenschutzgesetz übereinstimmen. Bei relevanten Abweichungen zwischen Bundesdatenschutzgesetz und landesrechtlichen Regelungen wird an der jeweiligen Stelle darauf eingegangen. Aufgrund des Erlasses der Datenschutz-Grundverordnung[388] dürften Diskrepanzen zwischen Bundes- und Landesdatenschutzgesetzen zudem ab Inkrafttreten der Verordnung an Bedeutung verlieren, da von der Verordnung abweichende Regelungen jedenfalls dann nicht mehr angewendet werden dürfen, wenn sie dem Regelungsbereich der Verordnung unterfallen.[389] Eine unterschiedliche Umsetzung wie bei der Datenschutzrichtlinie ist aufgrund des Verordnungscharakters der DSGVO nicht mehr möglich.

Wie gezeigt wurde, ist das Bundesdatenschutzgesetz (bzw. je nach Land die Landesdatenschutzgesetze) auf die Justiz grundsätzlich anwendbar. Hierbei wird differenziert zwischen Justizverwaltung und Rechtsprechungsaufgaben. Für die Betrachtung des elektronischen Rechtsverkehrs ist hier vor allem die Wahrnehmung von Rechtsprechungsaufgaben maßgeblich. Der Bereich der Justizverwaltung wird jedoch insoweit berücksichtigt, als er die Voraussetzungen für die zur Rechtsprechung erforderliche Kommunikation zwischen Gerichten einerseits und den Verfahrensbeteiligten andererseits schafft. Die Einrichtung bzw. Bereithaltung von elektronischen Kommunikationswegen, auf denen prozesserhebliche Mitteilungen versandt werden können, ist zwar keine der Judikative zuzurechnende Aufgabe, aber dient einzig und allein dazu, die Rechtsprechungstätigkeit zu ermöglichen und findet insoweit hier Berücksichtigung.

Für den Bereich der Rechtsprechung gilt zwar das Prinzip der richterlichen Unabhängigkeit, eine datenschutzrechtliche Kontrolle durch den Datenschutzbeauftragten ist hier nicht vorgesehen, gleichwohl gelten natürlich auch für den Bereich der Rechtsprechung die materiellen Datenschutzvorschriften.[390] Zusätzlich zu jenen, die im Bundesdatenschutzgesetz bzw. den

388 Vgl. hierzu oben unter 3.2.1.6.
389 Vgl. hierzu oben unter 3.2.1.6.
390 Wullweber in Abel, § 9 Rn. 4.

Landesdatenschutzgesetz enthalten sind, ergeben sich weitere Anforderungen aus anderen Gesetzen wie den Prozessordnungen und anderen Gesetzen wie beispielsweise der Aktenordnung[391]. Aufgrund der verfassungsrechtlichen Stellung der Justiz können hier jedoch Kollisionen entstehen. Oft stehen dem Datenschutz z.B. grundrechtlich geschützte Rechtspositionen wie das Recht auf Akteneinsicht als Bestandteil des Anspruchs auf rechtliches Gehör gemäß Art. 103 Abs. 1 GG gegenüber.[392] In jedem Fall gelten aber die Datenschutzanforderungen von Bundes- bzw. Landesdatenschutzgesetz hinsichtlich der Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung.[393] So müssen beispielsweise elektronische Datenbestände verschlüsselt werden, sofern sie außerhalb der Räumlichkeiten der datenverarbeitenden Stelle verarbeitet oder wenn sie an eine andere Stelle übermittelt werden sollen.[394]

Auch Rechtsanwälte fallen unter den Begriff der Organe der Rechtspflege im Sinne des Bundesdatenschutzgesetzes, sie sind jedoch keine öffentlichen Stellen.[395] Gleichwohl werden sie nach § 1 Abs. 2 Nr. 3 BDSG als nicht-öffentliche Stellen vom Anwendungsbereich des Bundesdatenschutzgesetzes erfasst, „soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben“. Insoweit finden auf sie die §§ 27 ff. BDSG Anwendung.[396] Wenngleich die meisten Rechtsanwälte und Kanzleien in der Regel bereits heute Datenverarbeitungsanlagen im Sinne des Bundesdatenschutzgesetzes zur Speicherung oder Bearbeitung von Mandantendaten nutzen dürften, werden durch die Verpflichtung zur elektronischen Übermittlung von Daten neue Anwendungsfälle des Bundesdatenschutzgesetzes eröffnet, für die entsprechende technische und organisatorische Sicherungen und Rechtsgrundlagen vorhanden sein müssen. Zudem ist insbesondere für Datenverarbeitungen durch Rechtsanwälte das Bundesdatenschutzgesetz nicht abschließend, sondern wird zum Teil ergänzt und zum Teil verdrängt durch Regelungen des anwaltlichen Berufsrechts. Insbesondere ist hier das Spannungsverhältnis zwischen Bundesdatenschutzgesetz einerseits und der anwaltlichen Verschwiegenheitspflicht gemäß § 203 Abs. 1 Nr. 3, Abs. 3 StGB und § 43a BRAO andererseits hervorzuheben. Das genaue Verhältnis zwischen anwaltlicher Verschwiegenheit und Datenschutz nach Bundesdatenschutzgesetz ist höchst umstritten.[397] Nach einer Ansicht soll das Bundesdatenschutzgesetz aufgrund der Besonderheiten der anwaltlichen Arbeit und der Weite der anwaltlichen Verschwiegenheitspflicht weitestgehend hinter dem anwaltlichen Berufsrecht

391 Wullweber in Abel, § 9 Rn. 6.
392 Wullweber in Abel, § 9 Rn. 11.
393 *Bäumler/Nordmann* in *Abel*, § 8 Rn. 10.
394 Wullweber in Abel, § 9 Rn. 43.
395 *Gola/Klug/Körffer* in *Gola*/*Schomerus*, § 2 Rn. 12.
396 *Weichert* in *Däubler*/*Klebe*/*Wedde*/*Weichert*, § 2 Rn. 6.
397 *Dobmeier*, 23.

zurücktreten.[398] Andere vertreten die Auffassung, Bundesdatenschutzgesetz und anwaltliche Verschwiegenheitspflicht würden parallel gelten und bestimmte Datenverarbeitungshandlungen müssten demzufolge kumulativ den Voraussetzungen aus Bundesdatenschutzgesetz und Berufsrecht genügen, mit der Folge, dass das Bundesdatenschutzgesetz einen Mindeststandard vorgebe, der nur unterschritten werden dürfe, wenn die Wahrung des Berufsgeheimnisses es verlange.[399] Nach einer vermittelnden Ansicht tritt das Bundesdatenschutzgesetz nur insoweit hinter Regeln des anwaltlichen Berufsrechts zurück, als das Berufsrecht den identischen Lebenssachverhalt regelt. Das Bundesdatenschutzgesetz solle Regelungslücken füllen, dies sei jedoch nur denkbar, wo überhaupt solche bestünden.[400] Vertreter dieser Ansicht argumentieren, dass Bundesdatenschutzgesetz und anwaltliches Berufsrecht in Teilen so unterschiedliche Materien behandeln und von so separaten Interessenlagen ausgingen, dass sie in direktem Widerspruch zueinander geraten könnten. So würden manche Datenverarbeitungen, die nach Bundesdatenschutzgesetz zulässig wären, zugleich einen Verstoß gegen § 203 StGB begründen.[401] Auch die Informationspflichten sowie Berichtigungs- und Löschungsansprüche würden den Besonderheiten des Mandatsverhältnisses nicht gerecht, insbesondere eine Nutzung von Daten der Gegenseite könnten hier mittels Vorschriften aus dem Bundesdatenschutzgesetz durch diese so eingeschränkt werden, dass eine effektive Vertretung im Mandatsverhältnis nicht mehr möglich wäre.[402]

Nach richtiger Auffassung ist – wie von der vermittelnden Auffassung verlangt – eine differenzierte Betrachtung danach, welcher Sachverhalt von den jeweiligen Normen geregelt werden soll, anzustellen. Für die Sachverhalte, die bereits durch das anwaltliche Berufsrecht geschützt werden, tritt das Bundesdatenschutzgesetz im Wege der Subsidiarität hinter die berufsrechtlichen Regelungen zurück. Hiermit werden mögliche Schutzlücken vermieden, die eine pauschale Nichtanwendung des Bundesdatenschutzgesetzes eröffnen könnte, da die Regelungen im Bundesdatenschutzgesetz mehr Konstellationen erfassen als das Berufsgeheimnis abdeckt. Ansonsten wäre die paradoxe Folge hieraus, dass das Schutzniveau in Fällen, die noch nicht zu einer Verletzung des Berufsgeheimnisses ausreichen würden, gegenüber Datenverarbeitungen durch Nicht-Berufsgeheimnisträger reduziert wäre. Eine kumulative Anwendung der Vorschriften aus Bundesdatenschutzgesetz und Berufsrecht, wie sie die Gegenansicht vorschlägt, findet jedoch ihrerseits keine Stütze im Gesetz. So ordnet § 1 Abs. 3 BDSG ausdrücklich die Subsidiarität des

398 So *Rüpke*, 163, der sogar von einer Verfassungswidrigkeit und damit Teilnichtigkeit des BDSG bis auf §§ 5 und 9 BDSG wegen der Unvereinbarkeit des BDSG mit den Besonderheiten anwaltlicher Tätigkeit ausgeht.
399 *Dix* in *Simitis*, § 1 Rn. 186.
400 *Abel* in *Abel*, § 1 Rn. 19.
401 *Abel* in *Abel*, § 1 Rn. 24.
402 *Abel* in *Abel*, § 1 Rn. 29.

Bundesdatenschutzgesetzes gegenüber Berufsgeheimnissen an.[403]

Nach dem hier vertretenen Ergebnis wäre das Bundesdatenschutzgesetz auf Daten, die durch § 203 StGB oder § 43a Abs. 2 BRAO vor unbefugtem Offenbaren geschützt werden, hinsichtlich des Offenbarens nicht anwendbar. Damit wäre nach der Terminologie des Bundesdatenschutzgesetzes die Übermittlung als Unterfall der Verarbeitung im Sinne von § 3 Abs. 4 Nr. 3 BDSG von dessen Anwendungsbereich ausgenommen. Andere Verarbeitungen jedoch wie beispielsweise die Speicherung oder Erhebung, die nicht vom Anwaltsgeheimnis erfasst werden, wären nach wie vor über das Bundesdatenschutzgesetz geschützt, da die Pflicht zur anwaltlichen Verschwiegenheit hierfür gerade keine Regelungen trifft. Zudem wird der Schutz des Berufsgeheimnisses durch Zeugnisverweigerungsrechte (§ 160a StPO) sowie ein Beschlagnahmeverbot in § 97 StPO geschützt.[404] Dieser Schutz gilt gerade auch gegenüber staatlichen Organen, insbesondere ist der Anwalt auch verpflichtet, das Berufsgeheimnis gegenüber einem Datenschutzbeauftragten zu bewahren.[405] Durch § 43a BRAO sind auch – im Gegensatz zur bloßen Anwendung von § 203 StGB – Daten von Personen erfasst, die nicht Mandanten sind.[406] Andere Datenverarbeitungen, die entweder mangels Mandatsbezugs oder mangels einer Übertragung nicht unter die berufliche Verschwiegenheitspflicht fallen, können hingegen dem Bundesdatenschutzgesetz unterliegen. Allerdings ist auch dies nur dort der Fall, wo sich aus den Besonderheiten des Berufsrechts nichts anderes ergibt. Daher muss immer betrachtet werden, ob berufsrechtliche Besonderheiten einer Anwendung des Bundesdatenschutzgesetz im Einzelfall entgegenstehen würden. Ist dies nicht der Fall, ist das Bundesdatenschutzgesetz insoweit anwendbar.

Rechtsfolge der Anwendbarkeit des Bundesdatenschutzgesetzes ist der diesem konstruktiv zugrunde liegende Vorbehalt des Gesetzes oder der Einwilligung nach § 4 Abs. 1 BDSG.[407] Danach ist eine Datenverarbeitung im Sinne des Gesetzes nur zulässig, wenn entweder eine gesetzliche Erlaubnis – die sowohl aus dem Bundesdatenschutzgesetz selbst als auch anderen Gesetzen kommen kann – oder die Einwilligung des Betroffenen vorliegt. An die Einwilligung werden darüber hinaus spezielle Anforderungen gestellt. Das Bundesdatenschutzgesetz verlangt gemäß § 4a Abs. 1 eine

403 Zwar ist der Wortlaut „bleibt unberührt“ hinsichtlich des Schutzes von Berufsgeheimnissen missverständlich, jedoch geht aus der Gesetzesbegründung zum insofern wortgleichen BDSG 1990 klar hervor, dass „sowohl gesetzliche Regelungen als auch von der Rechtsprechung für besondere Geheimnisse (z.B. Arztgeheimnis) entwickelte Grundsätze den Regelungen des BDSG vorgehen“ (BT-Drs. 11/4306, 39); a.A. *Dix* in *Simitis*, § 1 Rn. 184.

404 *Träger* in *Feuerich/Weyland*, § 43a BRAO Rn. 13.

405 *Härting*, AnwBl 2011, 50, 51.

406 *Härting*, AnwBl 2005, 131, 132; ebenso *Träger* in *Feuerich/Weyland*, § 43a BRAO Rn. 16; a.A. *Redeker* in *Abel*, § 3 Rn. 12.

407 Dieser wird teilweise in der Literatur auch als Verbot mit Erlaubnisvorbehalt bezeichnet, beispielsweise von *Gola/Klug/Körffer* in *Gola/Schomerus*, § 4 BDSG Rn. 3; Kritik an diesem Begriff äußern beispielsweise *Scholz* und *Sokol in Simitis, § 4 BDSG Rn. 2.*

sogenannte informierte Einwilligung, d.h. die Einwilligung in Kenntnis des Zwecks der Datenverarbeitung sowie ggf. den Folgen einer Verweigerung der Einwilligung. Soll die Einwilligung schriftlich erteilt werden, ist sie sobald mehrere Erklärungen zeitgleich erfolgen sollen, besonders hervorzuheben. Dies hat beispielsweise bei Verträgen zur Folge, dass eine drucktechnische oder inhaltliche Hervorhebung des datenschutzrechtlichen Einwilligungsverlangens wie etwa durch Fettdruck oder eine gesonderte Überschrift verlangt wird.[408] Rechtsfolge einer Nichtbeachtung dieser Anforderung ist die Unwirksamkeit der Einwilligung und damit auch ihrer rechtfertigenden Wirkung.[409]

Auch im Falle einer Rechtfertigung der Datenverarbeitung sind dieser Grenzen hinsichtlich Ausgestaltung, Umfang und Absicherung gesetzt. So enthält § 3a BDSG das Prinzip der Datensparsamkeit, nach dem so wenige Datenerhebungen, -verarbeitungen und -nutzungen wie möglich zu tätigen sind. Hierzu sind die Daten nach § 3a S. 2 BDSG möglichst durch Anonymisierung oder Pseudonymisierung von den jeweils Betroffenen zu entkoppeln, soweit das möglich und nicht unverhältnismäßig ist. Anonymisierung beschreibt nach § 3 Abs. 6 BDSG hierbei die so vollständige Entfernung des Personenbezugs von Daten, dass eine Verbindung der Daten mit dem Betroffenen nicht mehr oder nur noch mit unverhältnismäßig großem Aufwand möglich ist. Pseudonymisierung hingegen ist nach § 3 Abs. 6a BDSG das Ersetzen der Daten, die einen Personenbezug herstellen lassen (wie beispielsweise des Namens einer Person), durch ein Kennzeichen, das dies nicht erlaubt. Im Falle einer Pseudonymisierung ist unter Umständen für den Kenner der Zuordnungsliste eine Rekonstruktion des Personenbezugs möglich.[410] Insgesamt ist der Prozess der Anonymisierung und Pseudonymisierung nicht unproblematisch, da durch moderne Verarbeitungsalgorithmen und die Verknüpfung mehrerer Datenquellen aus scheinbar anonymen Daten oft doch die Identität des Betroffenen rekonstruiert werden kann.[411]

Ebenfalls zu beachten ist das datenschutzrechtliche Erfordernis der Zweckbindung, das verbietet, Daten für andere Zwecke als die, für die sie erhoben wurden, zu verarbeiten.[412] Schließlich verlangt § 9 S. 1 BDSG auch das Ergreifen von technischen und organisatorischen Vorkehrungen, um die Daten abzusichern. In der Anlage zu § 9 Abs. 1 finden sich zwar die hiermit zu verfolgenden Zwecke wie beispielsweise Schutz vor unbefugtem Zutritt, Zugang und Zugriff (Nr. 1 – 3), ohne allerdings konkrete Maßnahmen zu benennen, die zur Gewährleistung dieser Ziele ergriffen werden sollen. Eine Ausnahme besteht in der ausdrücklichen Nennung von Verschlüsselung als Mittel, um

408 *Plath* in *Plath*, § 4a BDSG Rn. 43.
409 *Simitis* in *Simitis*, § 4a Rn. 42.
410 *Schreiber* in *Plath*, § 3 BDSG Rn. 62.
411 Vgl. zu dieser Problematik und zu Strategien, um einer Deanonymisierung entgegenzuwirken *Häder*, 9 ff.
412 *Gola/Klug*, 48.

die Zugangs- und Zugriffskontrolle sowie die Weitergabekontrolle durchzusetzen in Satz 3 der Anlage. Für die Praxis wichtige Normen zu Sicherheitsvorkehrungen finden sich jedoch für IT-gestützte Systeme in den entsprechenden Werken des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere in den IT-Grundschutz-Katalogen des BSI.[413]

Eine gewisse Lockerung des Datenschutzes als Zugeständnis an die Praxis wird mit der Möglichkeit der Auftragsdatenverarbeitung erreicht. Diese ist in § 11 BDSG geregelt und stellt eine Sonderregelung sowohl für denjenigen, der im Auftrag eines Anderen Daten verarbeitet, als auch den Auftraggeber dar. Der Beauftrage einer Auftragsdatenverarbeitung zählt nicht als Dritter im Sinne des Bundesdatenschutzgesetzes, weshalb nicht die Anforderungen an eine Übermittlung von Daten nach § 15, § 16 oder § 28 BDSG erfüllt werden müssen. Die Voraussetzung für diese Erleichterung ist jedoch, dass bestimmte in § 11 Abs. 2 BDSG normierte Voraussetzungen an den Auftrag erfüllt sein müssen. Im Gegenzug ist nach § 11 Abs. 4 BDSG nicht der Auftragnehmer, sondern der Auftraggeber verantwortlich für die Erfüllung der Vorschriften des Bundesdatenschutzgesetzes, Ansprüche des Betroffenen der Datenerhebung sowie Schadensersatzansprüche richten sich im Falle einer Auftragsdatenverarbeitung nur gegen den Auftraggeber.

Verstöße gegen die Datenschutzvorschriften des Bundesdatenschutzgesetzes können mit Bußgeldern (§ 43 BDSG) in Höhe bis 50.000 bzw. 300.000 Euro (§ 43 Abs. 3 BDSG, der zudem in Satz 2 eine Überschreitung dieses Höchstbußgelder ermöglicht, wenn diese nicht zur Gewinnabschöpfung ausreichen[414]) oder im Falle des als Straftatbestand ausgestalteten § 44 BDSG mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe geahndet werden.

Für die Datenverarbeitungen im Rahmen des elektronischen Rechtsverkehrs stellt sich bei einer Beurteilung nach Bundesdatenschutzgesetz und Landesdatenschutzgesetzen zunächst einmal die Frage, ob diese Regelungen überhaupt auf die Datenverarbeitungen anwendbar sind. Zu denken ist hier zuerst – neben den bereits thematisierten Regelungen zum Berufsgeheimnis bei Anwälten – an speziellere Vorschriften, die das Bundesdatenschutzgesetz in ihrem Anwendungsbereich verdrängen. Auch eine Einwilligung in die jeweiligen Datenverarbeitungen ist denkbar. Schließlich ist auch an das Vorliegen einer gesetzlichen Gestattung im Sinne des § 4 Abs. 1 BDSG zu denken.

Der elektronische Rechtsverkehr mittels EGVP in Form des beA erfordert mehrere Datenverarbeitungen im Sinne des Bundesdatenschutzgesetzes. Aus der hier betrachteten anwaltlichen Perspektive müssen personenbezogene Daten, die – oft noch nicht maschinell und

413 *Ernestus* in *Simitis*, § 9 Rn. 22.
414 *Becker* in *Plath*, § 44 BDSG Rn. 18.

somit grundsätzlich noch nicht im Anwendungsbereich des Bundesdatenschutzgesetzes – in der Regel vom Mandanten erhoben werden, zunächst einmal gespeichert werden. Personenbezogene Daten sind hierbei natürlich einmal jene des Mandanten selbst, die zur Begründung des Mandatsverhältnisses erhoben werden. Hierzu zählen beispielsweise Name, Anschrift und Kontaktdaten. Ebenfalls personenbezogene Daten werden aber regelmäßig auch innerhalb des vom Anwalt zu eruierenden Sachverhalts enthalten sein, bei denen es sich nicht unbedingt um solche des Mandanten selbst handeln muss. So müssen beispielsweise im Zivilprozess auch personenbezogene Daten der Gegenseite erhoben werden, beispielsweise um Forderungen gegenüber dieser geltend zu machen oder Klage zu erheben. Auch können personenbezogene Daten von anderen Beteiligten, Zeugen oder Sachverständigen betroffen sein. Für diese Datenerhebungen muss es nach dem Bundesdatenschutzgesetz entweder eine Einwilligung der Betroffenen geben, oder eine gesetzliche Erlaubnis. Nach der Erhebung der Daten müssen diese auch in eine Datenverarbeitungsanlage eingepflegt werden, das den Anwendungsbereich des Bundesdatenschutzgesetzes eröffnet. Denn wenngleich das Verwalten und Bearbeiten der Informationen, die ein Anwalt im Laufe des Mandats erlangt, nicht zwingend mittels eines Computers erfolgen muss, zwingt das Erfordernis der elektronischen Einreichung beispielsweise nach § 130d ZPO i.V.m. § 130a ZPO in den ab 1.1.2022 geltenden Fassungen Anwälte letztlich dazu, die personenbezogenen Daten in eine Datenverarbeitungsanlage einzuspeisen, soweit sie in den an das Gericht zu übertragenden Schriftsatz einfließen sollen. Für eine Verdrängung des Bundesdatenschutzgesetzes ist gemäß § 1 Abs. 3 S. 1 BDSG eine Norm erforderlich, die auf „personenbezogene Daten einschließlich ihrer Veröffentlichung“ anwendbar ist. Gemeint ist hiermit eine fach- und bereichsspezifische Rechtsnorm des Bundes.[415] Um eine solche handelt es sich bei den genannten Normen zum elektronischen Rechtsverkehr jedoch gerade nicht, da diese allenfalls als Reflex den Umgang mit personenbezogenen Daten betreffen, ohne jedoch eine Verdrängung des Bundesdatenschutzgesetzes zu bezwecken. Auch eine Rechtfertigung nach § 4 Abs. 1 BDSG, nach dem eine „andere Rechtsvorschrift“ die Datenverarbeitung erlaubt oder anordnet, ist in den genannten Vorschriften nicht zu sehen. Mit anderen Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG sind zum einen keine Bundesgesetze gemeint, die gleichrangig mit dem Bundesdatenschutzgesetz wären und somit schon über § 1 Abs. 3 BDSG dieses bereichsweise verdrängen könnten.[416] Zum anderen müssen auch diese Vorschriften die Verarbeitung von personenbezogenen jedenfalls konkret ansprechen.[417] Eine ausdrückliche datenschutzrechtliche Erlaubnis wird man hieraus jedoch nicht ableiten können,

415 *Gola/Klug/Körffer* in *Gola*/*Schomerus*, § 4 BDSG Rn. 7; *Dix* in *Simitis*, § 1 BDSG Rn. 170; zusammenfassend *Conrad* in *Auer-Reinsdorff*/*Conrad*, § 34 Rn. 111 ff.

416 *Gola/Klug/Körffer* in *Gola*/*Schomerus*, § 4 BDSG Rn. 7; ebenso *Scholz/Sokol* in Simitis, § 4 Rn. 8, die allerdings auf die praktische Unerheblichkeit dieser Differenzierung wegen des letztlich gleichen Ergebnisses hinweisen.

417 *Gola/Klug/Körffer* in *Gola*/*Schomerus*, § 4 BDSG Rn. 7, ebenso *Scholz/Sokol* in Simitis, § 4 Rn. 14.

da die Pflicht zur elektronischen Einreichung nicht ausdrücklich personenbezogene Daten in Bezug nimmt. In Frage kommt allerdings für Daten des Mandaten eine Rechtfertigung nach § 28 Abs. 1 Nr. 1 BDSG.[418] Zwar wird für die personenbezogenen Daten der Mandanten praktisch immer mindestens eine konkludente, regelmäßig aber im Rahmen der Mandatsvereinbarung auch ausdrücklich erteilte datenschutzrechtliche Einwilligung vorliegen. Hinsichtlich einer Einwilligung muss für den elektronischen Rechtsverkehr jedoch zwischen den verschiedenen Arten von Beteiligten unterschieden werden. Eine Einwilligung wird man nicht annehmen können bei unfreiwilligen Beteiligten wie beispielsweise (manchen) Zeugen, und auch eine mindestens konkludente Einwilligung von Sachverständigen in die Verarbeitung ihrer personenbezogenen Daten kann jedenfalls nicht immer vorausgesetzt werden. Daraus folgt, dass es für die Verarbeitung von personenbezogener Daten dieser Beteiligten einer gesetzlichen Grundlage bedarf. Da sich bei der Speicherung von Daten und spätestens bei Übermittlung von Schriftsätzen aber regelmäßig nicht nach solchen Personen, die eine datenschutzrechtliche Einwilligung erteilt haben, und solchen, bei denen das nicht der Fall ist trennen lässt, betrifft das Erfordernis einer datenschutzrechtlichen Rechtfertigung faktisch den gesamten Kommunikationsvorgang.

Als Rechtfertigungsgrund für die Datenverarbeitung kommt jedoch § 28 Abs. 1 Nr. 2 in Betracht. Hierfür ist erforderlich, dass die Datenverarbeitung für die Wahrung der berechtigten Interessen des Anwalts als verarbeitende Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse an einem Ausschluss der Verarbeitung durch den Betroffenen dieses überwiegt. In diese Abwägung müssen auch alle Erwägungen ziehen, die den Anwalt faktisch zu einer elektronischen Datenverarbeitung personenbezogener Daten zwingen, wie es bei der Einreichungspflicht für elektronische Dokumente der Fall ist. Das Interesse der Betroffenen wird hier auch regelmäßig nicht das Interesse eines gewissenhaften, im Einklang mit dem Berufsrecht agierenden Rechtsanwalts überwiegen, der auch berufsrechtlich verpflichtet ist, seinen Mandanten optimal zu vertreten.[419] Zudem ist der Anwalt nach berufsrechtlich nach § 43a Abs. 2 BRAO sowie § 2 BORA umfassend zur Verschwiegenheit verpflichtet, was zudem durch den strafrechtlichen Schutz aus § 203 StGB abgesichert ist. Datenschutzrechtlich ist die Verarbeitung von personenbezogenen Daten im Rahmen des Mandatsverhältnisses somit gedeckt. Dies ist auch konsequent, da schon aufgrund des strafrechtlich abgesicherten umfassenden Schutzes des Mandatsgeheimnisses keine unverhältnismäßige Gefährdung des Rechts auf informationelle Selbstbestimmung zu besorgen ist. Die Pflicht zur Benutzung des elektronischen Rechtsverkehrs erweitert damit zwar im Gegensatz zur früheren Lage, bei der nicht davon ausgegangen werden

418 So auch Rüpke, NJW 1993, 3097, 3098 noch zur bis zum 18.5.2001 gültigen Fassung des BDSG.
419 Vgl. § 1 Abs. 3 BORA.

musste, dass alle Anwälte personenbezogene Daten mittels Datenverarbeitungsanlagen verarbeiten, den Kreis der von den Pflichten aus dem Bundesdatenschutzgesetz tatsächlich getroffenen Personen. Hierdurch ist jedoch durch die Rechtfertigung der jeweiligen Datenverarbeitungen und den starken Schutz (auch) der personenbezogenen Daten im Rahmen des Mandatsgeheimnisses keine stärkere Gefährdung des Datenschutzes zu befürchten.

In jedem Fall für den elektronischen Rechtsverkehr zu beachten sind gleichwohl die Anforderungen an die Sicherung von gespeicherten Daten. Nach der hier vertretenen Ansicht zum Verhältnis zwischen Berufsgeheimnisschutz und Bundesdatenschutzgesetz würde letzteres nicht verdrängt werden, da das Berufsgeheimnis insofern keine Regelungen trifft, und für eine intendierte Lücke keine Anhaltspunkte erkennbar sind. Den Maßstab für die Datensicherheit bildet § 9 BDSG in Verbindung mit der dazugehörigen Anlage. Während viele der dort genannten Maßnahmen bereits für Datenverarbeitungen außerhalb des elektronischen Rechtsverkehrs galten, erhalten die Maßnahmen der Zugangskontrolle (Anlage zu § 9 BDSG, S. 2 Nr. 2), Zugriffskontrolle (Nr. 3) und Weitergabekontrolle (Nr. 4) besondere Bedeutung. Denn obgleich personenbezogene Daten im Mandatsverhältnis bereits heute von vielen Anwälten elektronisch gespeichert werden und damit auch den Anforderungen aus § 9 BDSG unterfallen, werden manche Aufzeichnungen innerhalb der anwaltlichen Tätigkeit bisher nur analog in der Handakte abgelegt. Dies wird sich jedoch spätestens mit der Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs zwingend ändern: Um die erwarteten Einspareffekte durch den elektronischen Rechtsverkehr zu realisieren ist zu erwarten, dass Kommunikationsvorgänge der Gerichte mit den Anwälten in Zukunft jedenfalls schwerpunktmäßig elektronisch erfolgen werden. Selbst wenn diese elektronischen Eingänge von den Kanzleien sofort ausgedruckt und dann gelöscht werden würden, ohne eine digitale Kopie in den Datenverarbeitungsanlagen der Kanzlei aufzubewahren, fände damit jedenfalls eine vorübergehende Speicherung der Daten statt, die den Anwendungsbereich von § 9 BDSG eröffnen würde. Auf der anderen Seite müssten Anwaltskanzleien jedenfalls solche Dokumente, die Teil eines Schriftsatzes an das Gericht werden sollen, elektronisch erstellen oder – im Falle von Drittmaterial wie beispielsweise Beweismitteln – analog eingehende Dokumente einscannen und sie so ebenfalls zum Teil einer (automatisierten) Datenverarbeitung im Sinne von § 9 BDSG zu machen.

Eine Maßnahme zur Umsetzung der Voraussetzungen aus Anlage zu § 9 BDSG S. 2 Nr. 2 – 4 wäre nach Satz 3 der Anlage insbesondere die Verwendung einer dem Stand der Technik entsprechenden Verschlüsselung. Zwar beschränkt § 9 S. 2 BDSG die Maßnahmen auf solche, die „erforderlich“ sind, um die Anforderungen der Anlage zu erfüllen, und schränkt den Begriff der Erforderlichkeit in

Satz 3 dahingehend ein, dass ein angemessenes Verhältnis zum Schutzzweck bestehen müsse. Angesichts der Verfügbarkeit von – auch kostenlosen – Verschlüsselungslösungen[420] dürfte diese Hürde jedoch kaum einmal Bedeutung erlangen. Technologien zur Datenträgerverschlüsselung sind heutzutage Bestandteil aller gängigen Betriebssysteme. So gibt es für die verbreiteten Windows-Betriebssysteme die Software „Bitlocker“, die jeweils ab den Ultimate-Versionen von Windows Vista und Windows 7 und ab den Pro-Versionen von Windows 8[421] bis einschließlich Windows 10[422] enthalten ist. Spiegelbildlich hierzu bringt MacOS mit FileVault 2 ebenfalls eine Verschlüsselungstechnologie mit,[423] und unter Linux lässt sich eine Datenträgerverschlüsselung mit Bordmitteln mittels LUKS und dm-crypt[424] realisieren. Darüber hinaus gibt es freie Softwarelösungen, die eine betriebssystemübergreifende Verschlüsselung erlauben. Der prominenteste Vertreter dieser Software ist VeraCrypt, das aus dem mittlerweile eingestellten TrueCrypt-Projekt hervorgegangen ist, und das kostenlos und quelloffen für Windows, MacOS und Linux verfügbar ist.[425] Auch die Verschlüsselung des gesamten Datenträgers, die naturgemäß auch nicht personenbezogene Daten erfasst, ändert an der Beurteilung der Verhältnismäßigkeit nichts, da die Nutzung weniger effektiver Sicherheitsvorkehrungen für geringer gefährdete Daten innerhalb des gleichen Systems eher einen administrativen Mehraufwand als eine Erleichterung für den Verarbeiter bedeuten würde. Die Verschlüsselung des gesamten (System-)Datenträgers hat zudem den Vorteil, dass auch vom Nutzer unbemerkt angelegte Dateien wie beispielsweise temporäre Sicherheitskopien von Dokumenten und auf die Festplatte ausgelagterter Arbeitsspeicher (bei Windows beispielsweise die Datei pagefile.sys) automatisch mitverschlüsselt werden und somit ein weiterer möglicher Angriffsvektor entfällt.[426] Damit sollte für „ruhende“ Daten eine Verschlüsselung der diese enthaltenden Datenträger (bzw. für eine erhöhte Sicherheit auch der Systemdatenträger des Computersystems, auf dem die Daten gespeichert, gelesen und weiterverarbeitet werden sollen) angestrebt werden.

Für Daten auf dem Versandweg sollte eine Ende-zu-Ende-Verschlüsselung der Daten benutzt werden,[427] um eine unbefugte Kenntnisnahme durch Dritte (einschließlich des die Nachricht weiterleitenden Diensteanbieters) auch technisch ausschließen zu können. Zwar ist Kritikern dieser

420 Vgl. dazu oben unter 2.3.1.3.
421 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge, 15. EL Stand 2016, M 4.337 Einsatz von BitLocker Drive Encryption.
422 https://www.microsoft.com/en-us/WindowsForBusiness/Compare, zuletzt abgerufen am 18.12.2017.
423 https://support.apple.com/de-de/HT204837, zuletzt abgerufen am 18.12.2017.
424 *Schmidt*, c't 11/2011, 192, 193.
425 *Schirrmacher/Mett*, c't 14/2016, 136, 137 f.
426 *Schmidt*, c't 11/2011, 192, 194 f.; der Autor bezieht sich in dem Artikel zwar auf Linux-Systeme, die Grundprinzipien wie Speicherorte von Systemdiensten und Auslagerungsdateien sind aber in allen gängigen Betriebssystemen gleich und bieten vergleichbare Angriffsflächen.
427 Vgl. hierzu auch die Erwägungen oben unter 2.3.1.3.

Ansicht zuzugeben, dass eine absolute Sicherheit weder erreichbar ist, noch vom Gesetz kaum jemals vorausgesetzt wird, sondern vielmehr stets eine Abwägung zwischen der Bedrohungslage und dem zur Sicherung erforderlichen Aufwand nötig sei.[428] Aus dieser Erkenntnis ist jedoch noch nicht abzuleiten, wie das Ergebnis einer solchen Abwägung aussehen müsste. Kritischer Punkt hierbei dürfte die Frage nach dem „Preis" einer Ende-zu-Ende-Verschlüsselung sein, sowohl in technischer und finanzieller Hinsicht als auch unter Benutzbarkeitsgesichtspunkten. Das Argument, eine verpflichtende Nutzung einer Ende-zu-Ende-Verschlüsselung sei im weiteren Sinne unverhältnismäßig, geht zumindest für jene Zielgruppe fehl, die zur Nutzung des elektronischen Rechtsverkehrs gesetzlich verpflichtet wird und die einem strengen Berufsgeheimnis unterliegt.

Dies gilt insbesondere für Daten, die dem Anwaltsgeheimnis unterliegen und auf die nach der hier vertretenen Auffassung das Bundesdatenschutzgesetz nicht anwendbar wäre. Für diese Daten würde man durch die insoweit strengeren Vorschriften in § 43a Abs. 2 BRAO und § 203 Abs. 1 Nr. 3 StGB erst Recht zum Ergebnis kommen, dass ohne die ausdrückliche Einwilligung des Mandanten in eine unverschlüsselte Kommunikation derartige Daten jedenfalls bei einer Übertragung per E-Mail nur in verschlüsselter Form versendet werden dürfen.[429]

Zur Anpassung an die neue Datenschutzgrundverordnung hat der deutsche Gesetzgeber am 30. Juni 2017 das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) verabschiedet.[430] Kern dieses Gesetzes ist ein komplett neues Bundesdatenschutzgesetz, das zeitgleich mit dem Geltungsbeginn der Datenschutzgrundverordnung in Kraft tritt, Art. 8 Abs. 1 DSAnpUG-EU). In § 5 BDSG-neu ist ausdrücklich bestimmt, dass das Gesetz keine Anwendung findet, soweit das Recht der Europäischen Union, insbesondere der Datenschutzgrundverordnung, unmittelbar gilt. Diese Regelung ist die direkte Konsequenz aus dem Anwendungsvorrang der Datenschutzgrundverordnung und damit rein deklaratorisch. Für die Beurteilung des elektronischen Rechtsverkehrs kann die Neufassung des Bundesdatenschutzgesetzes damit allenfalls zur Ausfüllung von Lücken, die die Datenschutzgrundverordnung nicht regelt, herangezogen werden. Alle anderen Sachverhalte beurteilen sich unmittelbar nach den Regelungen der Datenschutzgrundverordnung.

428 *Heckmann/Seidl/Maisch*, 63 f.
429 *Miedbrodt* in Handbuch Datenschutzrecht, Abschnitt 4.9 Rn. 40; in *Feuerich/Weyland*, § 43a Rn. 25b.
430 BGBl I, 2097.

3.2.3.2 Telekommunikationsrecht

Weitere Voraussetzungen für den elektronischen Rechtsverkehr hinsichtlich des Datenschutzes im weiteren Sinne ergeben sich aus Normen im Telekommunikationsgesetz und Telemediengesetz. Das Telekommunikationsgesetz enthält in seinem Teil 7 datenschutzrechtliche Regeln für Diensteanbieter. Als Diensteanbieter gilt hierbei nach § 3 S. 1 Nr. 6 TKG, wer ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an deren Erbringung mitwirkt. Eine Gewinnerzielungsabsicht ist hingegen nicht erforderlich.[431] Telekommunikationsdienste in diesem Sinne sind gemäß § 3 S. 1 Nr. 24 TKG Dienste, die ganz oder überwiegend in der Signalübertragung über Telekommunikationsnetze bestehen. Die Definition von Telekommunikationsnetzen wiederum ist umfangreich, für die folgende Betrachtung genügt jedoch die Erkenntnis, dass in der in § 3 S. 1 Nr. 27 TKG enthaltenen Definition auch explizit das Internet genannt wird. Beispiele für Telekommunikationsdienste sind unter anderem E-Mail-Übertragungsdienste.[432] Dies gilt jedoch nur so weit, wie es um die Übertragung von Signalen (nicht: deren Verarbeitung) geht.[433] Over-the-top-Dienste, d.h. solche Dienste, die auf einer vorhandenen Netzinfrastruktur aufsetzen, und die keinen eigenen Anteil an der Signalübertragung haben, fallen somit gerade nicht unter den Begriff der Telekommunikationsdienste im Sinne von § 3 S. 1 Nr. 24 TKG. Zwar wird zum Teil vertreten, dass sich Anbieter von Over-the-top-Diensten die Signalübertragung der Telekommunikationsunternehmen, auf deren Netze sie zugreifen, zurechnen lassen müssen.[434] Diese Lesart gibt jedoch der Gesetzestext des Telekommunikationsgesetzes selbst nicht her. Denn nach § 3 Nr. 6 TKG ist nur derjenige Diensteanbieter, der entweder nach lit. a Telekommunikationsdienste erbringt oder nach lit. b an der Erbringung solcher Dienste mitwirkt. Dass ein Anbieter von Over-the-top-Diensten nicht selbst Telekommunikationsdienste erbringt, d.h. als Nachrichten identifizierbare elektromagnetische oder optische Signale aussendet, empfängt oder übermittelt, ergibt sich daraus, dass dieser regelmäßig gar keine faktische Einflussnahmemöglichkeit auf physikalische Infrastruktur haben wird, die zur Signalübertragung benutzt wird. Ein Mitwirken an der Signalübertragung im Sinne von § 3 Nr. 6 lit. b TKG scheitert daran, dass dieses eine Umkehrung des Anbieter-Nutzer-Verhältnisses darstellen würde. Denn der Anbieter eines OTT-Dienstes ist auf die Funktionsfähigkeit der verwendeten Netzinfrastruktur angewiesen, umgekehrt ist dies jedoch gerade nicht der Fall. Aus der

431 *Fetzer* in *Arndt*/*Fetzer*/*Scherer*/*Graulich*, § 3 TKG Rn. 27.
432 *Fetzer* in *Arndt*/*Fetzer*/*Scherer*/*Graulich*, § 3 TKG Rn. 104.
433 *Schuster*, CR 2016, 173, 177.
434 So z.B. VG Köln, Urteil vom 20.2.2015, 12 O 186/13 = CR 2016, 129, *Kühling/Schall*, CR 2015, 641, 650 f. und KG Berlin, Urteil vom 21.5.2017, 21 U 9/16 = CR 2017, 454, 457 Rn. 78.

Abhängigkeit eines OTT-Anbieters eine Mitwirkung zu schlussfolgern, wäre deswegen unzutreffend. Die Verpflichtungen aus dem Telekommunikationsgesetz treffen deswegen für den Bereich des elektronischen Rechtsverkehrs nur die Anbieter der Netzinfrastruktur, mithin die Internet Service Provider (ISPs), nicht jedoch die Anbieter der Einreichungswege wie De-Mail oder das beA.

Hiervon zu trennen ist die Frage, ob auch eine Beurteilung der Dienste für den elektronischen Rechtsverkehr nach Telemediengesetz erforderlich ist. Hierfür müsste es sich bei diesen Diensten zumindest auch um Telemediendienste im Sinne des § 1 Abs. 1 TMG handeln. In § 1 Abs. 1 TMG ist der Begriff der Telemediendienste negativ definiert als elektronische Informations- und Kommunikationsdienste, die keine Telekommunikationsdienste i.S.d. § 3 Nr. 24 TKG sind, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen.

Als Beispiel eines Dienstes, der lediglich überwiegend in der Signalübertragung besteht und damit sowohl als Telekommunikations- als auch als Telemediendienst zu qualifizieren sei, wird in der Gesetzesbegründung ausdrücklich die E-Mail genannt.[435] In Abgrenzung hierzu sollen Voice over IP-Dienste nicht als Telemediendienste anzusehen sein.[436] Dies erscheint insbesondere auf die obigen Erwägungen zum Telekommunikationsgesetz schwer nachvollziehbar. Auf technischer Ebene unterscheidet sich die Minimalanforderung an einen E-Mail-Anbieter nur durch die verwendeten Kommunikationsprotokolle von der an einen Voice over IP-Anbieter, da zur Bereitstellung einer E-Mail-Adresse bereits das Zurverfügungstellen eines Accounts auf einem Mailserver, der die entsprechenden Protokolle[437] benutzt, ausreicht. Das Telemediengesetz scheint hier jedoch von der praktischen Erwägung geleitet zu sein, dass aufgrund der äußerlichen Ähnlichkeit von Voice-over-IP-Technologien mit klassischer (analoger) Telefonie hierfür eine Anwendbarkeit des des Telekommunikationsgesetzes zielführend ist.[438] Ungeachtet der dogmatischen Bedenken, denen eine solche Betrachtung begegnet, lässt sich hieraus jedoch im Umkehrschluss folgern, dass andere, eher mit der E-Mail verwandte Dienste wie De-Mail und EGVP als Telemediendienste zu klassifizieren sind. Damit gelten die Regelungen des Telemediengesetzes auch für das EGVP in der Gestalt des besonderen elektronischen Anwaltspostfachs. Zu nennen sind für diese Betrachtung insbesondere die Pflicht des Anbieters nach § 13 Abs. 4 Nr. 3 TMG , durch technische und organisatorische Maßnahmen dafür zu sorgen, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt betrachten kann und die Pflicht

435 BT-Drs. 16/3078, 13.
436 BT-Drs. 16/3078, 13.
437 Für das Abrufen von Mail ist das Post Office Protocoll Version 3 (POP3) oder das Internet Message Access Protocol (IMAP), für das Versenden von Mail das Simple Mail Transfer Protocol (SMTP) heute Standard.
438 BT-Drs. 16/3078, 13.

des Anbieters nach § 13 Abs. 7 TMG im Rahmen des Möglichen und Zumutbaren den Dienst gegen unerlaubten Zugriff sowie gegen Datenschutzverletzungen durch Dritte und Störungen zu schützen.

3.3 Fazit zum geschichtlichen Rückblick

In der Gesamtbetrachtung der Entwicklung des elektronischen Rechtsverkehrs und seiner Rechtsgrundlagen wird klar, dass der elektronische Rechtsverkehr keineswegs ein neues Phänomen ist, das gleichsam aus dem Nichts auftaucht, sondern eine Entwicklung, die bereits seit über 20 Jahren läuft. Dementsprechend ist auch das besondere elektronische Anwaltspostfach, auch wenn es durch den Anschluss- und Benutzungszwang[439] für viele Anwälte die erste ernsthafte Auseinandersetzung mit dem elektronischen Rechtsverkehr mit den Gerichten sein mag, lediglich der nächste konsequente Entwicklungsschritt in einer langen Geschichte. Die Bedeutung dieser Erkenntnis liegt insbesondere darin, dass durch die über lange Zeiträume gesammelten Erfahrungen mit bestimmten Technologien und dazugehörigen Rechtsnormen wie beispielsweise der elektronischen Signatur und des elektronischen Gerichts- und Verwaltungspostfachs von einer hohen Qualität und Zuverlässigkeit dieser Technologien ausgegangen werden darf. Das Datenschutzrecht spielt in diese Entwicklungen stets hinein, da es mit Vorschriften zum Schutz personenbezogener Daten zugleich Anforderungen an die Datensicherheit aufstellt. Dies zeigt sich beispielsweise in der Forderung nach Verschlüsselung zur Sicherung von Daten.

Die Bedeutung der Qualität von Technologien, die zur Ersetzung von analoger Kommunikation dienen sollen, soll im folgenden Kapitel untersucht werden. Hierzu werden die Unterschiede zwischen papierbasierter Kommunikation und elektronischer Kommunikation herausgearbeitet, um in der Folge Anforderungen an den elektronischen Rechtsverkehr formulieren zu können, anhand derer später bestehende Lösungen bewerten werden und Empfehlungen für eine Weiterentwicklung des elektronischen Rechtsverkehrs gegeben werden können.

439 Vgl. hierzu oben unter 3.1.7.

2. Teil – Anforderungen an elektronischen Rechtsverkehr

Im nun folgenden zweiten Teil sollen die Anforderungen an den elektronischen Rechtsverkehr untersucht werden. Hierbei wird zum einen aufbauend auf den im 1. Teil vorgestellten Begriffen und Konzepten die Ausgangssituation elektronischer Kommunikation beschrieben, die besondere Regelungen und Techniken für elektronische Kommunikation erforderlich macht. Hierauf aufbauend werden dann Anforderungen an einen elektronischen Rechtsverkehr herausgearbeitet, der den vorher genannten Besonderheiten und Gefahren, aber auch den Vorteilen elektronischer Kommunikation möglichst gerecht wird. Im Zuge dieser Betrachtungen werden zudem die spezifischen Rechtsgrundlagen, die den rechtlichen Rahmen für den elektronischen Rechtsverkehr bilden, erläutert und einer kritischen Würdigung unterzogen.

4 Unterschiede zwischen papierbasierter und elektronischer Kommunikation

Trotz der oft ähnlichen Terminologie zur Beschreibung von papierbasierter und elektronischer Kommunikation weisen beide Kommunikationsarten erhebliche Unterschiede auf. Diese Unterschiede begründen sowohl Stärken als auch Schwächen der jeweiligen Kommunikationsart. Sich ihrer bewusst zu werden, ist notwendige Bedingung, um die Migration von papierbasierte auf elektronische Kommunikation zu vollziehen, ohne damit ungewollte Nachteile zu erleiden oder Risiken zu eröffnen. Insbesondere für den elektronischen Rechtsverkehr sind diese Unterschiede zentraler Ansatzpunkt für viele der Gestaltungsentscheidungen, die sowohl der Gesetzgeber als auch die Urheber der verwendeten Technologien getroffen haben. Die folgenden Betrachtungen bilden damit die Grundlage für die danach zu erarbeitendenen konkreten Anforderungen an einen sicheren und nutzbringenden elektronischen Rechtsverkehr.

Im folgenden Abschnitt werden die Eigenheiten dieser Kommunikationsarten nebeneinander gestellt und deren Folgen herausgearbeitet. Zunächst bedarf es jedoch einer Abgrenzung, was für diese Betrachtung die Begriffe papierbasierte Kommunikation und was elektronische Kommunikation jeweils beschreiben sollen.

Papierbasierte Kommunikation im Sinne dieser Betrachtung bedeutet, dass Informationen – gleich welchen Ursprungs und welcher Erstellungsweise – in einer für Menschen lesbaren Form mit einer gewissen Dauerhaftigkeit verkörpert werden. Insofern nähert sich diese Definition dem

zivilprozessualen Urkundsbegriff („schriftliche Verkörperung einer Gedankenerklärung durch Lautzeichen, die aus sich heraus ohne weiteres verständlich sind“[440]) an. Hierunter fallen zum Beispiel sowohl ein handschriftlich verfasster Brief als auch der Ausdruck eines am Computer erstellten Dokuments oder ein ausgedrucktes Fax. Das Material, auf dem die Schriftzeichen verkörpert sind, ist für diese Definition nicht erheblich, da es auf die menschliche Wahrnehmbarkeit ankommt, nicht jedoch darauf, ob die Zeichen auf Papier aufgedruckt, in Metall eingraviert oder sonst in menschenlesbarer Form mit einer gewissen Dauerhaftigkeit abgebildet sind. Die Bezeichnung „papierbasiert“ ist insofern je nach tatsächlich verwendetem Medium unscharf, soll jedoch hier trotzdem beibehalten werden, da die Verkörperung auf Papier mit großem Abstand der häufigste Fall im Rechtsverkehr sein dürfte. Nicht unter den Begriff der papierbasierten Kommunikation fällt jedoch beispielsweise die Abbildung auf einem Bildschirm oder eine ähnliche flüchtige Darstellung, da es sich hierbei nicht um eine dauerhafte Verkörperung der Daten handelt.

Elektronische Kommunikation im Sinne dieser Betrachtung bedeutet, dass Informationen als – außer im Falle einer Speicherung auf einem nur maschinenlesbaren Datenträger – nicht-verkörperte und nicht von Menschen unmittelbar lesbare digitale Repräsentation vorliegen. Hierunter fallen Dateien im Arbeitsspeicher von Computern, auf Datenträgern wie Disketten, CD-ROMs oder USB-Sticks sowie Daten, die sich auf dem Transportweg über ein Kommunikationsnetz wie das Internet befinden. Bei diesen Daten fehlt es zum Teil an einer Verkörperung, jedenfalls aber an einer unmittelbaren Wahrnehmbarkeit durch Menschen.

Zu unterscheiden ist schließlich auch noch zwischen dem bloßen Vorliegen von Daten (jeweils entweder in verkörperter oder in unverkörperter Form) einerseits und der Übertragung dieser Daten andererseits. Für die folgenden Betrachtungen im Hinblick auf den elektronischen Rechtsverkehr ist zwar die Datenübertragung besonders relevant, aber auch auf Eigenheiten von „unbewegten“ Daten muss eingegangen werden, da sich viele Eigenschaften verkörperter bzw. unverkörperter Daten unabhängig von möglichen Übertragungsarten ergeben.

4.1 Spurlose Kopierbarkeit

Eine der wesentlichen Eigenschaften digitaler elektronischer Kommunikation ist die (technische) Identität von Original und Kopie. Im Gegensatz zu Kopien von analogen Daten, die unvermeidbar unerwünschte Informationen in Form von Rauschen[441] enthalten, sind digitale Daten ohne jeden

440 *Schreiber* in MüKo-ZPO Band 2, § 415 Rn. 5 m.w.N.
441 Gemeint ist hiermit nicht (nur) das akustische Phänomen, sondern vielmehr jede zusätzlich abgespeicherte oder

Qualitätsverlust kopierbar.[442] Dies hat zur Folge, dass eine Kopie digitaler Daten identisch mit dem Original ist.[443] Eine Unterscheidung zwischen Original und Kopie kann im digitalen Bereich somit nicht wie im analogen Umfeld an Unterschieden zwischen Original und Kopie (z.B. der Qualitätsverschlechterung bei einer Fotokopie) festgemacht werden. Allenfalls Begleitumstände wie das verwendete Medium (eine beschreibbare CD-R ist ohne weiteres auch für den ungeübten Betrachter von einer gepressten Audio-CD unterscheidbar, wenngleich die auf beiden gespeicherten Daten identisch sein mögen) oder beim Kopieren hinzugefügte Metadaten (beispielsweise das in vielen Dateisystemen gespeicherte Erstellungsdatum einer Datei) erlauben noch eine Unterscheidung von zwei Kopien von Daten. Da aber digitale Daten weder an ein bestimmtes Medium, noch an eine Art der Speicherung gebunden sind, sind diese zusätzlichen Informationen nicht fest mit den eigentlichen digitalen Daten verbunden und lassen somit nur einen sehr eingeschränkten Erkenntnisgewinn zu. Im Gegensatz hierzu sind Papierdokumente stets auf einem Medium verkörpert, wodurch sich bei diesen in der Regel das Verhältnis von Kopie und Original nachvollziehen lässt. Dies gilt unproblematisch für analog erstellte Dokumente wie beispielsweise ein eigenhändig (§ 2247 BGB) verfasstes Testament, dessen Urheberschaft und Werdegang anhand eines graphologischen Gutachtens nachvollzogen werden kann. Selbst bei technisch erstellten Verkörperungen von (auch digitalen) Informationen lassen sich aus der Verkörperung bzw. dieser unvermeidbar innewohnenden Metainformationen Erkenntnisse zu Erstellungsdatum und Urheberschaft ziehen. So wären beispielsweise selbst bei einem nicht unterschriebenen Ausdruck eines Schriftsatzes Elemente wie Papierart, Druckertyp und ggf. vom Druckerhersteller in Ausdrucken durch Punktmuster einkodierte Informationen über den Drucker (bei Farblaserdruckern)[444] oder über typische Druckmuster[445] Anhaltspunkte, mit denen die Originalität und Urheberschaft eines Dokuments zumindest mit einer gewissen Wahrscheinlichkeit bestimmt werden kann. Bei einem Fax werden Metainformationen über den Kommunikationsweg und die beteiligten Geräte mitgeliefert, diese umfassen z.B. die Telefonnummer des versendenden Faxgerätes und die Uhrzeit des Dokumentenempfangs. Diese Elemente fehlen bei nicht verkörperten elektronischen Informationen prinzipbedingt.[446] Sind nicht beispielsweise durch Kommunikationsvorgänge zusätzliche Metainformationen hinterlegt, sind diese aus dem Dokument selbst nicht extrahierbar.

übertragene Information, die nicht zur eigentlich gewünschten Information beiträgt und deshalb eine Störung darstellt; In der Informationstheorie wird der Begriff als *Noise* bezeichnet, vgl. dazu *Weaver* in *Shannon/Weaver*, 8.

442 *Baumgartner*, 6.

443 *Gass*, ZUM 1999, 815, 815 f.

444 *Electronic Frontier Foundation*, Machine Identification Code in Printers; eine Liste von Druckern die ein solches Punktmuster einbetten und solcher, die dies nicht tun findet sich bei *Electronic Frontier Foundation*, Druckerliste.

445 *Mikkilineni/Khanna/Delp*, 1 f.

446 *Bergfelder*, 94 f.

Auch bei im elektronischen Rechtsverkehr vorrangig relevanten Textdateien kann durch das bloße Betrachten des Dokuments (beispielsweise einer mit Microsoft Word erstellten .docx-Datei) nicht festgestellt werden, ob es sich hierbei um die vom Verfasser ursprünglich erstellte Datei handelt oder um eine Kopie und durch wen diese Kopie erstellt wurde. Diese Eigenschaft führt für sich alleine im Bereich des elektronischen Rechtsverkehrs noch nicht zu Schwierigkeiten, wird aber beispielsweise im Urheberrecht (man denke an Kopien von gekauften Liedern oder Musikalben im populären mp3-Format) und für den Geheimnisschutz relevant.

Aus dieser Eigenheit folgt zudem, dass man digital vorliegenden Daten nicht „ansehen“ kann, ob und gegebenenfalls wie oft bereits Kopien von ihnen gefertigt wurden. Dadurch kann nicht bestimmt werden, ob es sich bei einem vorliegenden Datensatz um das einzige Exemplar handelt oder sich hunderte von Kopien dieser Daten im Umlauf befinden. Dies kann beispielsweise bei der Frage der Zugangssicherung zu Daten relevant werden und berührt dort sowohl datenschutzrechtliche und berufsrechtliche als auch strafrechtliche Aspekte. Auch bei prozessualen Vorschriften, die sich auf die Originalität von Urkunden berufen (wie beispielsweise die vollstreckbare Urteilsausfertigung nach § 724 ZPO) ist diese Eigenschaft digitaler Daten zu berücksichtigen.

Aus der postulierten perfekten und spurlosen Kopierbarkeit digitaler Daten ergeben sich zudem weitere Eigenschaften, die im Folgenden beschrieben werden.

4.2 Fehlende Nachvollziehbarkeit von Änderungen

Eine für den elektronischen Rechtsverkehr höchst relevante Eigenheit elektronischer Kommunikation ist die aus der oben betrachteten spurlosen Kopierbarkeit folgende spurlose Abänderbarkeit. Eine Änderung eines verkörperten Dokuments bedarf immer eines physikalisch wirksamen Änderungsvorgangs, der naturgemäß Spuren hinterlässt. Eine Durchstreichung und Änderung eines Wortes in einem Testament ist unmittelbar sichtbar und beispielsweise durch ein graphologisches Gutachten einem Urheber zuordenbar. Eine Fotokopie eines ausgedruckt vorliegenden Dokuments mit Änderungen ist – wenn nicht schon die Eigenschaft als Fotokopie erkennbar ist und aus sich heraus rechtliche Wirkungen vereitelt – jedenfalls von einem Experten oft als solche identifizierbar. Diese Erkenntnismöglichkeiten hängen jedoch von den genannten Metainformationen wie Schriftbild, kopierertypischen Artefakten, auf Kopien sichtbarem Schattenwurf von Kopiercollagen etc. ab. Da diese Metainformationen prinzipiell nicht bei nicht-

verkörperten elektronischen Informationen vorhanden sind,[447] ist eine Abbildung der Erkenntnismöglichkeiten über Urheberschaft und Originalität abhängig von extern – beispielsweise einer vertrauenswürdigen Stelle – hinzugefügten Metainformationen, die einer Fälschung nicht zugänglich sein dürfen.

Die Möglichkeiten einer inhaltlichen Veränderung sollen für diese Betrachtung in zwei Kategorien unterteilt werden: Inhaltliche Veränderbarkeit (Integrität) und urheberschaftliche Veränderbarkeit (Authentizität).

4.2.1 Inhaltliche Veränderbarkeit (Problem der Integrität)

Eine Form der oben abstrakt beschriebenen Veränderbarkeit elektronischer Kommunikation ist die inhaltliche Veränderbarkeit. Die inhaltliche Unverändertheit eines Dokuments wird im Folgenden als Integrität bezeichnet, da sich dieser Begriff in der Rechtswissenschaft für diesen Sachverhalt etabliert zu haben scheint.[448] Änderungen im Inhalt eines Dokuments können – unabhängig von der Urheberschaft – erhebliche rechtliche Wirkungen zeigen. So kann beispielsweise eine Partei eines Kaufvertrags eine von ihr veränderte E-Mail der Gegenseite vor Gericht als Beweisstück vorlegen (dann natürlich in verkörperter Form als Ausdruck), in der sich der vereinbarte Kaufpreis statt wie in der „echten“ E-Mail auf 5.000 Euro nunmehr auf 10.000 Euro beläuft. Aus dem Ausdruck selbst wäre in diesem Beispiel nicht erkennbar, dass die E-Mail mit diesem Inhalt nie bei der vorlegenden Seite eingegangen ist. Die Verkörperung in Form des Ausdrucks ändert hieran nichts, weil die aus dem Ausdruck selbst erkennbaren Metainformationen sowohl der Wahrheit entsprechen (z.B. ausgedruckt durch den Vorlegenden auf dessen Drucker unter Benutzung der von ihm gewohnheitsmäßig verwendeten Papiersorte und Druckertinte), als auch keine Informationen über den Prozess der Fälschung enthalten.

Ebenfalls hierunter fallen *unbeabsichtigte* Änderungen durch technische Fehler wie z.B. Defekte von Speichermedien, sonstige Hardware- oder Softwarefehler sowie menschliches Versagen. Ein Vorteil der digitalen Repräsentation von Daten ist zwar, dass die Wahrscheinlichkeit eines unbemerkten Fehlers durch Defekt des Speichermediums relativ gering ist, da selbst geringste Änderungen an digitalen Daten zu massiven Auswirkungen, nicht jedoch zu subtilen Fehlern

447 So spricht Roßnagel beispielsweise davon, dass „[e]lektronische Daten […] keine Geschichte [haben]“, *Roßnagel* in Telemediendienste, Einl. SigG Rn. 8.

448 Vgl. hierzu *Bergfelder*, 90 m.w.N., der allerdings den Begriff der Integrität auf eine Unverändertheit nach einer erfolgten Signierung beschränkt. Eine solche ist für die hier benutzte Definition gerade nicht nötig, da ansonsten gerade der Gewinn einer digitalen Signatur nicht anhand dieses Begriffes herausgearbeitet werden kann.

führen. Etwas anderes gilt jedoch für andere Fehlertypen wie systematische Fehler. So sind Fälle dokumentiert, in denen Scanner durch die verwendeten Kompressionsalgorithmen bestimmte Zahlen im Scan durch andere ersetzt haben, was ohne vorherige Kenntnis des Fehlers schwer zu reproduzieren ist und zu katastrophalen Folgen führen kann.[449]

4.2.2 Urheberschaftliche Veränderbarkeit (Problem der Authentizität)

Hiervon zu unterscheiden ist die Veränderung der Urheberschaft einer elektronischen Kommunikation. Das Zusammenfallen von tatsächlichem und scheinbaren Aussteller einer Nachricht wird im Folgenden Authentizität genannt.[450] Im genannten E-Mail-Beispiel würde dies einer Änderung der Namenswiedergabe am Ende der E-Mail („Mit freundlichen Grüßen, Mustermann“) und der abgebildeten E-Mail-Adresse („Max@mustermann.de“) entsprechen. Auch diese Änderung lässt sich weder anhand der Datei, in der die (veränderte) E-Mail gespeichert ist, noch an einem Ausdruck dieser veränderten E-Mail nachvollziehen. Eventuelle durch den verwendeten Computer hinzugefügte Metainformationen wie z.B. die Änderungszeit einer Datei können ungenau sein oder lassen sich sogar problemlos fälschen, beispielsweise durch das Verstellen der Systemzeit des verwendeten Rechners.[451] Die Speicherung dieser Metadaten ist dementsprechend auch nicht als Sicherheitsfunktion zu qualifizieren, sondern eher als „Bequemlichkeitsfunktion“ für den Nutzer, der seine eigenen Aktionen an Dateien nachvollziehen will.

4.3 Echtzeitübermittlung von Informationen

Eine weitere wesentliche Eigenschaft elektronischer Kommunikation ist die nahezu-Echtzeitübertragung von Daten. Im Gegensatz zur analogen Kommunikation per Post oder persönlichem Einwurf in den Briefkasten haben elektronisch übermittelte Daten das Potenzial, ihren Bestimmungsort nahezu verzögerungsfrei zu erreichen. Die auf dem Weg notwendigen Verarbeitungsschritte wie Weiterleitung einer Nachricht zwischen verschiedenen Mailservern im Falle einer E-Mail-Kommunikation laufen dabei im Regelfall so schnell ab, dass sie für praktische

449 *Opitz*, c't 19/2013, 40.
450 So unter anderem *Bergfelder*, 87; *Bernhardt* in *Heckmann*, Kap. 6 Rn. 127.
451 *Schatz/Mohay/Clark*, Digital Investigation 2006, 98.

Zwecke zu vernachlässigen sind. Allenfalls bei der Übertragung größerer Datenmengen können Verzögerungen durch das Hochladen der Daten auf Senderseite und das Herunterladen auf Empfängerseite zustande kommen. In diesen Fällen stellt sich die Frage, auch welchen Zeitpunkt bei der Bewertung des Zugangs abzustellen ist.

Die hohe Kommunikationsgeschwindigkeit ermöglicht für den elektronischen Rechtsverkehr selbst im Vergleich zum Fax nochmals eine höhere Geschwindigkeit, zumal Faxgeräte Datenübertragungen mit einer für das moderne Internet geradezu anachronistisch anmutenden Geschwindigkeit von maximal 64 kbit/s bei Übertragung zwischen ISDN-Gegenstellen[452] ermöglichen, moderne DSL-Anschlüsse sich aber im Bereich von 2 – 100 Mbit/s bewegen, womit sie die ca. 32-1600fache (sic!) Geschwindigkeit bei der Datenübertragung erreichen. Hierdurch ist es möglich, auch große Datenmengen innerhalb weniger Sekunden oder Minuten an den Bestimmungsort zu übertragen. Voraussetzung hierfür ist jedoch das Vorliegen einer hinreichend dimensionierten Kommunikationsinfrastruktur. Hier gibt es besonders im ländlichen Raum noch größere Lücken in der Versorgung mit Breitband-Internetanschlüssen (insbesondere DSL), wodurch die heute theoretisch erreichbare Geschwindigkeit bei weitem nicht überall realisierbar ist.

4.4 Automatisierbarkeit

Ein deutlicher Vorteil der Digitalisierung ist die damit einhergehende Automatisierbarkeit. Da digitalisierte Informationen einerseits nicht mehr an ein spezifisches Medium und damit auch nicht an einen bestimmten Speicherort gebunden sind, ist innerhalb bestimmter Grenzen eine automatisierte (Weiter-)Verarbeitung der Daten möglich. Beispiele sind die automatisierte Sortierung, Filterung und der Vergleich von Datensätzen.[453] Voraussetzung hierfür ist, dass die Daten in maschinenlesbarer Form vorliegen, wofür gegebenenfalls eine Aufbereitung erforderlich ist.

Offenkundige Vorteile hierfür ergeben sich beispielsweise bei der Archivierung und dem Durchsuchen von Informationen. Eingehende Daten können mit Schlagworten versehen werden, nach dem sie dann in einem Speichersystem wieder aufgefunden werden können. Zudem kann anhand von mitübertragenen Metadaten eine Vorsortierung der eingehenden Daten stattfinden und

452 *Kessler*, 286 f.
453 *Klink*, 35 m.w.N.

bestimmte Weiterverarbeitungsschritte (z.B. die automatische Weiterleitung eines Schriftsatzes nach dem mitübertragenen Aktenzeichen an die zuständige Geschäftsstelle, das automatische Setzen einer Wiedervorlagefrist o.Ä.) eingeleitet werden. Um diese Vorteile zu nutzen, ist es jedoch erforderlich, Datenformate und Metadaten möglichst einheitlich zu definieren und somit eine Interoperabilität zwischen den von den verschiedenen Beteiligten genutzten Softwareprodukten und -versionen zu gewährleisten. Zudem ist eine genaue Abwägung zwischen potentiellen Vorteilen einer Automatisierung wie Kosten- und Zeitersparnis und potentiellen Nachteilen wie Fehlzuordnungen von Dateneingängen, Programmierfehlern und Datenverlusten zu treffen. Auch können sich durch das automatische Korrelieren von Datensätzen, das durch die Automatisierung in einem Maße möglich ist, das bisher durch menschliches Handeln nicht erreicht werden konnte, Datenschutzprobleme auftun.[454] Hier muss gegebenenfalls durch die Gestaltung der Verarbeitungssysteme Datenschutzverstößen vorgebeugt werden.

4.5 Gleichzeitiger Zugriff

Eine Folge aus den Eigenschaften der einfachen, spurlosen Kopierbarkeit von elektronischen Daten einerseits und der (quasi-)Echtzeitübermittlung andererseits ist die Möglichkeit, die Benutzung von Datensätzen durch mehrere Personen zur gleichen Zeit zu gewährleisten. Dies ist eine echte Neuerung im Vergleich zu nicht elektronisch gespeicherten, verkörperten Daten, da diese in der Regel nicht gleichzeitig von mehreren Personen genutzt werden können.[455] Während dies dadurch umgangen werden kann, dass von verkörperten Originalen Kopien erzeugt und verschickt werden, geht dies jedoch regelmäßig mit einem erheblichen zeitlichen und personellen Aufwand einher, was den elektronischen Zugriff weit attraktiver macht. Gleichzeitig eröffnet diese Möglichkeit jedoch auch die Gefahr, die Herrschaft über die Daten zu verlieren, beispielsweise indem von Personen, die nur das Recht zum Einsehen, nicht jedoch zum Kopieren haben, unberechtigte Kopien der Daten gefertigt werden. Zum Teil kann man diesem Problem durch Kopierschutzmaßnahmen wie DRM[456] begegnen, wie es beispielsweise im Adobe PDF-Format vorgesehen ist. Jedoch ist zu berücksichtigen, dass auch ein solcher Schutz nicht lückenlos gewährleistet ist, da es mit einem gewissen Aufwand praktisch immer möglich ist, Kopien – wenn auch unter Qualitätsverlust durch

454 *Plath* in *Plath*, § 1 BDSG, Rn. 10.
455 *Klink*, 36 m.w.N.
456 *Digital Rights Management* (digitale Rechteverwaltung) ist ein Sammelbegriff für technische Vorkehrungen, die die Festlegung von bestimmten Berechtigungen (z.B. ansehen, kopieren, ausdrucken, Passwortschutz) für digitale Medien ermöglichen.

die Ausnutzung analoger Lücken (z.B. Abfotografieren vom Bildschirm) – von kopiergeschützten elektronischen Daten zu erstellen.

4.6 Datensicherheit

Ein weiterer zu berücksichtigender Punkt bei der elektronischen Kommunikation, der jedoch keine originäre Eigenart dieser darstellt, ist die Frage der Datensicherheit, d.h. der Sicherung der verwendeten Systeme und Übertragungswege gegen externe Angriffe und Störungen. Es bestehen aufgrund der genannten Eigenschaften der fehlenden Bindung an Trägermedien, der spurlosen Kopier- und Veränderbarkeit digitaler Daten, der Automatisierbarkeit sowie der elektronischen Übertragbarkeit in Echtzeit besondere Herausforderungen an die Absicherung von Daten. Denn aufgrund der genannten Eigenschaften ist beispielsweise ein Kopieren, Unterdrücken oder Abändern von Daten auf dem Übertragungsweg durch Dritte theoretisch unbemerkt möglich, sofern nicht entsprechende Sicherheitsvorkehrungen getroffen werden. Ein Abfangen und Kopieren eines Schriftstücks auf dem Transportweg ist zwar auch möglich (man denke beispielsweise an das Abfangen des Boten, der einen Schriftsatz zum Gericht bringen soll), dürfte allerdings kaum unbemerkt bleiben. Selbst das Anfertigen einer Fotokopie eines Schriftstücks, das keine Spuren an dem Dokument selbst hinterlässt, schlägt sich zumindest in der Eigenschaft der Kopie nieder, die in der Regel problemlos als bloße Kopie erkennbar sein dürfte. Auch unterliegen elektronisch gespeicherte Daten einer prinzipiell einfacheren Zugreifbarkeit als verkörperte Kopien. So sind in der Vergangenheit immer wieder Fälle publik geworden, in denen große Datenbanken mit Kundendaten durch Angreifer[457] entwendet wurden.[458] Hierbei ist regelmäßig ein Problem, dass für einen Angriff auf elektronisch gespeicherte Daten gerade kein physikalischer Zugriff auf das speichernde System notwendig ist, sondern ein Angriff von jedem Ort der Welt aus über Datennetzwerke möglich ist, sofern das angegriffene System über solche erreichbar ist. Je nach Beschaffenheit der verwendeten Sicherheitsvorkehrungen kann ein solcher Angriff auch deutlich schwerer zu erkennen sein als beispielsweise das Ansichbringen einer großen Anzahl von verkörperten Daten wie z.B. Handakten.

457 Wenngleich in der öffentlichen Debatte für Angreifer auf Computersysteme oft die Bezeichnung „Hacker“ verwendet wird, ist dieser Begriff nicht so klar definiert, dass er eine Gleichsetzung mit Kriminalität erlauben würde. Besser ist es, in diesem Zusammenhang beispielsweise von Computerkriminellen zu reden, zumal bei derartigen Angriffen regelmäßig eher die persönliche Bereicherungsabsicht als ein Austesten der Möglichkeiten und Grenzen von Technologie im Vordergrund stehen dürfe.

458 Ein Beispiel hierfür ist der großangelegte Angriff auf US-Unternehmen, mit dem Kreditkartendaten der Nutzer von über 1000 Unternehmen erbeutet wurden, vgl. *Holland*, Kreditkartenhack.

4.7 Abstreitbarkeit und Zugang

Ein weiteres Problem, das ebenfalls nicht originär für elektronische Kommunikation ist, von dieser aber gegebenenfalls verstärkt werden kann, ist die Frage der Beweisbarkeit des Zugangs, zum Teil auch unter den Begriffen Abstreitbarkeit (engl. *deniability*[459]) oder Nichtabstreitbarkeit behandelt. Zugangs- und Beweisbarkeitsprobleme sind bereits aus der analogen Welt hinlänglich bekannt. Sie treten beispielsweise im Zivilrecht beim Zugang von Willenserklärungen, im Verwaltungsrecht bei der Bekanntgabe von Verwaltungsakten und im Prozessrecht bei der Zustellung von bestimmenden Schriftsätzen wie Klagen auf. Eine Verschärfung dieser Probleme kann sich bei elektronischer Kommunikation in zweierlei Richtungen ergeben: Zum einen kann durch die „Geschichtslosigkeit“[460] von elektronischen Daten das (wahrheitswidrige) Abstreiten des Zugangs insgesamt oder zu einem bestimmten Zeitpunkt erleichtert werden, letzteres da wie oben gezeigt vom Endgerät selbst hinzugefügte einfache Zeitstempel trivial zu fälschen sind und somit praktisch keinen Beweiswert haben. Zum anderen kann der Absender hierdurch auch (wahrheitswidrig) behaupten, ein Dokument überhaupt oder früher als tatsächlich erfolgt versandt zu haben. Abhilfe kann in diesen Fällen durch eine Protokollierung von Absende- und Zugangszeitpunkten durch eine unabhängige Dritte Instanz (die auch in einer vor Veränderungen geschützen technischen Vorrichtung wie einem speziell gesicherten Kommunikationsprogramm bestehen kann) geschaffen werden. Ein Spannungsfeld ergibt sich hier jedoch dadurch, dass eine vollständige unabhängige Protokollierung sämtlicher Nutzerkommunikation datenschutzrechtliche wie grundrechtliche Probleme aufwirft. Dem kann jedoch dadurch begegnet werden, dass entsprechende Lösungen auf freiwilliger Basis angeboten werden und diese abhängig von einer Einwilligung des Nutzers sind.

Doch auch eine Abstreitbarkeit kann in manchen Konstellationen durchaus gewollt sein. In Fällen, wo es stärker auf die Vertraulichkeit einer Kommunikation als auf die (spätere) Beweisbarkeit der einzelnen Kommunikationsschritte ankommt, ist eine glaubhafte Abstreitbarkeit (engl. *plausible deniability*) gegebenenfalls gewünscht. Wenngleich sich ein solcher Anwendungsfall für den elektronischen Rechtsverkehr mit den Gerichten nicht aufdrängt, gibt es beispielsweise im Journalismus unter dem Gesichtspunkt der für Journalisten gefährlichen Berichterstattung und -materialsammlung und des Quellenschutzes hierfür sowohl ein Bedürfnis als auch technische Lösungsansätze.[461]

459 *Mao/Paterson*, 1 f.
460 Vgl. oben unter 4.2 zur spurlosen Veränderbarkeit von Daten.
461 Beispiele für technisch gewährleistete *plausible deniability* sind das off-the-record-messsaging (OTR) in Form eines Zusatzprogramms (*Plugins*) für verschiedene Kommunikationsprogramme (https://otr.cypherpunks.ca, zuletzt abgerufen am 18.12.2017) und das Programm Tor zur anonymen Nutzung des Internets (http://www.torproject.org,

4.8 Angriffsszenarien

Durch die herausgearbeiteten Eigenheiten von elektronisch gespeicherten Daten ergeben sich spezifische Gefahren und Angriffsszenarien, gegen die diese Daten zu schützen sind. Zwar erschöpfen sich die Bedrohungen für elektronische Daten nicht in bewussten Angriffen, da auch technische Fehler, menschliches Versagen und höhere Gewalt zur Kompromittierung und zum Verlust von elektronischen Daten führen können. Das Schadpotential gezielter Angriffe ist jedoch um ein vielfaches höher als bei zufälligen Schadereignissen, da bei Angriffen gezielt Schwachpunkte der Sicherheitsinfrastruktur ausgenutzt werden können. Deshalb lohnt sich eine Betrachtung dieser Angriffsszenarien, da diese als gewissermaßen schlimmster Fall bei der Informationssicherheit die Messlatte dafür darstellen, als wie sicher ein System gelten kann. Dies gilt umso mehr dann, wenn die fraglichen Daten oder eine Veränderung dieser Daten einen hohen wirtschaftlichen Wert haben, da sich hierdurch auch der potentielle Energieaufwand erhöht, den ein Angreifer zu investieren bereit sein wird, um ein System zu kompromittieren.

Um einen wirkungsvollen Schutz zu gewährleisten, ist es zunächst erforderlich, sich mit den möglichen Angriffsvektoren zu befassen, um Strategien gegen diese entwickeln und bewerten zu können.

4.8.1 Angriffe auf gespeicherte Daten

Eine Gruppe von Gefährdungen betrifft zunächst gespeicherte Daten. Hierzu zählen sowohl auf Datenträgern festgehaltene Daten, unabhängig davon, ob die Datenträger mit einer Datenverarbeitungsanlage verbunden sind (beispielsweise die Systemfestplatte in einem PC) oder lediglich als Speicher- oder Transportmedium dienen (beispielsweise die Backup-Festplatte im Tresor oder der USB-Stick zum Datentransport). Nach der hier verwendeten Definition sollen auch flüchtige Datenspeicher wie der Arbeitsspeicher (RAM)[462] von Computern erfasst sein, da diese genauso – wenn nicht sogar stärker – gefährdet sind als Daten, die auf einem nicht-flüchtigen Datenträger gespeichert sind.

zuletzt abgerufen am 18.12.2017).

462 Beim RAM (*Random Access Memory*, Speicher mit wahlfreiem Zugriff) oder auch Arbeitsspeicher spricht man von einem flüchtigen Speicher, weil der Speicherinhalt im Allgemeinen nur so lange vorgehalten wird, wie das System mit Strom versorgt ist. Vgl. zu den Einschränkungen hierzu jedoch Abschnitt 4.8.1.1.

4.8.1.1 Unbefugter physikalischer Zugriff

Das am wenigsten raffinierte Angriffsszenario auf Daten stellt die Erlangung physikalischen Zugriffs auf die Datenträger, auf denen die Daten gespeichert sind, dar. Diese Gefahr ist bereits aus der Arbeit mit Papierdokumenten bekannt, dementsprechend existiert eine Vielzahl von Sicherungsmitteln und Strategien, um solche Angriffe zu verhindern. Unter solche Sicherungsmittel (auch) für Informationsverarbeitende Systeme fallen in erster Linie Schlösser für Türen und Fenster der Räume, in denen Daten bzw. Datenverarbeitungsanlagen aufbewahrt bzw. betrieben werden,[463] Zugangskontrollen,[464] abschließbare Schränke und Tresore[465] und ähnliche physikalische Barrieren, die Unberechtigten den Zugang zu sensiblen Daten verwehren sollen. Besonderheiten bestehen hier insofern, als durch die höhere Speicherdichte von elektronischen Speichermedien der mögliche Schaden durch verlorene oder entwendete Speichermedien gegebenenfalls höher ist, da Datenspeicher für elektronische Daten im Verhältnis zum Platzbedarf für die Datenträger ungleich höhere Datenmengen speichern können, als auf Papier festgehalten werden kann. Damit verbunden besteht auch ein höheres Schadenspotential darin, dass gegebenenfalls sensible Daten zum Arbeiten von unterwegs auf mobilen Endgeräten wie Laptops oder Smartphones mitgeführt werden, deren Abhandenkommen zu einem entsprechend hohen Schaden führen kann. Zudem ist aufgrund der einfachen und spurlosen Kopierbarkeit von elektronisch gespeicherten Daten das unbefugte Kopieren auch einfacher, schneller und unbemerkter möglich als bei beispielsweise Papierakten, was ebenfalls zu einem höheren Schadenspotential führen kann.

Zusätzliche Sicherungsmittel, um sich gegen solche Angriffe zu schützen existieren jedoch ebenfalls im digitalen Bereich. So ist eine Alternative zum Mitführen von sensiblen Daten die Einrichtung eines Fernzugriffs[466] oder die Verwendung von Datenträgerverschlüsselung nach dem Stand der Technik. Vor allem letztere reduziert im Falle des Verlustes eines Datenträgers den eintretenden Schaden bei richtiger Anwendung auf die bloßen Materialkosten, verwehrt aber Dritten dauerhaft den Zugang zu den erlangten Daten, sofern sie nicht zusätzlich an den verwendeten Schlüssel gelangen können. Kehrseite dieses Effekts ist jedoch, dass bei Verlust des Schlüssels (beispielsweise durch einen Datenträgerdefekt) auch der berechtigte Nutzer nicht mehr auf die verschlüsselten Daten zugreifen kann. Bei Verwendung einer sicheren Verschlüsselung ist das

463 Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge M 1.19 – Einbruchsschutz.
464 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge M 2.6 – Vergabe von Zutrittsberechtigungen.
465 Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge M 1.36 – Sichere Aufbewahrung der Datenträger vor und nach Versand.
466 Siehe zu den Gefahren hierdurch aber Abschnitt 4.8.1.2.

Entschlüsseln der Daten ohne den passenden Schlüssel so rechenzeitaufwändig, dass diesbezüglich praktisch Unmöglichkeit vorliegt.[467]

Auch gegen eine komplette Verschlüsselung des Systems existieren jedoch Angriffe. So kann ein Angreifer mit physikalischem Zugriff auf einen (ein- oder ausgeschalteten) PC diesen so manipulieren, dass dieser beispielsweise eingegebene Passwörter automatisch mitschneidet und später an den Angreifer weitersendet. Auf Softwareebene werden solche Angriffe auch als *Evil Maid*-Angriffe bezeichnet[468], das es für diese vorgefertigte Werkzeuge gibt, mit denen auch Personen mit geringer Sachkenntnis über die Schwachstellen von Computersystemen solche Angriffe durchführen können. Ein weiteres Szenario, gegen das selbst eine Vollverschlüsselung des Systems nicht hilft, ist der direkte Angriff auf den Arbeitsspeicher, sofern der Angreifer physischen Zugriff auf den laufenden PC hat. Diese Angriffe erfordern grundsätzlich mehr technisches Verständnis und eine umfassendere Ausrüstung. Hierunter fallen der direkte Zugriff auf den Arbeitsspeicher des PCs über dessen Schnittstellen wie beispielsweise die IEEE1394-Schnittstelle (*Firewire*), die als insbesondere für die Videoverarbeitung gedachte schnelle Datenübertragungsschnittstelle konzipiert ist und eine direkte Verbindung zum Arbeitsspeicher des Computers hat.[469] Für einen hochprofessionellen Angreifer oder Strafverfolgungsbehörden bieten sich schließlich sogenannte *Cold Boot-Attacken* an, bei denen der Arbeitsspeicher des laufenden PCs vom Mainboard gelöst, mittels eines Kühlmittels künstlich stark abgekühlt wird, um die Verflüchtigung der Arbeitsspeicherinhalte zu verlangsamen, und in ein spezielles Lesegerät eingesetzt wird, mit dem der Speicherinhalt ausgelesen werden kann.[470] Gegen die genannten Angriffe gibt es selbstverständlich ebenfalls Gegenmaßnahmen. Da jedoch zu erwarten ist, dass auch in Zukunft neue Angriffe bei direktem Zugriff auf informationsverarbeitende Systeme entdeckt werden, dürfte der zuverlässigste Schutz sein, Unbefugten bereits den physischen Zugang zu Computern, die sensible Daten speichern oder verarbeiten (sollen), zu verwehren.[471]

Gegen den bloßen Verlust von Daten ohne Kenntnisnahme Dritter (beispielsweise durch technische Fehler, Havarien oder Fehlbedienung) helfen vom Nutzer regelmäßig erstellte Sicherungskopien, die gegen unbefugten Zugriff zu sichern und getrennt von den gesicherten Daten aufzubewahren

467 Hieran ändern auch publizierte mathematische Angriffe auf den heute vorrangig genutzten Kryptoalgorithmus AES nichts, da auch mit diesen das Errechnen eines AES-128-Schlüssels selbst mit Billionen (sic!) von extrem schnellen Computern mehrere Milliarden Jahre benötigen würde, vgl. *Neal*, AES is cracked.

468 *Schmidt*, c't 11/2011, 192, 195.

469 *Piegdon*, 7 f.

470 *Halderman/Schoen/Heninger/Clarkson u. a.*, 1.

471 Der bekannte Sicherheitsforscher und Verschlüsselungsspezialist Bruce Schneier fasst diese Situation wie folgt zusammen: „As soon as you give up physical control of your computer, all bets are off." *Schneier*, Schneier on Security 10/2009.

sind.[472]

4.8.1.2 Unbefugter Fernzugriff

Eine Besonderheit für die Sicherheit elektronisch gespeicherter Daten stellt die Möglichkeit dar, auch ohne physikalischen Zugriff auf die Speichermedien Kenntnis der Daten erlangen zu können. Solche Angriffe können zum einen dadurch erfolgen, dass viele Rechner, auf deren Datenträgern die zu schützenden Daten gespeichert sind, mit dem Internet verbunden sind. Zum Teil richten Nutzer auch bewusst einen Fernzugriff ein, um von unterwegs Zugriff auf die eigenen Daten zu haben. Ein solcher beabsichtigter Fernzugriff muss jedoch entsprechend abgesichert sein (beispielsweise durch einen Passwortschutz und Verwendung von Software, die frei von bekannten Sicherheitslücken ist), um den Kreis der Zugreifenden auf berechtigte Nutzer zu beschränken. Verbreitete Zugriffsarten sind beispielsweise FTP,[473] VNC[474] oder VPN[475].

Auch ohne Einrichtung einer Fernzugriffsmöglichkeit durch den Nutzer lassen sich jedoch über Sicherheitslücken in der auf den Rechnern verwendete Software Angriffe auf die Rechner und die auf ihnen gespeicherten Daten realisieren. Hierbei ist zu unterscheiden zwischen dem Einschleusen von schädlichen Programmen auf den anzugreifenden Rechner (z.B. in Form von Viren, Trojanern oder Würmern) einerseits und dem bloßen Ausnutzen von Sicherheitslücken der bereits auf dem Rechner verwendeten Software. Gegen die erste Variante kann Antivirensoftware einen gewissen (nicht jedoch einen absoluten!) Schutz bieten, der jedoch insbesondere von technischen Laien regelmäßig überschätzt wird. So hat eine vergleichende Studie dreier Google-Mitarbeiter zur Wahrnehmung von Sicherheitstechniken ergeben, dass die meisten befragten technischen Laien in erster Linie auf Antivirensoftware setzen, während die meisten Sicherheitsexperten als wichtigste Maßnahme das zeitnahe Installieren von Betriebssystem- und Anwendungsupdates bezeichneten.[476]

472 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge M 6.20 – Geeignete Aufbewahrung der Backup-Datenträger.

473 *File Transfer Protocol*, ein Kommunikationsprotokoll, dass den Zugriff auf Dateien über ein Netzwerk ermöglicht und mit Benutzername und Passwort abgesichert werden kann.

474 *Virtual Network Computing*, Überbegriff für den grafischen Fernzugriff auf eine Benutzeroberfläche (Desktop) eines entfernten Rechners über ein Netzwerk. Auch hier ist eine Absicherung – beispielsweise über ein Passwort – möglich.

475 *Virtual Private Network*, Überbegriff für verschiedene Protokolle (z.B: IPSEC, OpenVPN und PPTP), die die Verbindung mit einem nichtöffentlichen Computernetzwerk ermöglichen, indem sie durch ein als unsicher vermutetes Netzwerk wie z.B. das Internet einen verschlüsselten Tunnel öffnen, durch den sämtlicher Datenverkehr zwischen den Endpunkten geleitet wird.

476 *Ion/Reeder/Consolvo*, 331 ff.

Demzufolge sollte in erster Linie die verwendete Software stets auf dem aktuellen Stand gehalten werden, um bekannt werdende Sicherheitslücken zeitnah zu reparieren, und Zurückhaltung insbesondere beim Ausführen von Programmen aus dem Internet, wozu allerdings auch aktive Inhalte auf Webseiten wie Adobe Flash-Programme oder Java- bzw. JavaScript-Programme gehören, geübt werden. Für die zweite Variante, dem Ausnutzen von Sicherheitslücken in verwendeten Programmen, kann eine Firewall einen gewissen (aber auch hier wieder keinen absoluten) Schutz gewährleisten, insbesondere durch das Sperren des Fernzugriffs auf alle bis auf die wirklich unbedingt für die Nutzung benötigten Dienste. Neben dem Halten der verwendeten Software auf dem neusten Stand dürften das Verfolgen der einschlägigen Nachrichtenquellen für bekannt werdende Sicherheitslücken und die Schulung der Nutzer die wohl wichtigsten Verteidigungsinstrumente darstellen.

Nur ergänzend soll erwähnt werden, dass für einen Angreifer mit entsprechender krimineller Energie und Motivation auch das Ausspähen von Speicher- und Bildschirminhalten aus einiger Entfernung durch das Abfangen der elektromagnetischen Abstrahlung der verwendeten PCs oder von deren Peripheriegeräten möglich ist. Angriffe auf die elektromagnetischen Abstrahlungen von Bildschirmen haben unter dem Namen TEMPEST auch eine gewisse mediale Aufmerksamkeit erfahren.[477] Maßnahmen hiergegen unterliegen jedoch aufgrund des recht hohen Aufwandes einer wirksamen Verteidigung einer genauen Kosten-Nutzen-Analyse, da anzunehmen ist, dass diese Angriffe wegen der erforderlichen Kenntnisse allenfalls durch spezialisierte Angreifer mit einen großen Interesse an dem Angriff durchgeführt werden, jedoch keine flächendeckende Bedrohung, wie sie beispielsweise durch Schadsoftware gegeben ist, darstellen.

4.8.2 Angriffe auf dem Übertragungsweg

Angriffe, die darauf abzielen, unbefugt Kenntnis von Daten zu erlangen oder diese zu verändern, können auch auf dem Übertragungsweg stattfinden. Hierbei können Angriffe sowohl auf ein öffentliches Netzwerk wie das Internet als auch auf das private (lokale) Netzwerk eines der Kommunikationsteilnehmer erfolgen. Zur ersten Variante gehört zunächst die technische Übertragungsinfrastruktur im engeren Sinne, nämlich das Glasfasernetz (Backbone), das das eigentliche Internet bildet, und die Telefon- und Kabelnetze, die den Anschluss der Endnutzer an das Internet ermöglichen. Je nach verwendetem Kommunikationsprotokoll können auch noch von

477 *Schmundt*, Der Spiegel 14.8.2006, Datendiebstahl.

Dritten (d.h. nicht mit den Kommunikationsteilnehmern identischen natürlichen oder juristischen Personen) betriebene Server hinzutreten, beispielsweise Mailserver eines E-Mail-Anbieters, Webserver und dergleichen. Ein Angriff auf die Übertragungsleitungen selbst ist wegen der regelmäßig besseren Absicherung der öffentlichen Kommunikationsnetze schwieriger, da hierfür ein physischer Zugang zu dem Übertragungsweg (wie z.B. die Glasfaserkabel des Backbones oder den für den angegriffenen Kommunikationsteilnehmer zuständigen Outdoor-DSLAM oder Mobilfunkmast) erforderlich ist. Realistischer sind Angriffe auf die verwendeten Kommunikationsserver. Zwar sind auch diese Angriffe regelmäßig schwierig, allerdings werden auf Serverebene auch immer wieder kritische Schwachstellen sowohl bei zugrunde liegenden Technologien[478] als auch der Implementierung bei einzelnen Anbietern[479] bekannt, die Dritten Zugriff auf übertragene oder dort gespeicherte Daten ermöglichen.

Das wohl größte Risiko stellt schließlich ein Zugriff auf das private Netzwerk des Nutzers dar. Einen möglichen Angriffspunkt bieten hier insbesondere Funktechnologien wie WLAN, da Angriffe auf diese regelmäßig auch noch in einiger räumlicher Entfernung zum Ziel – je nach baulichen Gegebenheiten, Sichtverbindung und WLAN-Standard bis ca. 250 Meter[480] – möglich sind. Bei kabelgebundenen Netzwerken ist hingegen eine physikalische Verbindung notwendig, die regelmäßig mit einem größeren Entdeckungsrisiko für den Angreifer verbunden ist. Gerade bei zum Teil für Dritte zugängliche Räume wie beispielsweise einer Kanzlei ist aber hier an Netzzugangspunkte wie beispielsweise nicht verwendete, aber dennoch mit dem Netzwerk verbundene Netzwerkbuchsen zu denken, die von einem böswilligen Dritten als Eintrittspunkt in das Kanzleinetzwerk genutzt werden könnten.

Wenngleich die Angriffe auf öffentliche Kommunikationsnetze schwieriger sind als auf private, ist die Annahme, diese könnten nicht kompromittiert werden, durch die Enthüllungen des Whistleblowers und Ex-NSA-Mitarbeiters Edward Snowden als widerlegt anzusehen. Danach haben mindestens die Geheimdienste der USA (NSA) und von Großbritannien (GCHQ) über Jahre in einen Großteil der weltweiten Internetkommunikation mitgeschnitten und systematisch ausgewertet.[481] Ähnliche Überwachungsmaßnahmen für Geheimdienste anderer Länder

478 Ein sehr drastisches Beispiel hierfür ist der im April 2014 bekannt gewordene *Heartbleed-Bug* der flächendeckend im Internet genutzten *OpenSSL*-Bibliothek zur Transportverschlüsselung, der es Angreifern erlaubte, den Speicherinhalt von diese Bibliothek verwendenden Servern – einschließlich der verwendeten Zertifikatsschlüssel – auszulesen, vgl. *Bundesamt für Sicherheit in der Informationstechnik*, Pressemitteilung vom 11.4.2014.

479 So wurde im August 2015 eine Sicherheitslücke bei den großen E-Mail-Anbietern 1&1, GMX und web.de bekannt, die Dritten unter bestimmten Umständen Zugriff auf fremde E-Mail-Postfächer erlaubt hätte, vgl. *Schirrmacher*, WebMail.

480 *Tjensvold*, 3 f.

481 Eine gute Übersicht der als NSA-Skandal bekannt gewordenen Ereignisse bietet *Beuth*, ZEIT ONLINE vom 28.10.2013, 1.

auszuschließen, erscheint unrealistisch. Auch die Annahme, dass nur Geheimdienste unter strengster Kontrolle und gesetzlicher Regulierung nur bestimmten Datenverkehr analysieren, geht fehl, zumal auch innerhalb der NSA Fälle von Missbrauch der gesammelten Daten bekannt geworden sind.[482] Es ist vielmehr davon auszugehen, dass durch den menschlichen Faktor keine hundertprozentige Kontrolle und Sicherheit einmal gespeicherter Daten gegeben ist, so dass anderweitige Schutzmaßnahmen ergriffen werden müssen. Hierfür bietet sich beispielsweise eine Verschlüsselung von Daten insbesondere auf dem Transportweg an.

Bei der Benutzung von WLAN sollte eine Verschlüsselung nach dem Stand der Technik (z.B. WPA2 mit AES-Verschlüsselung) benutzt werden, Maßnahmen wie das Verstecken der Netzwerkkennung (SSID) oder das Zulassen nur bestimmter Hardwareadressen (MAC-Adress-Filterung) bieten hingegen aufgrund der leichten Umgehbarkeit keinen nennenswerten Schutz.[483] Für kabelgebundene Netzwerke sollte der Zugriff auf Netzwerkschnittstellen reguliert werden, indem beispielsweise nicht benutzte Netzwerkbuchsen physisch vom Netzwerk getrennt werden.

4.8.3 Angriffe an den Endpunkten der Kommunikation

Schließlich können sowohl Kommunikationsverbindungen als auch gespeicherte Daten angegriffen werden, indem der kommunizierende bzw. speichernde Rechner selbst kompromittiert wird. Hierfür existiert eine Vielzahl von Schadprogrammen, insbesondere sogenannte *Trojanische Pferde* (kurz *Trojaner*), d.h. Programme, die vorgeben, eine nützliche Funktion zu haben, zugleich jedoch Schadroutinen enthalten, um beispielsweise Daten zu kopieren oder Passworteingaben mitzuschneiden. Zudem gibt es mit *Spyware* und *Adware* eine verwandte Kategorie von Programmen, die zwar nicht direkt auf Angriffe auf Rechner ausgelegt ist, jedoch ebenfalls in einem vom Nutzer regelmäßig nicht erwünschten Umfang Daten sammelt oder Werbung einblendet. Wenngleich hier ein Nutzer durchaus mit diesem Umstand einverstanden sein kann, besteht eine Gefahr in der unsicheren Speicherung oder Übertragung der gesammelten Daten oder der fehlerhaften Programmierung, die jeweils wieder Ansatzpunkte für einen Angreifer sein können, Zugang zum System oder auf die Daten zu erlangen.

Als Einfallspunkte für Schadsoftware bietet sich zum einen das Internet an, über das beispielsweise massenhaft E-Mails mit Schadsoftware als Anhang versendet wird. Diese Angriffe sind in der Masse nicht gezielt, sondern sollen möglichst viele Nutzer erreichen, beispielsweise um durch

482 *Peterson*, washingtonpost.com vom 24.8.2013, The Switch.
483 *Geier*, Myth No. 1, 2.

erpresserische Manipulationen an Daten Betroffene zur Zahlung von Geld an die Angreifer zu veranlassen (sogenannte *Erpressungstrojaner* bzw. *Ransomware*[484]). Eine weitere Methode ist die Verbreitung von Schadsoftware über manipulierte Webseiten, was durch die Einbindung von Werbung Dritter auf vielen Seiten selbst seriöse Angebote treffen kann, die in Unkenntnis des schädlichen Inhalts beispielsweise ein manipuliertes Werbebanner eines Angreifers einbinden.[485]

Aber auch gezielte Angriffe sind natürlich möglich und werden auch so praktiziert, zum Beispiel indem eine E-Mail mit Schadsoftware gezielt an eine oder mehrere Personen gesendet wird, deren Rechner kompromittiert werden soll.

Ein weiterer Angriffsvektor, um Systeme mit Schadsoftware zu infizieren, ist das gezielte Platzieren eines Datenträgers mit der Schadsoftware in Reichweite des Angegriffenen, damit dieser aus Neugier den Datenträger in seinem PC einliest und so die Schadsoftware installiert. Diesen Angriff sollte man nicht unterschätzen, da er insbesondere bei großen Organisationen auf den am wenigsten sicherheitsbewussten Mitarbeiter als „schwächstes Glied in der Kette“ abzielt. Es wird zum Teil vermutet, dass beispielsweise der (äußerst professionelle) Hacker-Angriff auf die iranischen Anlagen zur Uranaufbereitung mittels des Computerwurms *Stuxnet* auf diesem Weg begonnen hat.[486]

Schließlich ist ein Angriff auf einzelne Rechner auch durch sogenanntes *Social Engineering* möglich. Hierunter versteht man das Ausnutzen des menschlichen Faktors durch Täuschung, Bestechung, Bedrohung oder ähnliche manipulative Maßnahmen gegenüber Menschen, die Zugriff auf die Rechner haben, die das Angriffsziel darstellen. Auch diese Bedrohung sollte man nicht unterschätzen, da hierdurch auch technisch sehr gut abgesicherte Systeme kompromittiert werden können. Gerade im Bereich der Täuschung erfordern solche Angriffe nur wenige Ressourcen und bringen für den Angreifer allenfalls ein geringes Risiko mit sich. So kann ein Angreifer sich beispielsweise telefonisch als Mitarbeiter des Technikdienstleisters des Angegriffenen auszugeben und diesen so zur Bekanntgabe seiner Zugangsdaten oder zur Installation von Schadsoftware zu überreden. Gegen diese Angriffsszenarien hilft in erster Linie eine Schulung aller Beteiligten im Bezug auf Sicherheitsfragen und -gefahren im Zusammenhang mit sensiblen Daten.

484 *Bundesamt für Sicherheit in der Informationstechnik*, digitale Erpressungswelle.
485 *Segura*, Malvertising.
486 *Falliere/O Murchu/Chien*, 3.

4.9 Fazit zu den Unterschieden zwischen papierbasierter und elektronischer Kommunikation

Wie die vorhergehenden Betrachtungen gezeigt haben, gibt es wesentliche Unterschiede zwischen papierbasierter und elektronischer Kommunikation. Diese Eigenschaften können Vor- aber auch Nachteile mit sich bringen. Oft sind die Eigenschaften auch ambivalent, so dass sich nur in Verbindung mit dem jeweiligen Kontext ergibt, ob in einer Eigenschaft ein Vorteil oder ein Nachteil für diese Art der Nachrichtenübertragung gesehen werden kann. Beispielsweise bringt die Möglichkeit der spurlosen und verlustfreien Kopierbarkeit Vorteile hinsichtlich der Lesbarkeit und der Erhaltung von Daten mit sich, da Effekte wie die sich stetig verschlechternde Bildqualität mehrerer Instanzen von Fotokopien vermeiden lassen. Andererseits werden hierdurch auch Gefahren eröffnet, da bisher aus der Papierwelt bewährte Strategien zum Umgang mit Medien in der elektronischen Welt keine oder nur noch eingeschränkte Geltung haben. Im Beispiel der Fotokopien wäre der Nachteil darin zu sehen, dass einem Dokument nicht mehr ansehbar ist, ob es sich um ein Original oder eine Kopie handelt, was beispielsweise bei vollstreckbaren Ausfertigungen und ähnlichen Anwendungen, die Wirkungen aus der Originalität eines Dokuments ableiten, zu berücksichtigen ist. Auch Eigenschaften wie die Automatisierbarkeit – mit dem Vorteil der schnellen Weiterverarbeitung von Dokumenten und dem Nachteil der Persönlichkeitsrechtsgefährdung durch hierdurch ermöglichte ganz neue Verknüpfung von scheinbar ungefährlichen Daten – oder die Miniaturisierung von Datenspeichern – mit dem Vorteil der Platzersparnis und des erleichterten Transports und dem Nachteil des erhöhten Schadenspotentials bei Diebstahl oder sonstigem Abhandenkommen solcher Datenspeicher – erfordern eine neue Herangehensweise an elektronische Kommunikation, die sich nicht im bloßen Ziehen von Analogien auf die papierbasierte Kommunikation erschöpfen darf. Mit der Erleichterung der Kopierbarkeit und der fehlenden Nachvollziehbarkeit von Änderungen schließlich treten auch Gefahren für die Integrität und die Authentizität von Nachrichten zu Tage, denen mit einer entsprechenden Gestaltung eines elektronischen Rechtsverkehrs begegnet werden muss.

Im Folgenden Abschnitt sollen die hier gewonnenen Kenntnisse nun genutzt werden, um Kriterien für einen elektronischen Rechtsverkehr aufzustellen, der diesen Besonderheiten gerecht zu werden versucht.

5 Voraussetzungen an den elektronischen Rechtsverkehr mit den Gerichten

Nachdem die Grundlegenden Eigenschaften elektronischer Kommunikation im Sinne dieser Betrachtung herausgearbeitet wurden, soll versucht werden, abstrakte Anforderungen an einen elektronischen Rechtsverkehr mit den Gerichten aufzustellen. Ziel dieses Abschnittes ist es, ein Gerüst zu schaffen, anhand dessen im darauf folgenden dritten Teil der Arbeit der geplante verpflichtende elektronische Rechtsverkehr mit den Gerichten mittels EGVP oder dem besonderem elektronischen Anwaltspostfach als dessen Anwendung untersucht und bewertet werden kann. Hierfür werden ausgehend von den im vorhergehenden Kapitel 4 erarbeiteten Besonderheiten elektronischer Kommunikation die abstrakten Kriterien zur Bewertung des elektronischen Rechtsverkehrs aufgestellt.

5.1 Authentizität und Integrität der Daten

Da durch die Besonderheiten der elektronischen Kommunikation auch neue Gefährdungen für Kommunikationsprozesse entstehen[487], muss beim elektronischen Rechtsverkehr besonderes Augenmerk auf die Kompensation dieser Nachteile gelegt werden. Insbesondere die Integrität und Authentizität von Nachrichten sind durch die einfacher durchzuführenden und schwerer oder in manchen Fällen gar nicht zu entdeckenden Manipulationsmöglichkeiten sowie die Gefahr unbeabsichtigter Fehler durch technisches Versagen oder Fehlbedienung zu schützen, um eine der Papierform ebenbürtige Sicherheit des elektronischen Rechtsverkehrs gewährleisten zu können.

5.1.1 Integritätsschutz

Ein unabdingbares Kriterium bei elektronischer Kommunikation ist die Sicherstellung der Integrität der übertragenen Daten. Der Begriff Integrität beschreibt dabei die Frage, ob die Daten genau so beim Empfänger ankommen, wie sie beim Absender versendet wurden. Eine der Besonderheiten elektronischer Kommunikation ist die spurlose Veränderbarkeit, wodurch sowohl Integrität als auch Authentizität der Daten stärker als bei papiergebundener Kommunikation gefährdet werden.[488] Um

487 Vgl. hierzu oben unter 4.2.
488 Vgl. hierzu bereits oben unter 4.2.1.

diesen – sich jedenfalls aus einer Beweissicherheitsperspektive so darstellenden[489] – Nachteil auszugleichen, muss bei Kommunikation im Rahmen des elektronischen Rechtsverkehrs besonderer Wert auf die Erhaltung der Integrität der übermittelten Nachrichten gelegt werden. Zur Vermeidung von Änderungen durch Übertragungsfehler bieten einerseits die gängigen Internetprotokolle einen gewissen Schutz. So verfügt das auch für die Auslieferung von Websites im World Wide Web (das nicht deckungsgleich mit dem Internet ist)[490] verwendete TCP/IP-Protokoll über eine eingebaute Fehlerkorrektur. Diese vergibt für jedes versendete Datenpaket eine Identifikationsnummer (die sogenannte Sequenznummer), und sieht für den Empfang jedes Datenpakets eine Bestätigung der Gegenseite vor. Bleibt eine solche Bestätigung aus, versendet der Absender ein „verlorenes“ Paket noch einmal.[491] Andere Übertragungsprotokolle wie das für Echtzeitübertragungen verwendete UDP bieten solche Fehlerkorrekturmechanismen jedoch nicht, womit sie eine bessere Leistung mit einer – bei manchen Übertragungen unschädlichen – erhöhten Fehlerneigung erkaufen.[492] Auf einer höheren Protokollebene[493] empfehlen sich jedoch Verfahren, die nicht nur gegen zufälligen Untergang oder zufällige Veränderung von Datenpaketen schützen, sondern auch vor gezielten Angriffen auf die Integrität der übertragenen Daten. Hierzu bieten sich insbesondere Prüfsummenverfahren an. Diese können sicherstellen dass die Daten in der Form angekommen sind, wie sie vom versendenden System verschickt wurden. Zur Vermeidung von Angriffen böswilliger Dritter auf die Kommunikation ist hierbei kryptografisch abgesicherten Verfahren der Vorzug zu geben, da einem Angreifer, der den Inhalt einer Nachricht verändern kann, in der Regel ebenso die Veränderung der ja auch elektronisch übertragenen Prüfsumme möglich sein wird. Weil solche Verfahren auch im Rahmen von (mindestens fortgeschrittenen) elektronischen Signaturen verwendet werden, geht mit Nutzung einer solchen elektronischen Signatur auch eine Sicherstellung der Integrität der Nachricht einher. Bei Nichtnutzung einer mindestens fortgeschrittenen

489 Tatsächlich ist die spurlose Veränderung von Daten nicht immer eine unerwünschte Eigenschaft, bietet sie doch beispielsweise die Möglichkeit, eigene Fehler zu korrigieren, bevor mögliche Empfänger von diesem Kenntnis erlangen. In manchen Feldern wie dem Persönlichkeitsrechtsschutz im Internet wird zum Abstellen einer Rechtsverletzung vom Verletzer sogar ausdrücklich verlangt, dass er die verletzende Äußerung entfernt und aus allen gängigen Cachingdiensten und Suchmaschinen löschen lässt (so z.B. BGH NJW 2014, 2180, 2182 f.). Eine Rekonstruktionsmöglichkeit der ursprünglich rechtsverletzenden Äußerung wäre hier kontraproduktiv.

490 Das World Wide Web stellt lediglich einen Dienst im Internet dar, mit dem untereinander mittels Hyperlinks verknüpfte Dokumente über das Hypertext Transfer Protocol (HTTP) ausgeliefert werden können. Andere Dienste im Internet beinhalten solche für elektronische Post/E-Mail (z.B. POP3 oder IMAP), Dateiübertragung (z.B. FTP), Videokonferenzen (z.B. SIP) und textbasierte Chats (z.B. IRC).

491 RFC-793, 4, „Reliability“, abrufbar unter https://tools.ietf.org/html/rfc793, zuletzt abgerufen am 18.12.2017.

492 RFC-768, 1, „Introduction“, abrufbar unter https://tools.ietf.org/html/rfc768, zuletzt abgerufen am 18.12.2017.

493 Nach dem gebräuchlichen OSI-Schichtenmodell, dass Netzwerkverkehr in 7 hierarchisch geordnete Schichten unterteilt, befinden sich die Protokolle für den Transport von Datenpaketen wie TCP und UDP auf der 4. Schicht. Im hier verwendeten Kontext bedeutet höhere Protokollebene eine steigende Abstraktion bis hin zur Anwendungsebene auf Layer 7; vgl. zum OSI-Schichtenmodell ITU-T Recommendation X.200 (07/94), abrufbar unter https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items, zuletzt abgerufen am 18.12.2017, 28.

elektronischen Signatur muss durch technische Vorkehrungen anderweitig sichergestellt werden, dass die Integrität der übertragenen Daten gewahrt bleibt.[494]

Wie bei allen Sicherheitstechniken ist jedoch stets zu berücksichtigen, dass es eine absolute Sicherheit nicht geben kann und damit eine jede Entscheidung für oder gegen eine Sicherungsmaßnahme stets das Ergebnis einer Abwägung zwischen Kosten und Nutzen sein muss. So ist einerseits zu berücksichtigen, wie hoch der Aufwand und die Kosten einer elektronischen Signierung von zu übermittelnden Daten sind, andererseits welche Bedrohungen der Daten realistischerweise erwartet werden können, und schließlich wie groß der mögliche Schaden im Falle einer Integritätsverletzung der Daten wäre. Zu trennen ist zwischen einer elektronischen Signierung der Daten in einer Art, die diese untrennbar mit dem Aussteller verknüpft, wie die qualifizierte elektronische Signatur nach Signaturgesetz es gewährleistet, und einer Integritätssicherung im Sinne einer (bloßen) Transportsicherung, so dass zwar eine Veränderung der Daten auf dem Transportweg ausgeschlossen werden kann, nicht aber ein Auseinanderfallen von tatsächlicher und vorgeblicher Urheberschaft der Daten. Kritiker des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten haben an den Gesetzesentwürfen verschiedentlich bemängelt, diese würden ohne Not auf die bewährte und bestätigte Sicherheit der qualifizierten elektronischen Signatur verzichten.[495] Andererseits wurde die Lockerung des Signaturerfordernisses damit begründet, dass die qualifizierte elektronische Signatur in der Praxis zu unhandlich wäre und deshalb kaum Verwendung finden würde.[496] Dem ist zuzugeben, dass nach der Konzeption des Signaturgesetzes jedenfalls finanzielle Aufwendungen nötig sind, um eine qualifizierte elektronische Signatur nutzen zu können. Kosten fallen insbesondere an für einen geeigneten Kartenleser – empfohlen werden hier oft aus Sicherheitsgründen zudem Geräte, die über eine eigene Tastatur und ein Display verfügen und dadurch zumindest im Vergleich zu einfacheren Geräten verhältnismäßig teuer sind[497] – sowie das qualifizierte elektronische Zertifikat auf einer Chipkarte, das eine begrenzte Laufzeit[498] hat und danach kostenpflichtig durch ein neues ersetzt werden muss.

494 So im Ergebnis auch *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 4, die an dem Erfordernis der qualifizierten elektronischen Signatur für bestimmende Schriftsätze grundsätzlich festhalten wollen, allerdings eine Herabsetzung des Sicherheitsniveaus bei Versand über das besondere elektronische Anwaltspostfach befürworten.

495 So beispielsweise der Deutsche Anwaltverein in seinen Stellungnahmen zum ERV-Gesetz *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 3 f.; *Volk/Burianski/Feil/Redeker u. a.*, DAV-Stellungnahme 87/2012, 8f.

496 So schon der erste Regierungsentwurf zum ERV-GesetzERV-Gesetz, BR-Drs. 818/12, 1 sowie der schließlich angenommene Regierungsentwurf, BT-Drs. 17/12634, 1.

497 So verweist die Bundesrechtsanwaltskammer für das besondere elektronische Anwaltspostfach auf ein Dokument, das eine Reihe von Kartenlesegeräten empfiehlt (*Zertifizierungsstelle der Bundesnotarkammer (Hrsg.)*, Anleitung beA-Schlüsselverwaltung, 3), die nach der aktuellen Preisliste des Herstellers zwischen rund 70 und rund 160 Euro kosten.

498 Nach § 14 Abs. 3 SigV beträgt dabei die (derzeit) maximal erlaubte Gültigkeitsdauer eines qualifizierten elektronischen Zertifikats zehn Jahre.

Da der Unterschied zwischen qualifizierter elektronischer Signatur und fortgeschrittener elektronischer Signatur aber in organisatorischen Maßnahmen (Verwendung von getrennten Sicherungsmitteln[499], besondere Pflichten für Zertifizierungsdiensteanbieter[500]) begründet liegt und eine fortgeschrittene elektronische Signatur technisch die gleiche Sicherheit bieten kann, spräche aus Integritätssicht nichts gegen eine Absenkung des Sicherheitsniveaus für den elektronischen Rechtsverkehr auf mindestens eine fortgeschrittene elektronische Signatur.

5.1.2 Authentizitätsschutz

Über den Schutz der Integrität hinaus bestehen bei elektronischer Kommunikation auch Gefährdungen für die Authentizität von Nachrichten. Authentizität beschreibt dabei das Auseinanderfallen von scheinbarem und tatsächlichem Aussteller[501]. Eine Integritätsverletzung wäre das Verändern einer Nachricht, die aber (bis auf die Änderungen) tatsächlich von dem Absender kommt, der auch für den Empfänger erkennbar ist, eine Authentizitätsverletzung demgegenüber das (unautorisierte) Versenden einer Nachricht unter dem Namen eines anderen Absenders durch einen Dritten. Wie der Integritätsschutz hat auch der Schutz der Authentizität erhebliche Bedeutung für den elektronischen Rechtsverkehr, da durch gefälschte prozesserhebliche Erklärungen erhebliche Schäden entstehen können. Auch die Authentizität kann durch elektronische Signaturverfahren gewährleistet werden. Der technische Vorgang der Bildung einer Prüfsumme und die Verschlüsselung dieser Prüfsumme mit dem eigenen privaten Schlüssel gewährleisten jedoch nur die Integrität der Nachricht. Zwar ist von der (technischen) Beweiskraft einer mindestens fortgeschrittenen elektronischen Signatur auch die Unterschrift unter einem Dokument erfasst, so dass bezüglich dieser eine Veränderung auf dem Transportweg ausgeschlossen werden kann. Was damit noch nicht gewährleistet ist, ist jedoch, dass diese Unterschrift auch tatsächlich von dem erkennbaren Aussteller und nicht etwa von einem Dritten stammt.[502] Gewähr hierfür kann lediglich dadurch gegeben werden, dass das verwendete Signaturzertifikat durch eine vertrauenswürdige Instanz auch sicher einer bestimmten berechtigten Person zugeordnet ist. Dies entspricht dem Sicherheitsniveau der qualifizierten elektronischen Signatur, bei dem der Zertifizierungsdiensteanbieter den Inhaber eines qualifizierten Zertifikates zuverlässig identifizieren

499 § 2 Nr. 3, Nr. 10 SigG i.V.m. § 15 SigV.
500 § 2 Nr. 3, Nr. 7 i.V.m. §§ 4 – 14 SigG.
501 Vgl. hierzu bereits oben unter 4.2.2.
502 Damit entspricht der so „unterschriebene“ Text praktisch dem Sicherheitsniveau einer einfachen elektronischen Signatur im Sinne des Signaturgesetzes, vgl. hierzu oben unter 2.3.2.

muss.

5.1.3 Konsistenz der Daten

Neben Authentizität und Integrität der übertragenen Daten ist auch die Konsistenz des gesamten Kommunikationsvorgangs zu berücksichtigen. Hierunter ist zu verstehen, dass die versendeten und die empfangenen Daten inklusive eventueller Metadaten auch übereinstimmen. Soweit man die Konsistenz der Nachricht auf den eigentlichen Nachrichteninhalt bezieht, liegt insofern eine Überschneidung mit der Integrität der Nachricht vor. Gleichwohl soll die Konsistenz hier als separater Punkt behandelt werden, um klarzustellen, dass der Schutz der Integrität sich nicht nur auf den eigentlichen Nachrichteninhalt beziehen sollte, sondern auch auf die mitversendeten Metadaten. Zu diesen gehören alle Angaben, die der Datei anlässlich des Versendens beigefügt werden. Bei einer E-Mail sind dies beispielsweise im Kopf der Nachricht (dem sogenannten E-Mail-Header[503]) enthaltene Informationen. Diese umfassen unter anderem Informationen über das vom Versender verwendete E-Mail-Programm, Namen und E-Mail-Adresse von Absender und Empfänger[504] und den mit Zeitstempeln dokumentierten Weg, den die Nachricht vom Rechner des Absenders über verschiedene Mailserver bis zum Empfänger nahm.[505] Für den elektronischen Rechtsverkehr ist hier darauf zu achten, dass – sofern die in den Metadaten enthaltenen Informationen wie Sende- und Empfangszeitpunkte eine Beweiswirkung erbringen sollen, technisch sichergestellt sein muss, dass diese Daten möglichst aussagekräftig sind. Bei der gewöhnlichen E-Mail ist eine Fälschbarkeit dieser Metadaten derart leicht möglich, dass beispielsweise Versender von massenhaften unerwünschten Nachrichten („Spam“) sich hinter einer faktischen Anonymität verstecken. Kernproblem der E-Mail ist, neben dem Vertrauen an den Mailserver, er werde die Metadaten korrekt eintragen, auch die Verfügbarkeit von unzureichend abgesicherten Mailservern überall auf der Welt, die praktisch beliebigen Dritten einen Zugriff und damit die Möglichkeit, Mails mit gefälschten Absender- und Transportangaben zu versenden, gewähren.[506] Sofern für den elektronischen Rechtsverkehr ein in sich geschlossenes System wie das EGVP oder das beA benutzt wird, dürfte zwar die Sicherung der verwendeten Server durch ein sehr homogenes System, das zudem unter der Kontrolle jeweils nur einer Stelle steht, deutlich einfacher fallen. Sichergestellt werden muss aber dennoch, dass eine sorgfältige Dokumentation des Weges jeder Nachricht erfolgt,

503 RFC-5322, abrufbar unter https://tools.ietf.org/html/rfc5322, zuletzt abgerufen am 18.12.2017, 7.
504 RFC-5322, abrufbar unter https://tools.ietf.org/html/rfc5322, zuletzt abgerufen am 18.12.2017, 22 f..
505 RFC-5322, abrufbar unter https://tools.ietf.org/html/rfc5322, zuletzt abgerufen am 18.12.2017, 30.
506 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1210 f.

um späteren Beweisschwierigkeiten aus dem Weg zu gehen. Sofern sowohl die verwendete Software als auch die Server, die die Mail transportieren, Zeitstempel erstellen, müssen diese die gleiche Referenzzeit verwenden. Um dies sicherzustellen, ist es nötig eine vertrauenswürdige Instanz als Quelle für Zeitstempel festzulegen, um Abweichungen (beispielsweise durch eine falsch eingestellte Systemzeit des Absenders) zu vermeiden. Neben dem Schutz vor zufälligen Abweichungen ist hier insbesondere an bösgläubige Kommunikationsteilnehmer zu denken, die die eigene Systemzeit bewusst falsch einstellen, um sich später einen prozessualen Vorteil (beispielsweise die scheinbare Wahrung einer Frist) hierdurch zu sichern.

5.1.4 Authentizität, Integrität und Konsistenz bei Medienbrüchen

Ein Sonderproblem stellt die Gewährleistung von Authentizität, Integrität und Konsistenz von Daten im Fall eines Medienübergangs („Medienbruch“) dar. Ein solcher liegt beispielsweise vor, wenn ein körperlich vorliegendes Dokument wie eine Urkunde in die digitale Form überführt werden soll. Bedrohungen liegen hierbei weniger in gezielten Angriffen Dritter (wenngleich solche natürlich ebenso wie bei der Übertragung von Daten über das Internet nicht völlig auszuschließen sind), da die Angriffsfläche hierfür deutlich kleiner ist. Eine Gefahr liegt jedoch in unbeabsichtigten Fehlern, die sich bei der Übertragung einstellen können. Diese reichen von trivial zu beseitigenden Fehlern wie der nicht vollständigen Erfassung des Scangutes bis hin zu komplexen technischen Fehlfunktionen wie der Änderung (!) von Zeichen aufgrund der vom Scangerät oder der Scansoftware verwendeten Kodierung oder Komprimierung[507]. Auch muss berücksichtigt werden, dass naturgemäß durch einen Scan nicht alle Eigenschaften eines körperlichen Gegenstands vollständig wiedergegeben werden. Sofern es nur auf den textlichen und bildlichen Inhalt ankommt, ist dies hinzunehmen. In Sonderfällen jedoch, in denen beispielsweise später die Echtheit einer Unterschrift durch ein graphologisches Gutachten geprüft werden muss, müssen hierfür jedoch Vorkehrungen getroffen werden, wie beispielsweise die Aufbewahrung des eingescannten Dokuments zu späteren Beweiszwecken.

Das Bundesamt für Sicherheit in der Informationstechnik hat mit der Technischen Richtlinie Ersetzendes Scannen (TR-RESISCAN)[508] Anforderungen aufgestellt, an denen sich Verantwortliche für Scanprozesse orientieren können. Sie befasst sich mit der Vorbereitung von Dokumenten für den Scan, dem eigentlichen Scannen, der Nachverarbeitung und der abschließenden

507 Vgl. hierzu bereits oben unter 4.2.1.
508 Siehe hierzu oben unter 3.1.7.

Integritätssicherung. Die spätere (beweiswerterhaltende) Aufbewahrung jedoch ist kein Bestandteil der Richtlinie.[509] Sie stützt sich dabei auf eine Schutzbedarfsanalyse durch die Scanverantwortlichen, um aufbauend auf dem IT-Grundschutzkatalog eine dem jeweiligen Schutzbedarf der Dokumente entsprechende Sicherheitsstufe zu erreichen. Die Verwendung von Kompressionsverfahren, die systematische Veränderung von Zeichen erlauben (sog. „Symbol Coding"), ist nach der TR-RESISCAN nicht zulässig.[510] Hiermit können gerade die obengenannten gefährlichen, weil schwer entdeckbaren systematischen Fehler in Scanprodukten vermieden werden. Nach dem eigentlichen Scanvorgang muss nach der Richtlinie eine Qualitätssicherung erfolgen, die sicherstellt, dass keine relevanten Informationen verlorengegangen sind.[511] Zudem soll ein Transfervermerk erstellt werden, der unter anderem das Ergebnis der Qualitätssicherung enthält und eine Bestätigung darüber, dass das Scanprodukt bildlich und inhaltlich mit dem Original übereinstimmt.[512]

5.1.5 Rechtliche Sicherstellung von Integrität und Authentizität

Die Wahrung von Integrität und Authentizität kann durch das rechtliche Erfordernis elektronischer Signaturen sichergestellt werden.[513] Während diese sich in der Vergangenheit im deutschen Recht nach dem Signaturgesetz richteten, ist mit Inkrafttreten der eIDAS-Verordnung eine neue Rechtsgrundlage für elektronische Signaturen begründet worden. Fraglich ist jedoch, ob die Verordnung auch Verfahren für den elektronischen Rechtsverkehr erfassen soll. Nach Art. 2 Abs. 2 eIDAS-VO sollen keine Vertrauensdienste erfasst werden, die „ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden". Ausweislich des Erwägungsgrundes 21 eIDAS-VO sollten demgegenüber nur der Öffentlichkeit erbrachte Vertrauensdienste mit Wirkung gegenüber Dritten erfasst sein. Damit könnte der elektronische Rechtsverkehr nach Lesart des ERV-Gesetzes mittels EGVP und beA bereits wegen dieser Beschränkung vom Anwendungsbereichs der eIDAS-Verordnung ausgenommen sein.[514] Bei genauerer Betrachtung ist jedoch zu trennen zwischen dem elektronischen Rechtsverkehr mittels des beA einerseits und anderen Verfahren wie der Einreichung per De-Mail oder per E-Mail mit qualifizierter elektronischer Signatur andererseits.

509 *Bundesamt für Sicherheit in der Informationstechnik*, TR RESISCAN, 10.
510 *Bundesamt für Sicherheit in der Informationstechnik*, TR RESISCAN, 25.
511 *Bundesamt für Sicherheit in der Informationstechnik*, TR RESISCAN, 26.
512 *Bundesamt für Sicherheit in der Informationstechnik*, TR RESISCAN, 26 f.
513 Vgl. hierzu bereits oben unter 2.3.2.
514 So z.B. *Roßnagel*, MMR 2015, 359, 361; *Roßnagel*, NJW 2014, 3686, 3691.

5.1.5.1 Elektronische Einreichung mittels beA

Zunächst ist für die Einreichung mittels des beA das Merkmal der Öffentlichkeit zu untersuchen. Der Begriff der Öffentlichkeit dürfte hier zwar so verstehen zu sein wie der Begriff des öffentlich zugänglichen elektronischen Kommunikationsdienstes aus der Datenschutzrichtlinie für elektronische Kommunikation. Durch die Einschränkung „mit Wirkung gegenüber Dritten“ wird der an sich weite Bereich der Öffentlichkeit jedoch – im Gegensatz zur Telekommunikations-Datenschutzrichtlinie – zusätzlich eingegrenzt. Erwägungsgrund 21 eIDAS-VO konkretisiert diese Abgrenzung noch weiter, indem er feststellt, die Verordnung solle „insbesondere […] nicht die Erbringung von Vertrauensdiensten erfassen, die ausschließlich innerhalb geschlossener Systeme zwischen einem bestimmten Kreis von Beteiligten verwendet werden und keine Wirkung auf Dritte entfalten“. Dies ist im Fall des beA gegeben: Beim beA besteht eine geschlossene Benutzergruppe, nämlich sämtliche in Deutschland zugelassenen Anwälte. Wesentlich ist hierbei das Merkmal, dass die Anwaltszulassung notwendige, aber auch hinreichende Bedingung für die Einrichtung und damit den Zugang zu einem solchen Anwaltspostfach ist. Für die Anwaltszulassung wiederum ist Voraussetzung nach § 4 BRAO die Befähigung zum Richteramt nach dem Deutschen Richtergesetz[515] oder – für europäische Anwälte – das Erfüllen der Eingliederungsvoraussetzungen[516] oder das Bestehen der Eignungsprüfung[517] nach dem Gesetz über die Tätigkeit europäischer Rechtsanwälte in Deutschland. Auch ohne Zulassung erfolgt zudem eine Eintragung ins Gesamtverzeichnis und damit die Einrichtung des beA gemäß § 31a BRAO bei einer Tätigkeit als niedergelassener europäischer Rechtsanwalt im Sinne von § 2 Abs. 1 EuRAG.[518] Damit handelt es sich bei den zugelassenen Anwälten um eine geschlossene Benutzergruppe, der nicht beliebige Personen beitreten können, sondern deren Mitgliedschaft an konkrete rechtliche Kriterien und Voraussetzungen geknüpft ist. Das Erfordernis der Anwaltszulassung oder Kammermitgliedschaft begründet damit einen geschlossenen Benutzerkreis im Sinne der eIDAS-VO.[519]

Da somit der Anwendungsbereich der eIDAS-Verordnung für das beA nicht eröffnet ist, stellt sich als Folgeproblem die Frage, nach welchen Regeln sich elektronische Signaturen im Rahmen des

515 § 5 Abs. 1 DRIG.
516 §§ 11 ff. EuRAG.
517 § 16 Abs. 1 EuRAG.
518 Die etwas missverständliche Formulierung der Verweisung in § 6 Abs. 1 EuRAG, der auf §§ 31 bis 31c BRAO verweist, ist so zu lesen, dass auch für niedergelassene europäische Rechtsanwälte, die zwar Kammermitglied sind, aber keine Zulassung zur Rechtsanwaltsschaft haben, ein Eintrag in das Verzeichnis der örtlichen Rechtsanwaltskammer sowie das Gesamtverzeichnis der BRAK erfolgen soll, vgl. hierzu BT-Drs. 18/6915 25.
519 So im Ergebnis auch *Roßnagel*, Vertrauensdienste, 46; *Bundesrechtsanwaltskammer*, beA-Newsletter 14/2017,

beA dann richten, da das Signaturgesetz als mögliche Rechtsgrundlage für diese aufgehoben wurde.

Richtigerweise ist der Anwendungbereich der eIDAS-Verordnung in Erwägungsgrund 21 nur so zu verstehen, dass er eine positive Anwendbarkeit der Verordnung bestimmen soll, nicht jedoch negativ eine Bezugnahme auf die Verordnung durch andere, nicht in den Anwendungsbereich fallende Dienste verbieten möchte. Diese Lesart wird auch durch Erwägungsgrund 24 eIDAS-VO gestützt, in dem es heißt „Die Mitgliedstaaten können nationale Vorschriften für Vertrauensdienste im Einklang mit dem Unionsrecht beibehalten oder einführen, soweit diese Dienste durch die vorliegende Verordnung nicht vollständig harmonisiert sind. Vertrauensdienste, die dieser Verordnung entsprechen, sollten jedoch im Binnenmarkt frei verkehren können.“ Damit ist klargestellt, dass die eIDAS-Verordnung keinesfalls abschließend zu verstehen ist, sondern gerade auch alternative Gestaltungen außerhalb ihres Anwendungsbereichs zulässt. Erst recht muss daher die Möglichkeit bestehen, auch in Bereichen, die originär nicht in den Anwendungsbereich der Verordnung fallen, auf diese zu verweisen.

Schließlich stellt sich jedoch die Frage, ob innerhalb des beA von der Verweisungsmöglichkeit auf die eIDAS-Verordnung überhaupt Gebrauch gemacht wird. Die Einrichtungsvorschrift des § 31a BRAO nimmt selbst keinen Bezug auf elektronische Signaturen. Dies ist auch kongruent zu den prozessualen Vorschriften zur Einreichung mittels des besonderen elektronischen Anwaltspostfachs wie beispielsweise § 130a Abs. 3, Abs. 4 Nr. 2 ZPO, nach denen eine qualifizierte elektronische Signatur nur erforderlich ist, soweit nicht einer der in § 130a Abs. 4 genannten sicheren Einreichungswege benutzt wird. Eine Verpflichtung zur Benutzung qualifizierter elektronischer Signaturen gibt es somit nicht. Allerdings wird in der Rechtsanwaltsverzeichnis- und Postfachverordnung auf elektronische Signaturen Bezug genommen. So sind nach § 11 Abs. 1 RAVPV die Daten für die Eintragung in das Verzeichnis mittels automatisierter Verfahren und nach § 12 Abs. 1 die Daten für Berichtigungen, Sperrungen, Entsperrungen und Löschungen im Verzeichnis mit einer mindestens fortgeschrittenen elektronischen Signatur zu versehen. Für die Erstanmeldung am Postfach schließlich nimmt § 22 Abs. 1 RAVPV ausdrücklich Bezug auf die eIDAS-Verordnung, ohne jedoch ausdrücklich deren Anwendbarkeit zu bejahen, indem dort für Hardwarekomponenten zur Erstanmeldung am Postfach und zur Erteilung von Zugangsberechtigungen für das Postfach vergleichbare Anforderungen wie in Anhang II der eIDAS-Verordnung gefordert werden. Damit sind die Anforderungen der eIDAS-Verordnung an fortgeschrittene elektronische Signaturen und Signaturerstellungseinheiten mittelbar auch für den elektronischen Rechtsverkehr mit dem beA maßgeblich.

Abschnitt „Die qualifizierte elektronische Signatur“.

5.1.5.2 Elektronische Einreichung mittels anderer Verfahren

Einfacher stellt sich die Lage für Einreichungswege, die nicht nur Rechtsanwälten vorbehalten sind, wie dem EGVP, De-Mail oder dem Versand einer qualifiziert elektronisch signierten E-Mail dar. Da diese Einreichungswege grundsätzlich allen Interessierten offenstehen, ist das Merkmal eines geschlossenen Systems im Sinne von Erwägungsgrund 21 eIDAS-Verordnung nicht gegeben. Hieran ändert auch der Umstand nichts, dass der EGVP-Client eine spezielle Software benötigt – jedenfalls ohne Vermittler in Form von Gateway-Produkten – keine Kommunikation mit anderen Systemen wie der E-Mail ermöglicht. Da die Erstellung eines EGVP-Postfachs allen interessierten Personen ohne Weiteres möglich ist, bildet das EGVP in seiner „Grundform", also ohne das beA, kein geschlossenes System. Diese Erwägungen gelten im gleichen Maße für De-Mail-Accounts und natürlich erst recht für die normale E-Mail. Die eIDAS-Verordnung ist somit auf diese Einreichungswege unproblematisch anwendbar.

5.1.5.3 Fazit zur eIDAS-Verordnung für den elektronischen Rechtsverkehr

Nach dem oben gesagten sind die Vorschriften der eIDAS-Verordnung entweder unmittelbar (für die E-Mail mit qualifizierter elektronischer Signatur, das EGVP ohne beA und für De-Mail) oder kraft Verweisung (für das beA) auf den elektronischen Rechtsverkehr anwendbar. Dieses Ergebnis ist auch folgerichtig, da der deutsche Gesetzgeber mit der im eIDAS-Durchführungsgesetz enthaltenen Aufhebung des Signaturgesetzes dem elektronischen Rechtsverkehr ansonsten die Grundlagen für elektronische Signaturen entzogen hätte.

Wenngleich für das beA gerade keine elektronische Signatur zur Einreichung gefordert ist, bedient sich das System doch an verschiedenen Stellen elektronischer Signaturen. Dies erscheint nur konsequent, da mit dem aufgehobenen Signaturgesetz und nun nach der eIDAS-Verordnung bereits ein rechtlicher Rahmen für solche Signaturen besteht, der auch genutzt werden sollte. Für die Einreichung über das beA bleibt zudem die Nutzung einer qualifizierten elektronischen Signatur optional möglich.[520] Dies mag ein Zugeständnis an kritische Stimmen zum ERV-Gesetz sein, die in der Aufgabe des Signaturerfordernisses eine unnötige Verschlechterung des Sicherheitsniveaus sahen.[521] In jedem Fall ist die weiterhin bestehende Nutzungsmöglichkeit für qualifizierte elektronische Signaturen wünschenswert.

520 Vgl. hierzu *Bundesrechtsanwaltskammer*, beA-Newsletter, Abschnitt „Die qualifizierte elektronische Signatur".
521 Vgl. hierzu oben unter 3.1.7.

5.2 Datenschutz

Eine weitere Fragestellung im Zusammenhang mit der Einführung eines verpflichtenden elektronischen Rechtsverkehrs ist der Datenschutz. Wie bereits gezeigt, ist ab dem 5. Mai 2018 die maßgebliche Rechtsgrundlage für die datenschutzrechtliche Beurteilung des elektronischen Rechtsverkehrs die Datenschutzgrundverordnung.[522] Da der elektronische Rechtsverkehr mittels EGVP in Form des beA erst zum 1. Januar 2018 für die Anwaltschaft passiv verpflichtend wird,[523] liegen zwischen dem Beginn einer ersten Nutzungspflicht und der Anwendbarkeit der Datenschutzgrundverordnung nicht einmal fünf Monate. Dementsprechend müssen die Rechtsgrundlagen für den elektronischen Rechtsverkehr bereits jetzt den den Vorgaben der Datenschutzgrundverordnung genügen, um spätere, zu Rechtsunsicherheit führende Änderungen am System zu vermeiden.

Hinsichtlich der Rechtsanwälte als Nutzer des elektronischen Rechtsverkehrs stellt sich wie bereits für das Bundesdatenschutzgesetz auch für die Datenschutzgrundverordnung die Frage nach dem Verhältnis zwischen dieser und beruflichen Verschwiegenheitspflichten.[524] Die Datenschutzgrundverordnung selbst geht beispielsweise in Art. 9 Abs. 2 lit. i, Art. 9 Abs. 3, Art. 14 Abs. 5 lit. d sowie in Art. 90 Abs. 1 davon aus, dass neben ihr weiterhin berufsrechtliche Verschwiegenheitspflichten bestehen sollen.[525]

Wie bereits oben dargestellt gilt auch im Rahmen der Datenschutzgrundverordnung das Prinzip des Vorbehalts der Einwilligung oder des gesetzlichen Erlaubnistatbestands, welches in Art. 6 Abs. 1 DSGVO enthalten ist. Art. 6 Abs. 1 lit. f DSGVO erlaubt die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, solange die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen. Hiermit ist ähnlich wie in Art. 28 Abs. 1 Nr. 2 BDSG der Weg zu einer Interessenabwägung geebnet. Der Begriff des berechtigten Interesses ist hierbei der gleich wie in Art. 7 Abs. 1 lit. f DSRL, der auch in Art. 28 Abs. 1 Nr. 2 BDSG aufgenommen wurde, und kann somit anhand der zu diesem Begriff aufgestellten Kriterien des EuGH und des deutschen Gesetzgebers ausgelegt werden.[526] Dabei sprechen wie schon unter dem Bundesdatenschutzgesetz gute Gründe für eine Rechtfertigung der Datenverarbeitung, da die Verarbeitung personenbezogener Daten auch von Dritten im Rahmen der Mandatsberarbeitung

522 Vgl. oben unter 3.2.1.6.
523 Vgl. hierzu oben unter 3.1.7.
524 Vgl. zum Verhältnis der beruflichen Verschwiegenheitspflichten und dem Bundesdatenschutzgesetz oben unter 3.2.3.1
525 *Schantz* in *Shantz*/*Wolff*, Rn. 1362.
526 *Nebel* in Europäische Datenschutz-Grundverordnung, § 3 Rn. 109.

letztlich Teil der anwaltlichen Berufspflichten ist, und für eine effektive Rechtsdurchsetzung oft unerlässlich sein wird. Bei den möglicherweise entgegenstehenden Interessen der Betroffenen ist zu beachten, dass diese nach dem Wortlaut des Art. 6 Abs. 1 lit. f DSGVO nicht berechtigt sein müssen. Aus diesem Grund können auch illegitime Interessen des Betroffenen in die Abwägung mit einbezogen werden.[527] Dies kann insbesondere für die personenbezogenen Daten anderer Personen als der Mandanten der Fall sein – so wird beispielsweise im Zivilprozess die Gegenseite regelmäßig ein Interesse daran haben, dass ihre pesonenbezogenen Daten nicht verarbeitet werden, weil dies die Verfolgung rechtlicher Ansprüche ihres prozessualen Gegners erleichtern bzw. erst ermöglichen könnte. Im Rahmen der sodann erfolgenden Abwägung werden solche Interessen jedoch regelmäßig hinter den berechtigten Interessen des Anwalts an der gewissenhaften Mandatsbearbeitung und der Erfüllung seiner zivilrechtlichen Verpflichtungen aus der Mandatsvereinbarung zurückstehen müssen. Die Rechtfertigung von Datenverarbeitungen im Rahmen des elektronischen Rechtsverkehrs ist somit wie schon unter dem Bundesdatenschutzgesetz[528] auch unter der Datenschutzgrundverordnung gewährleistet.

Hinsichtlich der Betroffenenrechte enthält die Datenschutzgrundverordnung in Art. 14 DSGVO Verpflichtungen für den Verantwortlichen einer Datenerhebung, die nicht beim Betroffenen selbst stattfindet, diesen unter anderem über die Rechtsgrundlage der Datenverarbeitung, deren Zweck und über die Kategorien verarbeiteter Daten zu informieren. Für Berufsgeheimnisträger wie Rechtsanwälte findet sich hierzu jedoch in Art. 14 Abs. 5 lit. d DSGVO eine ausdrückliche Ausnahme, so dass diese Verpflichtung jedenfalls Rechtsanwälte hinsichtlich der vom Berufsgeheimnis geschützten Geheimnisse nicht trifft.

Auch für das Sicherheitsniveau stellt die Datenschutzgrundverordnung im Grundsatz ähnliche Anforderungen auf wie das Bundesdatenschutzgesetz vor dem 25. Mai 2018, erweitert und konkretisiert diese jedoch. Zunächst muss die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 den Grundsätzen von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz genügen,[529] unterliegen einer Zweckbindung,[530] dem Grundsatz der Datenminimierung,[531] ihre Richtigkeit muss sichergestellt sein,[532] ebenso wie eine begrenzte Speicherdauer[533] und die Integrität und Vertraulichkeit der Daten.[534] Darüber hinaus unterliegt der Verantwortliche für die Verarbeitung

527 *Schulz* in *Gola*, Art. 6 Rn. 58.
528 Vgl. hierzu oben unter 3.2.3.1.
529 Art. 5 Abs. 1 lit. a DSGVO.
530 Art. 5 Abs. 1 lit. b DSGVO.
531 Art. 5 Abs. 1 lit. c DSGVO.
532 Art. 5 Abs. 1 lit. d DSGVO.
533 Art. 5 Abs. 1 lit. e DSGVO.
534 Art. 5 Abs. 1 lit. f DSGVO.

auch noch einer Rechenschaftspflicht.[535]

Schließlich werden auch im Rahmen der Datenschutzgrundverordnung in Art. 32 DSGVO technische und organisatorische Maßnahmen gefordert, um ein hohes Schutzniveau hinsichtlich personenbezogener Daten sicherzustellen. Funktional entspricht Art. 32 DSGVO damit dem hierdurch verdrängten § 9 BDSG sowie der Anlage zu § 9 S. 1 BDSG, ohne jedoch deren Konkretisierungsgrad zu erreichen.[536] Nach Art. 32 Abs. 1 DSGVO schließen geeignete technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. a die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein, nach lit. b die Fähigkeit der dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der im Zusammenhang mit der Verarbeitung stehenden Systeme und Dienste, nach lit. c die Möglichkeit der schnellen Wiederherstellbarkeit der Verfügbarkeit und des Zugangs zu personenbezogenen Daten im Störungsfall und nach lit. e ein Verfahren zur regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen. Geprägt ist der Art. 32 DSGVO hierbei von einer umfassenden Abwägung, in die Faktoren wie Eintrittswahrscheinlichkeit und Schwere möglicher Datenschutzrisiken, der Stand der Technik Umfang, Umstände und Zwecke der Datenverarbeitung und Kosten der Implementierung von Sicherheitsmaßnahmen hineinspielen. Dementsprechend fordert Art. 32 DSGVO gerade keinen absoluten Schutz, sondern lediglich ein angemessenes Schutzniveau.[537] Insbesondere hinsichtlich der Verschlüsselung dürfen die Anforderungen jedoch nicht zu gering angesetzt werden: Im Hinblick auf die oben unter 4.8 dargestellten Bedrohungen bei gleichzeitiger Verfügbarkeit von effektiven und kostengünstigen Gegenmaßnahmen wie der Benutzung von Transport- und Inhaltsverschlüsselung sowie der Verschlüsselung von Datenträgern kann von Nutzern erwartet werden, dass sie etablierte Sicherheitsverfahren einsetzen. Spiegelbildlich hierzu müssen Technologien für den elektronischen Rechtsverkehr ebenfalls ein am Stand der Technik orientiertes Sicherheitsniveau aufweisen.

5.3 Interoperabilität

Neben der Möglichkeit einer Veränderung von Daten auf dem Übertragungsweg besteht zudem die Gefahr einer unterschiedlichen Interpretation von an sich unveränderten Daten durch Sende- und Empfangssystem. Diese Problematik zieht sich durch die gesamte IT, angefangen bei der

535 Art. 5 Abs. 2 DSGVO.
536 *Piltz* in *Gola*, Art. 32 DSGVO Rn. 4.
537 *Piltz* in *Gola*, Art. 32 DSGVO Rn. 11.

Übertragung von einfachen Textdateien bis hin zu komplexen proprietären Dateiformaten. Bereits bei der Übertragung einfacher Textdateien zwischen verschiedenen Rechnern, erst recht auch mit verschiedenen Betriebssystemen oder Betriebssystemversionen kann es Probleme durch unterschiedliche Zeichenkodierungen geben. Während ein gemeinsamer Nenner die sogenannte ASCII-Codierung[538] darstellt, gibt es bedingt durch Sprachen mit Sonderzeichen wie den deutschen Umlauten, diakritischen Zeichen (z.B. das unter anderem im Französischen benutzte Cédille-Zeichen ç) und gänzlich unterschiedlichen Buchstabensystemen wie kyrillischen oder griechischen Buchstaben bereits im europäischen Raum verschiedenste Zeichenkodierungen, über deren Benutzung bei Sender und Empfänger Einigkeit herrschen muss. Abhilfe schafft hier das komplexere Unicode-System, das in der Lage ist, eine Vielzahl von Zeichen aus den verschiedensten Schriftsystemen darzustellen. Auch über die Verwendung von Unicode muss jedoch bei den Kommunikationspartnern Einigkeit bestehen, da bei Interpretation eines Textes aus einem anderen Zeichensystem im besten Fall Auslassungen bei in der interpretierenden Zeichenkodierung fehlenden Zeichen angezeigt werden (beispielsweise in Form von Fragezeichen statt Umlauten), schlimmstenfalls der ganze Text unlesbar wird.[539]

Problematischer wird dieses Phänomen bei komplexeren Dateiformaten wie beispielsweise Microsoft Word-Dateien. Durch die fortschreitende Entwicklung der Word-Produktreihe einschließlich Portierungen auf neue Betriebssysteme wie Android oder MacOS und kompatible Office-Produkte von Drittherstellern gibt es mehrere verschiedene Versionen von Word-Dateien, die zueinander nur teilweise kompatibel sind.[540] Zwar können neuere Word-Versionen in aller Regel von älteren Versionen erstellte Dateien lesen, jedoch sind hier gerade bei komplexeren Formatierungen oder ungewöhnlichen Zeichensätzen Fehler möglich. Je nach Art und Schwere des Fehlers kann dies auch zu sinnentstellenden Fehldarstellungen beim Empfänger führen, beispielsweise wenn in einer Tabelle eingetragene Werte durch eine fehlerhaft interpretierte Formatierung in andere Zeilen oder Spalten verrutschen. Abhilfe kann hier die Verständigung auf bestimmte anerkannte Versionen der jeweiligen Textverarbeitungsprogramme und Dateiformate schaffen. Dies kann jedoch im Hinblick darauf, dass nicht jeder Anwalt Microsoft Word zum Verfassen seiner Schriftsätze benutzt, problematisch sein. Deswegen ist es nötig, neben proprietären

538 American Standard Code for Information Interchange, ein Standard zur Kodierung von Buchstaben als Zahlen, um eine letzliche Speicherung bzw. Übertragung als von Computern verarbeitbare Binärdaten zu ermöglichen.

539 Vgl. zu diesem Problem *Spolsky*, Unicode and Character Sets, Abschnitt „The Single Most Important Fact About Encodings“, der zugleich auch einen guten Gesamtüberblick über das Problem der Zeichenkodierung in IT-Systemen aus Programmierersicht gibt.

540 Eine Übersicht der verschiedenen Funktionen, die für die diversen Versionen von Word-Dateien zur Verfügung stehen, findet sich unter https://support.office.com/de-de/article/%c3%96ffnen-eines-Dokuments-in-einer-fr%c3%bcheren-Version-von-Word-45c4dd2f-bf7b-4a0d-9ff2-7b2ff6b733f0?ui=de-DE&rs=de-DE&ad=DE, zuletzt abgerufen am 18.12.2017.

Formaten wie Microsoft Word-Dateien auch zumindest standardisierte Formate[541] wie etwa das PDF-Format anzubieten. Dieses lässt sich aufgrund der recht strengen Standardisierung mit verschiedenen Programmen auf allen gängigen Betriebssystemen sowohl lesen als auch schreiben.[542]

Gleiches gilt für andere Dateiformate wie Bilddateien, Videos und Klangdateien, technische Zeichnungen, 3D-Modelle etc., für die alle eine Unzahl möglicher Dateiformate existiert. Hier muss in einer Abwägung zwischen den Kosten für die Bereitstellung entsprechender Leseprogramme und der Ermöglichung eines elektronischen Rechtsverkehrs für möglichst viele Nutzer ein sinnvoller Satz von gängigen Dateiformaten definiert werden, der jedoch auch beständig an jeweils aktuelle und verbreitete Formate angepasst werden muss. Zudem sollte für Dateiformate, die nicht von einer solchen Aufzählung erfasst sind, in begründeten Ausnahmefällen die Möglichkeit eines Zugriffs des Gerichts – sei es durch einen Fernzugriff, die Beschaffung entsprechender Software oder die Anhörung eines Sachverständigen – auf die fraglichen Daten geben. Zudem muss sichergestellt werden, dass – bei Benutzung einer Software für den elektronischen Rechtsverkehr – die Kompatibilität zwischen den Sende- und Empfangssystemen gewahrt bleibt. Dies obliegt natürlich zum Teil den Herstellern von Fachsoftware, die entsprechende Programme anbieten, bedeutet aber auch für die Anbieter von Übertragungswegen, dass ihre Softwareschnittstellen gut definiert und dokumentiert sein müssen, Änderungen rechtzeitig angekündigt werden um den Softwareherstellern Zeit für Anpassungen zu geben und – soweit dies möglich ist – Änderungen auf der Schnittstellenebene nicht die Verwendung älterer Software ausschließen (sogenannte Abwärtskompatibilität).

5.3.1 Hardware

Für den elektronischen Rechtsverkehr ist zudem die Verfügbarkeit entsprechender Hardware unabdingbar. Zum einen betrifft das natürlich die Gerichte, die geeignete Technik vorhalten müssen, um elektronische Nachrichten empfangen und weiterverarbeiten zu können, sowie analoge

541 Zwar besteht mit dem OpenDocument-Standard eine Standardisierung für ein Dateiformat, das neuere Microsoft-Word-Versionen beherrschen, jedoch weist auch dieser Standard gewisse Lücken auf, weshalb Microsoft selbst ihn bisher als lediglich optional neben dem proprietären .docx-Format, welches weiterhin die Standardeinstellung ist, anbietet, vgl. https://support.office.com/de-de/article/Unterschiede-zwischen-dem-OpenDocument-Textformat-ODT-und-dem-Word-Format-DOCX-d9d51a92-56d1-4794-8b68-5efb57aebfdc, zuletzt abgerufen am 18.12.2017.

542 Beispielsweise bietet die Berliner Verwaltung Dokumente wie Gesetzestexte, Terminzettel etc. ausnahmslos als PDF-Dateien an und empfiehlt zum Lesen dieser Dateien neben dem proprietären Adobe Acrobat-Reader den Nutzern kostenlose und zum Teil quelloffene Alternativen; vgl. z.B. https://www.berlin.de/landesverwaltungsamt/ueber-uns/artikel.230990.php, zuletzt abgerufen am 18.12.2017.

Materialien wie beispielsweise Urkunden zu digitalisieren. Problematischer dürften jedoch die Anforderungen an die Anwaltschaft sein, die im Gegensatz zur Justiz regelmäßig weder über zentrale IT-Stellen, noch durch frühere Vorstöße zur elektronischen Akte bereits über große Teile der Infrastruktur für den elektronischen Rechtsverkehr verfügen werden.[543] Der elektronische Rechtsverkehr trifft damit auf Anwaltsseite auf eine äußerst heterogene Kanzleistruktur, die von komplett analoger Mandatsbearbeitung bei Einzelanwälten oder kleineren Kanzleien bis hin zu einer umfangreichen IT-Infrastruktur mit hunderten oder gar tausenden von Rechnern in Großkanzleien reicht.[544] Extremfälle wie die vollständige Abwesenheit von Computertechnik werden sich bei einer Anschluss- und Benutzungspflicht, wie sie das ERV-Gesetz vorsieht, nicht berücksichtigen lassen. Hier stellt sich die Frage, inwieweit eine solche Pflicht im Einzelfall unverhältnismäßig sein kann, und ob gegebenenfalls Härtefallregelungen geschaffen werden können, ohne gleichzeitig die erhofften Effizienz- und Einspareffekte zu gefährden.

Für den großen Teil der bereits auf die ein oder andere Art EDV-technisch ausgerüsteten Kanzleien wird in aller Regel ebenfalls ein Aufwand durch die gegebenenfalls notwendige Anschaffung zusätzlicher Hardware wie hinreichend leistungsfähiger Scanner und Kartenleser sowie Signaturkarten für fortgeschrittene oder qualifizierte elektronische Signaturen entstehen. So rechnen nach einer Befragung im Rahmen des Soldan Berufsrechtsbarometers 2013 45% der befragten Kanzleien mit sehr hohen bis hohen Aufwänden für die Umstellung auf den elektronischen Rechtsverkehr.[545] Verfahren für den elektronischen Rechtsverkehr sind deswegen nicht zuletzt danach zu beurteilen, wie groß oder gering die – technische und finanzielle – Hürde für die verpflichteten Teilnehmer ist, an dem System zu partizipieren. Dies ist gerade im Hinblick auf die Berufsfreiheit im Sinne von Art. 12 Abs. 1 GG notwendig, um eine Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs verfassungskonform auszugestalten.

5.3.2 Software

Entsprechend der oben genannten heterogenen Hardwareausstattung in den Kanzleien ist es

543 Dieser Vorsprung der Justiz ergibt sich daraus, dass für diese jedenfalls grundsätzlich mit Erlass des Justizkommunikationsgesetzes vom 22.3.2005 durch den neuen § 298a ZPO die Möglichkeit geschaffen wurde, Prozessakten elektronisch zu führen.

544 Einen zumindest teilweisen Einblick geben die Ergebnisse einer in *Bundesrechtsanwaltskammer*, BRAK-Magazin 2/2014, 6, 7 f. veröffentlichten Studie der Bundesrechtsanwaltskammer zur Vorbereitung der Kanzleien auf den elektronischen Rechtsverkehr. Danach gaben 20% der teilnehmenden Kanzleien an, über keinen Internetzugang zu verfügen. Da es sich um eine Online-Umfrage handelte, ist jedoch mit einer hohen „Dunkelziffer“ zu rechnen.

545 *Kilian/Rimkus*, AnwBl 2014, 913, 917 f.

erforderlich, auch eine möglichst große Anzahl von – gängigen – Systemkonfigurationen zu unterstützen. Sofern für die Teilnahme am elektronischen Rechtsverkehr spezielle Software auf den Teilnehmersystemen benötigt wird, ist dafür zu sorgen, dass diese eine möglichst große Zahl von verbreiteten Hardwarekonfigurationen und Betriebssystemen unterstützt. Zwar ist davon auszugehen, dass der weitaus größte Teil der Anwender Windows-Betriebssysteme nutzt, jedoch gibt es auch bei diesen Kompatibilitätsunterschiede zwischen verschiedenen Versionen, die zudem stark unterschiedlich verteilt sind.[546] Zudem gibt es Kanzleien und Anwälte, die aus technischen, ideellen oder finanziellen Gründen andere Betriebssysteme wie MacOS oder Linux benutzen, wenngleich diese verhältnismäßig selten vorkommen.[547] Auch der Zugriff mittels mobiler Endgeräte auf den elektronischen Rechtsverkehr sollte möglich sein. Zwar gibt es bei den mobilen Betriebssystemen mit Googles Android und Apples iOS praktisch nur noch zwei Mobilbetriebssysteme mit relevanten Marktanteilen.[548] Gerade beim Marktführer Android ist jedoch durch die starke Anpassung durch verschiedene Gerätehersteller eine starke Streuung der verschiedenen Android-Versionen zu beobachten.[549] Da dies auch mit Folgen für die Kompatibilität von Anwendungen einhergeht, sollte die Software für den elektronischen Rechtsverkehr im Idealfall deswegen auf mehreren unterschiedlichen Betriebssystemen und Betriebssystemversionen lauffähig sein.

Eine andere Möglichkeit, mit der der größere Wartungs- und Pflegeaufwand durch verschiedene unterstützte Betriebssysteme reduziert werden kann, ist die Bereitstellung nicht einer Software, sondern eines Onlineportals, dessen Nutzung allein einen Webbrowser voraussetzt. Auch hier ist zwar auf die Kompatibilität mit den gängigsten Browsern zu achten, jedoch wird dies durch die Verfügbarkeit von universellen Standards in der Web-Programmierung sowie die Kompatibilität einiger gängiger Browser mit verschiedenen Betriebssystemen vereinfacht.[550] Nachteil einer solchen Lösung ist jedoch die mangelnde Einbindung in die Arbeitsabläufe der Kanzleien. Eine Kompromisslösung wäre insofern sowohl die Bereitstellung eines Onlinedienstes für den elektronischen Rechtsverkehr als auch einer Schnittstelle für die Nutzung durch Drittanbieter. Auf diese Weise könnte dem anwaltlichen Nutzer eine Nutzung ohne zusätzliche Software ermöglicht

546 *Kannenberg*, „Statistisch gesehen“: Windows 7 auf Desktops immer noch deutlich vor Windows 10, heise Online-Meldung vom 28.9.2016.

547 So nutzen von den im Rahmen der ERV-Studie der Bundesrechtsanwaltskammer befragten Anwälten 8% Apple-Betriebssysteme (gemeint dürfte hier MacOS in seinen verschiedenen Versionen sein) sowie 2 % Linux, vgl. *Bundesrechtsanwaltskammer*, BRAK-Magazin 2/2014, 6, 7.

548 *Briegleb*, heise Online-Meldung vom 19.8.2016.

549 Eine Übersicht mit Stand Mai 2016 findet sich bei *Wirtgen*, heise Online-Meldung vom 4.5.2016.

550 Beispielsweise ist der Browser Chrome von Google für Windows, MacOS und Linux verfügbar, ebenso der populäre quelloffene Browser Firefox, womit der mit Windows-Betriebssystemen mitgelieferte und nur für diese verfügbare Internet Explorer praktisch eine Ausnahme bildet.

und zugleich für Softwarehersteller die Möglichkeit geschaffen werden, vorhandene oder neue Anwaltssoftware kompatibel mit dem Verfahren für den elektronischen Rechtsverkehr zu machen. Das Kompatibilitätsproblem wäre damit auf die Dritthersteller verlagert, mit dem Vorteil, dass diese den elektronischen Rechtsverkehr nahtlos in die Arbeitsabläufe ihrer Anwaltssoftware integrieren können. Voraussetzung ist hierfür jedoch die Zurverfügungstellung entsprechender Schnittstellen (APIs) durch die Anbieter der Übertragungswege.

5.4 Verfügbarkeit

Ein wichtiges Thema neben der Sicherheit des elektronischen Rechtsverkehrs ist die Frage der Verfügbarkeit. Mit der kommenden Verpflichtung der Anwaltschaft zur Nutzung des elektronischen Rechtsverkehrs ist aufgrund der verfassungsrechtlich geschützten Berufsfreiheit nach Art. 12 GG der tatsächlichen Möglichkeit, den elektronischen Rechtsverkehr auch nutzen zu können, besonderes Gewicht zu geben. Zu trennen ist hierbei zwischen der zentralen Infrastruktur für den elektronischen Rechtsverkehr auf der einen Seite und der individuellen Erreichbarkeit dieser Infrastruktur auf der anderen Seite.

5.4.1 Verfügbarkeit der zentralen Systeme

Soweit der elektronische Rechtsverkehr auf einer zentralisierten Infrastruktur basiert,[551] ist sicherzustellen, dass diese Server auch stets erreichbar sind. In Anbetracht der Tatsache, dass durch Wartungen, Stromausfälle, Havarien, technische Probleme und dergleichen immer mit dem Ausfall von Servern gerechnet werden muss und kein Rechenzentrum eine hundertprozentige Verfügbarkeit garantieren kann oder will, ist eine redundante Infrastruktur vorzuhalten. Redundanz bedeutet in diesem Kontext, dass Notfallsysteme bereitstehen, die bei einem Ausfall einzelner Server deren Funktion zumindest zeitweilig übernehmen können.[552] Doch nicht nur die Ausfallsicherheit ist zu berücksichtigen, sondern auch eine ausreichende Dimensionierung der vorhandenen Server und deren Netzanbindung. In Anbetracht der großen zu erwartenden Nutzerzahlen und Datenmengen

551 D.h. auf einer bestimmten Anzahl von für diesen bereitgestellten Servern zur Übertragung der Nachrichten, im Gegensatz zu einer dezentralen peer-to-peer-Struktur, bei der alle Teilnehmer eines Kommunikationsnetzwerks nach belieben dazukommen oder das Netz verlassen und alle Teilnehmer gleichzeitig Nutzer und Anbieter sind, und damit auch selbst die Rolle von Servern einnehmen

552 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutzkataloge, M 1.52 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur.

müssen die Server ausreichend dimensioniert sein, um auch zu „Stoßzeiten“ die auftreffende Datenflut beherrschen zu können. Hierbei ist auch an Zeiten mit zu erwartender besonders hoher Belastung zu denken. Für den Bereich des elektronischen Rechtsverkehrs bedeutet dies, dass eine umfassende Bedarfsanalyse für die Dimensionierung der Infrastruktur der Einreichungswege erfolgt. In diese müssen sowohl das durchschnittliche Datenaufkommen durch die Kommunikation zwischen Anwälten und Gerichten als auch Auslastungsspitzen und -täler einbezogen werden.[553] So ist beispielsweise für Tage, an denen sich Fristenden häufen (wie beispielsweise den Monatsanfang, die Monatsmitte und das Monatsende) mit einem verstärkten Kommunikationsaufkommen mit den Gerichten zu rechnen, das entsprechend abgebildet werden muss. Auch Schwankungen im Tagesverlauf sind zu berücksichtigen, beispielsweise wenn Anwälte kurz vor Mitternacht vermehrt versuchen, den gerade noch fertig gewordenen Schriftsatz fristwahrend bei Gericht einzureichen.

Da jedoch selbst mit einer entsprechenden Infrastruktur keine lückenlose Verfügbarkeit in jedem Fall garantiert werden kann, müssen hierdurch entstehende Erreichbarkeitslücken mit hinreichend weitgehenden Ausnahmeregelungen abgefangen werden.

5.4.2 Erreichbarkeit durch den einzelnen Teilnehmer

Neben der generellen Verfügbarkeit der Server muss der einzelne Anwalt auch die Möglichkeit haben, diesen zu erreichen. Voraussetzung hierfür ist ein ausreichend breitbandiger Internetanschluss. Während dies in städtischen Ballungsgebieten regelmäßig gegeben sein wird, könnten sich hier gerade für Anwälte in ländlichen Gegenden Probleme auftun. Denn zum jetzigen Zeitpunkt gibt es trotz der öffentlich bereitgestellten Fördergelder für den Bereitbandausbau und entsprechende Initiativen der Bundesregierung abseits städtischer Ballungsgebiete viele Versorgungslücken.[554] Dies relativert die grundsätzlich gut klingenden Angaben im Breitbandatlas, der für Mitte 2016 eine Abdeckung von 93,6% im Bereich ≥ 6 MBit/s und von 87,2 % im Bereich ≥ 16 MBit/s für leitungsgebundene Technologien nennt.[555] Bei diesen Zahlen ist allerdings zu beachten, dass diese sich auf Privathaushalte beziehen, lediglich die Downloadbandbreite (nicht aber die für den elektronischen Rechtsverkehr ebenfalls relevante Uploadbandbreite, die zumindest

553 Auch wenn die Berücksichtigung von Zeiten geringer Belastung der Netzwerke zunächst kontraintuitiv erscheint, ist sie doch mindestens im Hinblick auf eine mögliche Zeitweise Abschaltung bzw. Heruntertaktung von nicht benötigten Systemen aus wirtschaftlichen und ökologischen Gründen relevant – gleichzeitig muss aber natürlich berücksichtigt werden, dass bei danach auftretendem Mehrbedarf eine hinreichend schnelle Anpassung der Leistung nach oben erfolgen kann.

554 *Schultze/Deutsche Presse-Agentur*, heise Online-Meldung vom 2.1.2016.

555 *Bundesministerium für Verkehr und digitale Infrastruktur*, Breitbandverfügbarkeit, 3.

bei ADSL-Anschlüssen regelmäßig deutlich geringer ausfällt) und die Zahlen auf Angaben der Breitbandanbieter basieren.[556] Für Geschäftskundenanschlüsse wird dementsprechend eine geringere Versorgung mit 66 % Abdeckung (hier allerdings für Anschlüsse ≥ 50 MBit/s) angegeben.[557] Wenngleich die Zahlen aufgrund des älteren Datums nur eingeschränkt aussagekräftig sind, zeigen demgegenüber die Umfragen der Bundesrechtsanwaltskammer zum elektronischen Rechtsverkehr eine deutlich geringere Versorgung von Kanzleien, bei denen zum Umfragezeitpunkt November 2013 – Januar 2014 noch 15% lediglich mit ISDN an das Internet angebunden waren, und mehr als 42 % über einen Upload von unter 1 MBit/s verfügten.[558] Auch ohne konkrete Zahlen bezüglich der Bandbreitenanforderungen für den elektronischen Rechtsverkehr für den einzelnen Nutzer ist davon auszugehen, dass ein Upload von 1 MBit/s deutlich zu langsam für eine zumutbare Benutzung hierfür ist, da damit ein Upload einer 30 MB großen Datei (was derzeit das Größenlimit für das EGVP darstellt[559]) bereits vier Minuten dauern würde.[560] Entsprechend höher wären die Wartezeiten bei größeren Übertragungsmengen, wie sie zum Beispiel schnell durch umfangreichere Schriftsätze, Scans, Digitalfotos, Videos oder Audiodateien entstehen können.[561]

Der zum Teil hinsichtlich des Breitbandausbaus erfolgende Verweis auf Technologien wie Vectoring, das über vorhandene DSL-Leitungen eine höhere Bandbreite erlaubt, ist dem gegenüber nicht zielführend, da es nur auf die bessere Versorgung bereits erschlossener Gebiete abzielt,[562] zugleich aber Konkurrenz für das diese Technologie verwendende Unternehmen im gleichen Gebiet faktisch ausschließt.[563] Ebenfalls keine dauerhafte Lösung ist es, auf Funktechnologien statt auf (Glasfaser-)Verkabelung zu setzen, da erstere (mit Ausnahme von Richtfunkstrecken) stets als Shared Medium ausgestaltet sind, wodurch sich viele Teilnehmer die Bandbreite eines Zugangspunktes teilen müssten.[564] Hierdurch kann es gerade zu Zeiten verstärkter Datennutzung (unter der Woche regelmäßig abends, an den Wochenenden und Feiertagen mitunter auch ganztägig) zu Bandbreitenengpässen und Verbindungsabbrüchen kommen. Im Hinblick auf den verfassungsrechtlichen Schutz der Berufsfreiheit muss für einen elektronischen Rechtsverkehr

556 *Bundesministerium für Verkehr und digitale Infrastruktur*, Breitbandverfügbarkeit, 2.
557 *Bundesministerium für Verkehr und digitale Infrastruktur*, Breitbandverfügbarkeit, 5.
558 *Bundesrechtsanwaltskammer*, BRAK-Magazin 2/2014, 6, 8.
559 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 15.
560 30 MB = 30720 B = 240 MBit / 1 MBit/s = 240s = 4 min. Entsprechend der in der IT üblichen Konvention wird bei Datenmengen nicht mit den SI-Präfixen (Mega, Kilo, Tera etc.) in der üblichen Bedeutung als Vielfache von 1000, sondern als vielfache von 1024 gerechnet. Korrekter wäre deswegen die Angabe MiB statt MB, da hierdurch eine Abgrenzung vom SI-Präfix stattfindet, die sich allerdings soweit ersichtlich bisher nicht in der Breite durchsetzen konnte.
561 Wenngleich einige dieser Dateitypen nicht sofort für den elektronischen Rechtsverkehr ins Auge fallen mögen, können sie durchaus als Beweismittel Bestandteil eines Schriftsatzes werden, insbesondere in spezialisierten Kanzleien wie beispielsweise solchen mit medienrechtlicher Ausrichtung.
562 *Krempl*, heise Online-Meldung vom 12.9.2016.
563 *Briegleb*, heise Online-Meldung vom 1.9.2016.
564 *Henschler*, Internet im Schneckentempo, Onlinemeldung auf tagesspiegel.de vom 13.11.2015.

gewährleistet werden, dass auch Nutzer in Gebieten abseits der Ballungsgebiete eine nutzbare und hinreichend schnelle Internetanbindung haben. Wo dies nicht möglich ist, müssen die auftretenden Probleme soweit es geht durch technische Gestaltung des elektronischen Rechtsverkehrs (beispielsweise in Form von Sende- und Empfangsprotokollen, die stabil im Hinblick auf langsame Übertragungsraten und gelegentliche Verbindungsabbrüche reagieren) abgefangen werden. Im Extremfall sollten zudem Ausnahmeregelungen für Anwälte, denen an ihrem Standort die Nutzung des elektronischen Rechtsverkehrs nicht möglich ist, gewährt werden, da andernfalls Klagen bis hin zu Verfassungsbeschwerden von jenen, für die der elektronische Rechtsverkehr eine besondere Härte darstellt, angestrengt werden könnten.

5.5 Kosten

Ein wichtiger, immer wieder in Aufsätzen und Stellungnahmen zum elektronischen Rechtsverkehr genannter Punkt sind die Kosten für den elektronischen Rechtsverkehr.[565] Auf Justizseite stellt sich die Situation dabei einfacher dar als aus anwaltlicher Sicht, war doch ein Beweggrund für den Erlass des ERV-Gesetz die Hoffnung, hierdurch Einsparungen seitens der Justiz verwirklichen zu können.[566] Die Kosten auf Anwaltsseite, auf die sich im Folgenden konzentriert werden soll, betreffen sowohl die Verhältnismäßigkeit der Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs, als auch die zu erwartende Akzeptanz desselben. Trotz der Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs für anwaltliche Nutzer ist die Akzeptanz dabei ein auch wirtschaftlich nicht unerheblicher Faktor, da das ERV-Gesetz verschiedene Einreichungswege nebeneinander vorsieht, und Nutzer bei zu geringer Attraktivität eines Einreichungswegs auf einen anderen, vom Preis-Leistungs-Verhältnis attraktiver erscheinenden Weg ausweichen könnten. Dies hätte auch für die öffentliche Hand negative Folgen, weil sich bereits getätigte Investitionen in die jeweilige Infrastruktur so im Nachhinein als Fehlinvestition herausstellen könnten.

Eine Kostenneutralität ist für verpflichtete Nutzer wie Anwälte weder rechtlich erforderlich noch praktisch realisierbar. Die Verpflichtung zu einer mit Kosten verbundenen Handlung ist ein Eingriff in die Berufsausübungsfreiheit gemäß Art. 12 Abs. 1 GG. Ein solcher Eingriff kann jedoch gerechtfertigt sein, wenn er durch hinreichende Gründe des Gemeinwohls gerechtfertigt ist, die gewählten Mittel zur Zweckerreichung geeignet sind und die Folge für den Betroffenen zumutbar

565 Exemplarisch seien hier genannt *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 10; *Backs/Kühnelt/Sandkühler/Schmid u. a.*, BRAK-Stellungnahme Nr. 6/2012, 3; *Rechtsanwaltskammer Sachsen*, FAQ zu ERV, Frage 15; *Sandkühler*, KammerMitteilungen Rechtsanwaltskammer Düsseldorf 1/2014, 45 f.

566 Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, BR-Drs. 818/12, 4 f.

ist.[567] Grundsätzlich hat der Gesetzgeber hier einen weiten Beurteilungsspielraum.[568] Eine Rechtfertigung des Eingriffs liegt jedoch dann nicht mehr vor, wenn die Kosten sich insgesamt als unverhältnismäßig darstellen.[569] Dies erscheint jedoch insbesondere im Verhältnis zu sonstigen Kosten, die gemeinhin durch die Ausübung des Anwaltsberufs entstehen, sowie den nach RVG als Mindeststandard festgelegten Gebühren für anwaltliche Leistungen als eher fernliegend. Somit verbleibt als Bemessungskriterium für die Kosten die rein wirtschaftliche Betrachtung des Kosten-Nutzen-Verhältnisses sowie die Akzeptanz der Anwaltschaft für den elektronischen Rechtsverkehr als Erfolgskriterium für diesen.

Zu beachten sind hierbei nicht nur die unmittelbaren Kosten, die direkt als Folge einer Zulassung zur Anwaltschaft und für die Nutzung der Einreichungswege entstehen, sondern auch nur mittelbar auf den elektronischen Rechtsverkehr zurückzuführende Kosten, beispielsweise solche für die Anpassung der Kanzleiorganisation.

5.5.1 Unmittelbare Kosten

Zu den unmittelbaren Kosten des elektronischen Rechtsverkehrs auf Nutzerseite gehören zunächst einmal die Anschaffungskosten für die erforderliche Hard- und Software.[570] Als „echte“ Kosten bezogen auf die Hardware für den elektronischen Rechtsverkehr zu betrachten sind Anschaffungskosten für nicht vorhandene PC-Technik, Terminals für Signaturkarten und Scanner sowie Drucker. Hierbei muss jedoch berücksichtigt werden, dass die meisten Kanzleien zumindest Teile dieser Ausrüstung bereits nutzen dürften und somit durch den elektronischen Rechtsverkehr keine oder nur geringe zusätzlichen Kosten anfallen. Eine explizite Ausnahme ist die Anschaffung eines geeigneten Kartenlesegeräts mit PIN-Eingabe sowie einer Signaturkarte mit (ggf. qualifiziertem) Zertifikat für eine (qualifizierte) elektronische Signatur, die in den meisten Kanzleien noch kein Standard ist.[571]

Softwareseitig können Kosten durch eventuell benötigte Software zur Teilnahme am elektronischen Rechtsverkehr entstehen. Wenngleich verfassungsrechtlich keine Pflicht zur Kostenneutralität des Systems für den Nutzer besteht, empfiehlt es sich aus Akzeptanzgründen, die Einstiegskosten

567 *Hofmann* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 12 Rn. 61.
568 *Hofmann* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 12 Rn. 61.
569 *Hofmann* in *Schmidt-Bleibtreu*/*Hofmann*/*Henneke*, Art. 12 Rn. 62.
570 Vgl. dazu oben unter 5.3.1 bzw. 5.3.2.
571 Nach der vom Soldan Institut durchgeführten Studie zum elektronischen Rechtsverkehr nutzten 2013 74 % der befragten Anwälte bisher die qualifizierte elektronische Signatur nicht, vgl. *Kilian/Rimkus*, AnwBl 2014, 913, 915.

hierfür möglichst gering zu halten. Denkbar ist dies beispielsweise in Form des Anbietens eines Webinterfaces für den benötigten Einreichungsweg. Eine Beschränkung auf die Zurverfügungstellung einer kostenneutralen oder möglichst kostengünstigen Lösung ist jedoch weder angezeigt noch empfehlenswert. Für Nutzer, die beispielsweise bereits Fachsoftware nutzen (was den größten Teil der digitalisierten Anwaltschaft betreffen dürfte[572]), sollte zur Erhaltung bisheriger Investitionen und eingespielter Arbeitsabläufe eine Nutzung des Einreichungsverfahrens mit Drittanbietersoftware möglich sein. Um dies zu erreichen, muss den Herstellern von Software auf deren Wunsch eine Schnittstelle zum Einreichungsweg zur Verfügung gestellt werden (eine sogenannte API[573]), mittels derer die Nutzung des Einreichungsweges auch aus der Fachsoftware heraus erfolgen kann. Dies hat nicht nur die positive Folge einer gesteigerten Akzeptanz durch die Nutzer, da diese gegebenenfalls ihre bisherige Fachsoftware weiternutzen können, wenn auch in einer neueren Version, sondern wirkt auch wirtschaftlich ausgleichend. Bezüglich des kostenfreien EGVP könnte es Bedenken bezüglich einer möglichen Wettbewerbsverzerrung geben, da dieses als kostenlos angebotenes und mit Steuergeldern finanzierte Produkt sich bezüglich seiner Funktionalität zumindest teilweise im Wettbewerb mit der (kostenpflichtigen) Fachsoftware befand.[574] Durch die Zurverfügungstellung von APIs einerseits und den Rückzug aus dem aktiven Anbieten von Software zur Nutzung jenseits eines „Minimalprodukts“ wird dieser mögliche Konfliktherd entschärft.

Neben den Kosten für Hard- und Software können noch laufende Kosten in Form von Nutzungsgebühren kommen. Beispielsweise sind für die Nutzung der De-Mail-Angebote verschiedener Anbieter regelmäßig sowohl eine Grundgebühr als auch Entgelte für bestimmte Übertragungsarten zu entrichten. Die Preise der Anbieter schwanken hierbei, zum Teil werden auch Volumenpakete angeboten, die bereits ein bestimmtes vorbezahltes Kontingent an Nachrichten enthalten. Grundsätzlich müssen anfallende Kosten für die Nutzung eines Einreichungsweges kein Manko sein, da auch bei der Nutzung des (analogen) Postweges bzw. je nach Kanzlei auch von Kurierdiensten stets Kosten angefallen sind. Aufgrund der weiten Verbreitung von kostenfreien E-Mail-Accounts einerseits und den bereits für Signaturkarten und Hardware anfallenden Kosten dürfte jedoch bei vielen Nutzern die Bereitschaft, für einen Einreichungsweg zu zahlen, tendenziell

572 Verlässliche Zahlen hierfür sind schwer zu bekommen, nach einer Erhebung der AG Kanzleimanagement des Deutschen Anwaltvereins von 2013 sollen jedoch geschätzte 80 bis 90 % der Kanzleien eine anwaltsspezifische Fachsoftware einsetzen. Die Angabe wird aber im Artikel selbst releativiert, indem mit Verweis auf nicht näher bezeichnete Branchenkenner eine Schätzung in Höhe von 30% Marktabdeckung angegeben wird, *Schnee-Gronauer/Schnee-Gronauer*, Anwaltsblatt 2013, 776 f.

573 Application Programming Interface.

574 Im Falle einer kostenlosen Abgabe von Zahnarztsoftware durch die Kassenärztliche Vereinigung an ihre Mitglieder hat das OLG Karlsruhe entschieden, dass hierin ein Verstoß gegen § 1 UWG liege, selbst wenn Gründe der Daseinsvorsorge dieses Vorgehen motiviert hätten, OLG Karlsruhe, Urteil vom 11.4.1991, Az. 4 U 20/90.

eher als gering einzuschätzen sein. Um die Nutzer von einem kostenpflichtigen Dienst zu überzeugen, der stets auch mit den anderen nach dem ERV-Gesetz zulässigen Einreichungswegen konkurriert, muss dieser aus Nutzersicht einen deutlichen Mehrwert mit sich bringen.

Schließlich hat die Bundesrechtsanwaltskammer als Teil der Mitgliedsbeiträge eine Umlage für das besondere elektronische Anwaltspostfach, das verpflichtend für jeden Anwalt von dieser eingerichtet wird, erhoben. Eine gegen den hierauf gerichteten Umlagebescheid in Höhe von 63 € für das Jahr 2015 erhobene Klage vor dem Anwaltsgerichtshof hat der Bundesgerichtshof in Anwaltssachen in der Berufungsinstanz abgewiesen.[575]

5.5.2 Mittelbare Kosten

Zu den mittelbaren Kosten gehören für den Nutzer Investitionen in Arbeitsabläufe und Infrastruktur der Kanzlei, die sich zwar nicht allein oder direkt dem elektronischen Rechtsverkehr zuordnen lassen, aber zumindest teilweise diesem zugute kommen oder durch ihn verursacht werden. Hierunter fallen beispielsweise Kosten für einen leistungsfähigeren Internetanschluss oder – im Falle einer heutzutage allerdings nur noch im Mobilfunkbereich üblichen – Abrechnung nach Nutzungsumfang auch Mehrkosten für Datenübertragungen, die im Zuge des Empfangs oder Versands von Dokumenten im elektronischen Rechtsverkehrs anfallen. Mehrkosten für die Absicherung des Kanzleinetzwerks können sich insofern als mittelbare Kosten des elektronischen Rechtsverkehrs darstellen, wenn sie aufgrund einer verstärkten Bedrohungslage – beispielsweise durch Hackerangriffe auf ERV-Nutzer – als geboten erscheinen. Die mittelbaren Kosten sind insofern schwieriger zu beurteilen, da sie regelmäßig jedenfalls hinsichtlich der konkreten Ausgestaltung der kostenverursachenden Maßnahme nicht zwingend sind. So gibt es regelmäßig für Sicherungsmaßnahmen hinsichtlich der IT-Ausstattung ein breites Bündel möglicher Maßnahmen, die von einer (eventuell kostengünstigeren, aber risikobehafteten) Selbstvornahme bis hin zur Bestellung eines Fachunternehmens zur IT-Absicherung einschließlich der hieraus resultierenden erheblichen Kosten reichen. Sofern sich aus dem elektronischen Rechtsverkehr bestimmte (mittelbare) Kostenfolgen zwingend ergeben, gelten insoweit die obigen Feststellungen zu den unmittelbaren Kosten. Auch hier ist keinesfalls eine Kostenneutralität vonnöten, eine solche bzw. möglichst geringe Nutzungskosten fördern jedoch die Akzeptanz des elektronischen Rechtsverkehrs bzw. des jeweiligen Einreichungsweges.

575 BGH, Urteil vom 11. Januar 2016, Az. AnwZ (Brfg) 33/15 = openJur 2016, 319.

5.5.3 Kosteneinsparungen

Neben den durch die Einführung des elektronischen Rechtsverkehrs anfallenden Mehrkosten ist aber auch die Kostenersparnis durch diesen zu berücksichtigen. Seitens der Justiz war eine der Motivationen, einen verpflichtenden elektronischen Rechtsverkehr mit den Gerichten zu fordern, die Hoffnung, hierdurch Kosten durch Scannen, Drucken und postalischen Versand von Schriftstücken einsparen zu können.[576] Ob sich diese Hoffnung realisiert, dürfte auch ganz entscheidend von der letztlichen Akzeptanz des elektronischen Rechtsverkehrs und der raschen Schließung verbleibender Medienbrüche zwischen analogen und digitalen Kommunikationswegen abhängen.

Doch auch auf Anwaltsseite ergeben sich Einsparmöglichkeiten durch den elektronischen Rechtsverkehr. So entfällt auch hier perspektivisch zumindest ein Teil der Druck- und Versandkosten. Im Länderentwurf des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten wurde die mögliche Ersparnis durch die kostenlose Nutzung der Einreichung mittels EGVP noch mit Einsparungen zwischen 19.250.000 und 50.750.000 Euro pro Jahr gerechnet.[577] Dies gilt jedoch nur für die Kommunikation mit der Justiz und gegebenenfalls Vertretern der Gegenseite, nicht jedoch mit Mandanten, da für diese keine Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs besteht. Zudem ist die Zahl auf die Gesamtheit der gerichtlichen Verfahren bezogen, nicht auf den einzelnen Anwalt. Teilt man die Angaben durch die Anzahl der zugelassenen Anwälte,[578] ergibt sich statistisch für den einzelnen Anwalt lediglich eine Ersparnis zwischen rund 118 und rund 310 Euro. Diese Ersparnis erscheint hinsichtlich möglicher Investitionskosten klein, kann sich aber über die Nutzungsdauer durchaus summieren und dürfte – die Richtigkeit der Zahlen unterstellt – die anfänglichen Investitionen in den elektronischen Rechtsverkehr verhältnismäßig schnell abdecken. Für sich genommen dürfte die unmittelbare finanzielle Ersparnis jedoch kaum eine taugliche Motivation darstellen, die eigene Kanzleiorganisation an den elektronischen Rechtsverkehr anzupassen, zumal hierfür auch ein (geldwerter) Zeitaufwand erforderlich ist. Aus diesem Grund spielt auch die Nutzerfreundlichkeit und der Bedienkomfort eine große Rolle für die Einsparmöglichkeiten seitens der Anwaltschaft, da hiervon ganz maßgeblich abhängen dürfte, in welchem Maße auch Mandanten freiwillig elektronische Kommunikationskanäle benutzen. Wird auch seitens der Mandanten ein hoher

576 Vgl. hierzu die Ausführungen oben unter 5.5.
577 BR-Drs. 818/12, 3; die Passage wurde im Regierungsentwurf unverändert übernommen, vgl. BT-Drs. 17/12634, 3.
578 Mit Stand 1.1.2016 sind dies nach der Statistik der Bundesrechtsanwaltskammer (abrufbar unter http://www.brak.de/w/files/04_fuer_journalisten/statistiken/2016/grosse-mitgliederstatistik-2016.pdf, zuletzt abgerufen am 18.12.2017) im Bundesgebiet 163.772 zugelassene Anwälte.

Nutzungsgrad erreicht, kann durch Vermeidung von Medienbrüchen auch auf anwaltlicher Seite eine deutliche Kostenersparnis eintreten.

5.6 Ergonomie

Um eine möglichst hohe Akzeptanz für den elektronischen Rechtsverkehr zu erzeugen, darf zudem die Frage der ergonomischen Gestaltung nicht unberücksichtigt bleiben. Hierunter ist die Einfachheit und Klarheit der Benutzerführung zu verstehen, aber ebenso die Berücksichtigung von Benutzern mit körperlichen oder sensorischen Einschränkungen, denen schon aus verfassungsrechtlichen Gründen zwingend eine zumutbare Benutzung des elektronischen Rechtsverkehrs ermöglicht werden muss.[579]

5.6.1 Barrierefreiheit

Unter dem Begriff der Barrierefreiheit wird die Gestaltung von Anlagen, Gegenständen oder Systemen verstanden, die durch Nutzer mit Behinderungen ohne Einschränkungen – gegebenenfalls jedoch mit Hilfsmitteln – nutzbar sind.[580] Dies stellt nicht nur eine gesellschaftliche Selbstverständlichkeit dar, sondern ist auch ein völkerrechtlich, verfassungsrechtlich und einfachgesetzlich verbrieftes Recht. Auf völkerrechtlicher Ebene ist hier zunächst die UN-Behindertenrechtskonvention zu nennen, die von der EU am 23. Dezember 2010 ratifiziert wurde[581] und in Deutschland bereits am 26. März 2009 in Kraft getreten ist.[582] Auch in der EMRK findet sich mit dem Diskriminierungsverbot in Art. 14 ein Menschenrecht, das nach der Spruchpraxis des EGMR mittlerweile auch Behinderung als sonstigen Status erfasst.[583] Schließlich enthält das deutsche Gesetzesrecht an verschiedenen Orten Diskriminierungsverbote und Regelungen zur Barrierefreiheit. Hierzu zählt neben dem Behindertengleichstellungsgesetz sowie den darauf basierenden Rechtsverordnungen und dem Allgemeinen Gleichbehandlungsgesetz beispielsweise § 45 TKG, der eine Berücksichtigung der Interessen behinderter Nutzer von Telekommunikationsdiensten vorsieht.

Für die Ausgestaltung des elektronischen Rechtsverkehrs ist daraus zu folgern, dass eine Gestaltung

579 Zur verfassungsrechtlichen Dimension von barrierefreien Kommunikationsmitteln vgl. *Welti*, 663.
580 Vgl. hierzu die Legaldefinition in § 4 BGG.
581 AnwBl 3/2011, VIII.
582 BGBl. II 812.
583 *Peters/König* in *Dörr*/*Grote*/*Marauhn*, Kap. 21 Rn. 207.

in der Art zu erfolgen hat, dass auch behinderte Menschen ihn ohne Einschränkung nutzen können. Für die von Trägern öffentlicher Gewalt bereitgestellten Produkte ergibt sich diese Anforderung aus § 12 Abs. 1 BGG,[584] nach dem Internetauftritte und -angebote und grafische Programmoberflächen barrierefrei gestaltet sein müssen. Konkretisiert werden diese Anforderungen in der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV 2.0). Diese umfassen beispielsweise das Angebot von alternativen Darstellungen zu bildlichen Gestaltungselementen,[585] den Verzicht auf Technologien, die inkompatibel zu Hilfsmitteln wie Bildschirmlupen, Screenreadern oder Braille-Zeilen sind[586] sowie die Steuerungsmöglichkeit mittels Tastatureingaben oder alternativen Eingabemethoden.[587]

Bezüglich privatrechtlicher Anbieter von Zugangswegen finden diese Regeln jedoch keine direkte Anwendung. Dies gilt beispielsweise gegenüber Diensten wie De-Mail oder E-Mail-Anbietern (die in Verbindung mit der qualifizierten elektronischen Signatur ebenfalls die Teilnahme am elektronischen Rechtsverkehr ermöglichen). § 5 BGG eröffnet deswegen die Möglichkeit von Zielvereinbarungen zwischen nach § 15 Abs. 3 BGG anerkannten Verbänden und Unternehmen und Unternehmensverbänden, die überdies auch vertragsstrafenbewehrt sein können. In der Praxis hat sich das Regelungsinstrument Zielvereinbarung jedoch dem Evaluationsbericht zu § 5 BGG zufolge praktisch nicht bewährt.[588]

Auch Softwareanbieter wie beispielsweise die Hersteller von Fachsoftware für Anwälte trifft grundsätzlich keine entsprechende Pflicht zur barrierefreien Gestaltung. Dies könnte zumindest im Hinblick auf den elektronischen Rechtsverkehr jedoch gegebenenfalls hingenommen werden, solange jedenfalls ein von der öffentlichen Verwaltung angebotener Einreichungsweg zur Verfügung steht, der barrierefrei ausgestaltet ist. Wünschenswert wäre indes natürlich eine Sensibilität der Softwarehersteller für die Belange behinderter Menschen und eine entsprechende Gestaltung ihrer Produkte. In Anbetracht der Erfahrungen mit § 5 BGG sowie des verhältnismäßig geringen Anteils von Nutzern mit entsprechenden Anforderungen[589] ist hiermit jedoch jedenfalls allein anhand einer

584 Vormals § 11 Abs. 1 BGG, so auch beispielsweise von der nach § 12 Abs. 1 BGG erlassenen Rechtsverordnung referenziert, nach Änderung durch das Gesetz vom 19.7.2016, BGBl. I 1757 durch den neu eingefügten § 11 BGG nunmehr § 12 Abs. 1 BGG .

585 Vgl. Anforderung 1.1 in Anlage 1 zu § 3 und § 4 Abs. 1 BITV 2.0. Hierfür steht im HTML-Standard beispielsweise der sogenannte Alt-Text zur Verfügung, der von entsprechend konfigurierten Webbrowsern an Stelle von Bildern angezeigt bzw. vorgelesen werden kann und dazu gedacht ist, eine textuelle Umschreibung von Bildinhalten zur Verfügung zu stellen; vgl. https://www.w3.org/standards/webdesign/accessibility.html#examples, zuletzt abgerufen am 18.12.2017.

586 Vgl. Anforderungen 1.3 und 4.1 in Anlage 1 zu § 3 und § 4 Abs. 1 BITV 2.0.

587 Vgl. Anforderung 2.1 in Anlage 1 zu § 3 und § 4 Abs. 1 BITV 2.0.

588 *Ritz* in *Kossens*/*Heide*, *von der*/*Maaß*, § 5 BGG Rn. 23 f.; zum gleichen Schluss kommt bereits *Welti*, 665.

589 Den Umfragen der Bundesrechtsanwaltskammer zur Vorbereitung auf den elektronischen Rechtsverkehr zu Folge gaben nur 0,4 % der Teilnehmer an, spezielle Hardware für behinderte Nutzer sowie 1,4 % der Teilnehmer,

Selbstregulierung nicht zu rechnen.

5.6.2 Nutzbarkeit für Nutzer ohne Behinderung

Auch für Nutzer ohne Behinderung sollte selbstverständlich eine möglichst ergonomische, transparente und einfache Bedienung des elektronischen Rechtsverkehrs gewährleistet sein. Rechtliche Regelungen hierzu finden sich beispielsweise in der Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten (Bildschirmarbeitsverordnung – BildscharbV). Im Anhang über an Bildschirmarbeitsplätze zu stellende Anforderungen zur BildscharbV sind unter Nr. 20 ff. auch Anforderungen an Software beschrieben. Diese betreffen eine ergonomische Gestaltung der Software (Nr. 20), eine Anpassung an die zu erfüllende Aufgabe (Nr. 21.1), Angaben über die Dialogabläufe und deren Beeinflussbarkeit sowie Fehlerkorrekturmöglichkeiten (Nr. 21.2, 21.3), eine Anpassung an Kenntnisse und Erfahrungen der Benutzer im Hinblick auf die zu erfüllende Aufgabe (Nr. 21.4) sowie ein Verbot der „qualitativen oder quantitativen Kontrolle“ (Nr. 21.5). Die Bildschirmarbeitsverordnung wurde mit Wirkung zum 3. Dezember 2016 durch die Verordnung zur Änderung von Arbeitsschutzverordnungen aufgehoben und ihre Inhalte zum Teil in die Arbeitsstättenverordnung (ArbStättV) übernommen.[590] Die Anforderungen an Bilschirmarbeitsplätze finden sich nunmehr in Nr. 6, die genannten Anforderungen an Softwaresysteme unter Nr. 6.5 des Anhangs zu § 3 Abs. 1 ArbStättV.

Aufgrund der offenen Gestaltung des elektronischen Rechtsverkehrs und der Grundkonzeption, die kommerzielle Anbieter zur Integration der erlaubten Einreichungswege in ihre Fachsoftware motivieren will, ist mit einem umfangreichen Markt für entsprechend ausgestattete Fachsoftware zu rechnen. Die Verfügbarkeit einer großen Auswahl von Produkten verringert dabei den Druck auf einzelne Anbieter, alle Nutzer mit der Ausgestaltung ihrer Software anzusprechen. Andererseits dürfte durch die Konkurrenz zwischen den Anbietern ein wirtschaftliches Bedürfnis für diese erzeugt werden, möglichst benutzerfreundliche und effiziente Software herzustellen. Voraussetzung hierfür ist allerdings ein funktionierender Markt für Anwaltssoftware, der für den elektronischen Rechtsverkehr insbesondere eine für alle gleichermaßen nutzbare Softwareschnittstelle zu Einreichungswegen zur Verfügung stellt. Seitens der öffentlichen Verwaltung muss hier insbesondere dafür gesorgt werden, dass kein Anbieter durch Gestaltung der Schnittstellen, die Dokumentation oder den Zugriff zu ihnen gegenüber seinen Wettbewerbern privilegiert wird.

entsprechende Software zu verwenden, vgl. *Bundesrechtsanwaltskammer*, BRAK-Magazin 2/2014, 6, 8.

590 BGBl I 2681, Art. 3.

5.7 Haftungsrisiken

Ein weiteres wesentliches Kriterium für den elektronischen Rechtsverkehr ist schließlich die Regelung von Haftungsrisiken für die zur Nutzung verpflichteten Nutzer. Wenngleich Anwälte gesetzlich zum Abschluss einer Berufshaftpflichtversicherung mit einer Deckungssumme in Höhe von mindestens 250.000 Euro pro Schadensfall und einer Begrenzung auf nicht mehr als 1 Million Euro pro Jahr verpflichtet sind,[591] Partnerschaftsgesellschaften sogar mit mindestens 2,5 Millionen Euro pro Versicherungsfall und mindestens 10 Millionen Euro pro Jahr,[592] stellen Haftungsfälle ein erhebliches Risiko dar. Denn zum einen bietet die Versicherung nur in Höhe der jeweils vereinbarten Deckung Schutz vor (persönlicher) Haftung des Anwalts. Auch ist zu berücksichtigen, dass sich je nach Verschulden des Anwalts Regressansprüche der Versicherung ihm gegenüber ergeben könnten. Schließlich stellt auch ohne Regressansprüche oder Überschreitung der Deckungssumme jeder Haftungsfall eine Belastung dar, da sich hierdurch die Versicherungsprämie erhöhen und der professionelle Ruf des den Haftungsfall auslösenden Anwalts stark leiden kann. Diese Komponenten erlangen im Hinblick auf das strenge Berufsrecht der Rechtsanwälte Bedeutung, da im Falle der Insolvenz als Rechtsfolge – neben den damit einhergehenden wirtschaftlichen Schwierigkeiten – gemäß § 14 Abs. 2 Nr. 7 BRAO auch der Widerruf der Anwaltszulassung droht.

Zu denken ist zwar an einen Regressanspruch gegenüber dem jeweiligen Anbieter des Übermittlungsweges, falls durch eine technische Störung dieses Weges ein Haftungsfall eintritt. Jedoch existiert für Schadensersatzansprüche, die aus einer Verletzung der Vorschriften aus dem TKG resultieren, in § 44a TKG eine Haftungsbegrenzung auf 12.500 Euro pro Nutzer oder bei einer Vielzahl von betroffenen Nutzern auf höchstens 10 Millionen Euro. Diese Haftungsbegrenzung gilt unabhängig vom Rechtsgrund des Schadens für fahrlässig verursachte reine Vermögensschäden und enthält damit eine Besserstellung für Anbieter von Telekommunikationsdiensten.[593] Eine solche Begrenzung könnte damit den Anwalt ohne eine weitergehende Regelung weitgehend schutzlos gegenüber den teilweise erheblich höheren Ansprüchen, denen er sich im Haftungsfall ausgesetzt sehen kann, stellen. Allerdings ist eine einzelvertragliche Abweichung von dieser Haftungsregelung gegenüber Unternehmern möglich.[594] Sofern von den Anbietern von Einreichungswegen mit anwaltlichen Nutzern keine abweichenden Haftungsregelungen vereinbart werden, sollte durch den Gesetzgeber zumindest für private Anbieter von Einreichungswegen für den elektronischen

591 Vgl. § 12 Abs. 2 i.V.m. § 51 BRAO.
592 Vgl. § 51a Abs. 2 BRAO.
593 *Scholz* in *Arndt*/*Fetzer*/*Scherer*/*Graulich*, § 44a TKG Rn. 2.
594 *Scholz* in *Arndt*/*Fetzer*/*Scherer*/*Graulich*, § 44a TKG Rn. 6.

Rechtsverkehr evaluiert werden, ob diese Haftungsprivilegierung auch für die Interessenkonstellation im elektronischen Rechtsverkehr haltbar ist, oder ob hier gegebenenfalls Modifikationen vorgenommen werden müssen.

Im Folgenden sollen die möglichen haftungsträchtigen Konstellationen herausgearbeitet werden, die durch den elektronischen Rechtsverkehr verursacht werden können.

5.7.1 Haftungsrisiken durch Verfügbarkeitsmängel

Der gedanklich naheliegendste Haftungsfall beim elektronischen Rechtsverkehr betrifft ein durch einen Verfügbarkeitsmangel ausgelöstes Schadensereignis. Ein solches kann sich insbesondere in Form einer Fristversäumung äußern, was dem Erwartungsbild bei Betrachtung der Häufigkeit verschiedener durch Anwälte verursachte Haftungsfälle entspricht. Der in der Praxis der Berufshaftpflichtversicherungen häufigste Haftungsfall ist die Fristversäumnis durch den Anwalt.[595] Die Möglichkeit einer Wiedereinsetzung in den vorigen Stand (beispielsweise nach § 233 ZPO oder § 60 VwGO) kann dies nur zum Teil auffangen, da hierfür stets eine Fristversäumung „ohne Verschulden“ erforderlich ist. Zwar ist im Falle der Faxübertragung bei einer Fristversäumung aufgrund eines technischen Versagens seitens des Gerichts regelmäßig eine Wiedereinsetzung zu gewähren, jedoch soll dennoch der Anwalt das Risiko einer anderweitigen Belegung des Anschlusses tragen und diesem Umstand durch entsprechend frühzeitige Absendung des Schriftsatzes Rechnung tragen.[596]

Voraussetzung für eine Wiedereinsetzung ist allerdings, dass die sich darauf berufende Partei die Gründe für die Wiedereinsetzung – mitunter auch das fehlende Verschulden – glaubhaft macht (z.B. § 236 Abs. 2 ZPO). Dies kann hier zum einen daran scheitern, dass der anwaltliche Nutzer regelmäßig keinen Einblick in die IT-Infrastruktur des Gerichts haben dürfte, der ihm eine Einschätzung erlaubt, wessen Risikosphäre eine Fehlübermittlung zuzurechnen ist. Zum anderen kann auch ein Verschulden selbst bei einem technischen Versagen außerhalb der Risikosphäre des Anwalts zu einer verschuldeten Verspätung führen, nämlich dann, wenn ein Ausweichen auf einen anderen Einreichungskanal noch möglich gewesen wäre.[597] Für den elektronischen Rechtsverkehr

595 So spricht *Sommerschuh*, Berufshaftung und Berufsaufsicht, 57, davon, dass mit Stand 2002 Fristversäumnisse mit ca. 40 % den häufigsten Versicherungsfall bei Berufshaftpflichtversicherungen für Anwälte darstellen, wobei davon ca. die Hälfte der Fälle auf die Versäumung von prozessualen Fristen entfalle. Bei *Diller/Klein*, BRAK-Mitteilungen 2013, 65, 66 werden als Anteil 30 % genannt, allerdings ohne bezifferte Trennung zwischen prozessualen und materiellen Fristen.

596 *Greger* in *Zöller*, § 233 ZPO Rn. 23, Stichwort „Telefax“.

597 Für das Telefax so beispielsweise BGH, Urteil vom 5.9.2012, VII ZB 25/12, zitiert nach *Engels*, ITRB 2013, 28.

kommt zudem noch erschwerend hinzu, dass der Nutzer genau prüfen muss, ob das Gericht auch den elektronischen Rechtsverkehr durch den verwendeten Weg eröffnet hat. Die Rechtsprechung hat hierzu entschieden, dass alleine die Anlage einer entsprechenden Kontaktadresse durch das Gericht noch nicht ausreicht, um eine Empfangsbereitschaft auf dem jeweiligen Kanal zu begründen.[598] Für die Zukunft sollten sich derartige Probleme in der Theorie zwar durch die bundesweite Einführung des elektronischen Rechtsverkehrs mit den Gerichten nach Ablauf der Übergangszeit zumindest größtenteils erledigen. Zu klären ist hingegen, wie mit der Koexistenz verschiedener Einreichungswege und einer Verpflichtung der Gerichte zur Bedienung dieser Wege umgegangen werden muss. Dementsprechend muss sich ein Einreichungsweg für den elektronischen Rechtsverkehr auch daran messen lassen, wie sehr man sich auf dessen Akzeptanz verlassen kann. Hierfür sind entsprechende rechtliche Regelungen notwendig.

Da zudem Verfügbarkeitsmängel bei durch Dritte angebotenen Einreichungswegen auftreten können, muss hier zumindest eine Erkennbarkeit durch den Nutzer vorliegen. Dies kann beispielsweise in der Form von Sende- und Empfangsbestätigungen und zeitnaher Fehlermeldungen im Falle fehlschlagender Zustellungen erfolgen. Im Hinblick auf die zeitkritische Natur der anwaltlichen Kommunikation müssen solche Bestätigungen und Fehlermeldungen auch sehr schnell erfolgen, damit der Nutzer im Fehlerfall noch auf einen anderen, funktionsfähigen Einreichungsweg ausweichen kann.

5.7.2 Haftungsrisiken durch Datenschutz- und Datensicherheitsmängel

Auch eine durch Datenschutzverstöße im weiteren Sinne ausgelöste Haftung ist denkbar und kann beim elektronischen Rechtsverkehr oder einer diesem angepassten Kanzleiorganisation virulent werden. Neben den bereits beim Abschnitt zum Bundesdatenschutzgesetz thematisierten drohenden Bußgeldern kann die Verletzung von Datenschutzgesetzen oder der anwaltlichen Verschwiegenheitspflicht auch nach § 280 Abs. 1 oder § 823 Abs. 2 BGB in Verbindung mit § 43a BRAO zu einem Schadensersatzanspruch des Geschädigten gegenüber dem Anwalt führen.[599] Je nach betroffener Information und Geschädigtem können hierdurch erhebliche Ansprüche entstehen, die mitunter die wirtschaftliche Existenz einer Kanzlei oder eines Einzelanwalts bedrohen könnten. Hierbei ist für die Haftungsfrage grundsätzlich danach zu unterscheiden, ob ein Schadensereignis durch den Anwalt rechtswidrig und schuldhaft verursacht wurde (bei § 823 Abs. 2 BGB) oder eine

598 OLG Düsseldorf, Urteil vom 24.7.2013, Az. VI-U (Kart) 48/12 = openJur 2013, 32422.
599 *Henssler*, NJW 1994, 1817, 1818.

Pflichtverletzung vorliegt, die der Anwalt zu vertreten hat (bei § 280 Abs. 1 BGB) oder nicht. Eine Rechtswidrigkeit kann jedoch dann entfallen, wenn das zum Schaden führende Verhalten letztlich nur einer gesetzlich zwingend verordneten Gestaltung wie beispielsweise der Nutzung eines bestimmten zugelassenen, gleichwohl unsicheren Übermittlungsweges entspricht. Die Rechtsprechung muss jedoch in Zukunft noch herausarbeiten, unter welchen Voraussetzungen angesichts der Möglichkeit, unter mehreren Übermittlungswegen für den elektronischen Rechtsverkehr wählen zu können, hier ein Verschulden des einzelnen anwaltlichen Nutzers ausscheidet. Dies kann jedoch nur dann relevant werden, wenn der Schadenseintritt durch das Verfahren an sich bedingt ist und nicht vom Nutzer – beispielsweise durch Auswählen der sichereren unter mehreren vom Einreichungsweg angebotenen Versandoptionen. Im Zweifel ist als praktische Lösung durch den Anwalt vorab in Absprache mit dem Mandanten zu klären, welches Sicherheitsbedürfnis dieser hat und welche Übermittlungswege dementsprechend durch den Anwalt genutzt werden dürfen.

Darüber hinaus sind auch Haftungsfälle denkbar, in denen durch eine Durchbrechung der Integrität oder der Authentizität übertragener Nachrichten ein Schadensereignis eintritt. Denkbar sind hier in erster Linie betrügerische Handlungen durch den Anwalt, den Mandanten oder Dritte, die zu einem Schaden führen. Wenngleich es immer möglich ist, solche Fälle zu konstruieren, ist zumindest für den analogen Rechtsverkehr bisher nicht ersichtlich, dass die – theoretisch auch dort bestehende – Möglichkeit zur Fälschung von beispielsweise bestimmenden Schriftsätzen, um im Prozess eine gewünschte Folge zu erzielen, in relevanter Häufung auftreten würden. Einzelne Fälle wie beispielsweise der einer Täuschung eines Anwalts gegenüber seinem Mandanten, mittels der der Anwalt diesem vorspiegelte, ein Verfahren für ihn zu betreiben, das indes längst eingestellt worden war, und dabei sogar ein Gerichtsurteil fälschte,[600] bleiben hier die exotische Ausnahme. Es ist zwar denkbar, dass durch den elektronischen Rechtsverkehr und die damit je nach Einreichungsart möglicherweise einfacheren Möglichkeiten, Fälschungen anzufertigen, derartige Fälle vermehrt auftreten könnten. Eine dahingehende Prognose ist jedoch schwierig und wird deshalb eher einer Evaluierung der Auswirkungen des elektronischen Rechtsverkehrs mit den Gerichten überlassen bleiben müssen. Grundsätzlich besteht jedoch mit dem strafrechtlichen Schutz gegen Fälschungen nach § 267 und 269 StGB und Betrug nach § 263 StGB bzw. Computerbetrug nach § 263a StGB ein recht umfassender Schutz gegen derartige Gefährdungen.

Einfacher – wenngleich nicht weniger haftungsträchtig – stellt sich die Lage bei einer durch eine

600 OLG Hamm, Beschluss vom 12.5.2016, Az. 1 RVs 18/16, abrufbar unter http://www.justiz.nrw.de/nrwe/olgs/hamm/j2016/1_RVs_18_16_Beschluss_20160512.html, zuletzt abgerufen am 18.12.2017.

dem elektronischen Rechtsverkehr angepasste Kanzleiorganisation dar. Hier ist davon auszugehen, dass ungeachtet der Besonderheiten des elektronischen Rechtsverkehrs wie beispielsweise Bearbeitung und Versand von Schriftsätzen auf elektronischem Wege und Einscannen von Posteingängen die bisherigen Grundsätze zur Kanzleiorganisation weitergelten. Hiervon umfasst ist beispielsweise die Pflicht zum Führen eines Fristenkalenders, für den auch bei elektronischer Form die Vollständigkeit und Richtigkeit gewährleistet sein muss und Datenverluste durch menschliche oder Systemfehler ausgeschlossen werden müssen.[601] Für die Aktenführung und den Umgang mit personenbezogenen Daten gelten die dargestellten Grundsätze der anwaltlichen Verschwiegenheit und subsidiär des Bundesdatenschutzgesetzes. Der Anwalt wird sich im Schadensfall nicht darauf zurückziehen können, dass eine bestimmte Gestaltung der Kanzleiorganisation qua Gesetzes vorgeschrieben gewesen sei, da praktisch sämtliche Erfordernisse an die Kanzleiorganisation für den elektronischen Rechtsverkehr nicht im Gesetz oder der entsprechenden Rechtsverordnung festgelegt werden, sondern sich allenfalls mittelbar oder aus rein praktischen Erwägungen durch den elektronischen Rechtsverkehr ergeben. Entsprechend hoch ist hier dementsprechend das Risiko, durch eine ungünstige Gestaltung der Kanzleiorganisation dem Mandanten oder Dritten einen Schaden durch Datenverlust zu verursachen.

601 *Sommerschuh*, Berufshaftung und Berufsaufsicht, 67.

3. Teil – Umsetzung in der Praxis

6 Das elektronische Gerichts- und Verwaltungspostfach

Im Folgenden soll näher auf das elektronische Gerichts- und Verwaltungspostfach als zulässiger Einreichungsweg für den elektronischen Rechtsverkehr eingegangen werden. Die historische Entwicklung des EGVP wurde bereits oben unter 2.3.3 und die konkrete Ausgestaltung als besonderes elektronisches Anwaltspostfach unter 2.3.4 umrissen.

Eine Beschäftigung mit den Eigenschaften des elektronischen Gerichts- und Verwaltungspostfachs kann nicht schon deshalb unterbleiben, weil der EGVP-Classic-Client zum 1.1.2016 abgekündigt wurde und nach dem 1.1.2018 auch nicht mehr zum Download zur Verfügung stehen wird.[602] Dies ergibt sich jedoch noch nicht bereits daraus, dass sich (vorbehaltlich einer gezielten „Aussperrung“ des EGVP-Clients aus dem EGVP-System) der Client nach diesem Termin nicht weiter nutzen ließe. Da der Support für die Software jedoch zum 31.12.2016 beendet wurde, dürfte dieser früher oder später funktionslos werden, weil ohne einen fortgesetzten Support nicht gewährleistet ist, dass der EGVP-Client auch mit später erfolgenden Änderungen am EGVP-System oder an Softwarevoraussetzungen wie den unterstützten Betriebssystemen oder der JAVA-Laufzeitumgebung auch in Zukunft lauffähig und sinnvoll einsetzbar ist. Über die Nutzung des EGVP-Clients hinaus bleibt jedoch das System EGVP mit seinen Eigenarten bestehen, gleich ob es über die Software von Drittanbietern genutzt wird oder über eine staatlicherseits bereitgestellte Software. Auch das besondere elektronische Anwaltspostfach wird einschließlich seines Webinterfaces letztlich das bereits bestehende EGVP-System benutzen. Was neu hinzukommt sind die Anwaltspostfächer, die von der Bundesrechtsanwaltskammer zur Verfügung gestellt werden, die Kommunikation wird jedoch über das EGVP-System in der Form einer Benutzung des diesem zugrundeliegenden OSCI-Protokolls erfolgen.[603] Die hier im Sinne des auf dem OSCI-Standard aufbauenden Systems benutzte Bezeichnung EGVP behält damit auch für das kommende besondere elektronische Anwaltspostfach ihre Gültigkeit. Wo sich Abweichungen durch eine andere Gestaltung des beA ergeben, wird an der jeweiligen Stelle auf diese eingegangen.

602 Vgl. hierzu oben unter 2.3.3.
603 *Rechtsanwaltskammer München*, Fragen zum ERV, Frage 6.

6.1 Merkmale

Im Folgenden soll auf die Merkmale des Systems EGVP eingegangen werden. Besonderes Augenmerk wird hierbei auf solche Merkmale gelegt, die Bedeutung für die unter Kapitel 5 aufgestellten Kriterien für den elektronischen Rechtsverkehr haben.

6.1.1 Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung

Ein wesentlicher Bestandteil des vom EGVP verwendeten OSCI-Protokolls (genauer gesagt des Protokolls OSCI-Transport als Untermenge des OSCI-Standards) ist die konsequente Verwendung von Verschlüsselung. Auf der Transportebene äußert sich diese zunächst in Angebot einer Transportverschlüsselung in Form eines „doppelten Umschlags“,[604] womit die Inhaltsdaten unabhängig von den Nutzungsdaten verschlüsselt werden können. Für diese – zwingende – Transportverschlüsselung wird das verbreitete Protokoll SSL benutzt.[605] Auf diese Weise können die zur Übermittlung und Speicherung von OSCI-Nachrichten verwendeten Server – im OSCI-Standard als Intermediäre bezeichnet[606] – die zur richtigen Zuordnung oder Weiterleitung von Nachrichten notwendigen Daten zwar entschlüsseln, haben jedoch keinen Zugang zu dem Klartext der im „inneren Umschlag“ enthaltenen Inhaltsdaten, sofern letzterer vom Absender verschlüsselt übermittelt worden ist. Wenngleich das OSCI-Protokoll lediglich die Möglichkeit der Verschlüsselung bereitstellt, ohne deren Benutzung zwingend vorauszusetzen,[607] können spezifische Implementierungen des Protokolls dies tun. So setzt die Software für das elektronische Gerichts- und Verwaltungspostfach zwingend eine Ende-zu-Ende-Verschlüsselung ein.[608] Zur Anwendung kommt hierbei nach OSCI 1.2 eine asymmetrische Verschlüsselung (Public-Key-Verfahren) in Form der Verschlüsselungsverfahren Triple-DES und AES für die symmetrische Verschlüsselung und RSA für den Schlüsselaustausch.[609] Dies wird für das besondere elektronische Anwaltspostfach ebenfalls der Sicherheitsstandard sein, auch dieses wird als Transportprotokoll OSCI 1.2 und eine zwingende Verschlüsselung mit AES und einer Schlüssellänge von 256 Bit (der bei diesem Standard

604 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 12; die Fortentwicklung des Standards als OSCI 2.0 befindet sich nach wie vor in der Entwicklung und wird bisher nicht als Transportstandard für das EGVP bzw. das besondere elektronische Anwaltspostfach benutzt, vgl. *Governikus GmbH & Co. KG*, Governikus-Prüfprotokoll, 19.
605 *egvp.de*, Testkonzept, 4 u. 10.
606 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 7.
607 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 6.
608 *Berlit*, JurPC Web-Dok. 13/2006, Abs. 22.
609 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 23.

höchsten verfügbaren Schlüssellänge) sowie RSA mit einer Schlüssellänge von 2048 Bit für den Schlüsselaustausch verwenden.[610] Damit entsprechen die (derzeit) verwendeten Schlüssellängen den aktuellen Empfehlungen des BSI.[611]

6.1.2 Zugangsbestätigungen

Der OSCI-Standard als Grundlage des EGVP bietet auch die Möglichkeit, Zugangsbestätigungen zu erteilen und diese auf Wunsch des Nutzers durch eine fortgeschrittene oder qualifizierte elektronische Signatur zu beglaubigen.[612] Die Zugangsbestätigungen werden hierbei in Form eines Laufzettels erteilt, anhand dessen sich der Weg einer Nachricht und der auf dem Weg erfolgten Signaturprüfungen nachverfolgen lässt.[613] Ein Bestandteil des Laufzettels sind hierbei auch Zeitstempel, die den Zeitpunkt des Eingangs einer Nachricht auf dem Empfangsserver protokollieren.[614] Die Umsetzung des Laufzettels im EGVP ermöglicht dem Nutzer damit, auf einen Blick den Weg einer Nachricht einschließlich Eintreffen beim Server und Abholung durch den Empfänger nachzuvollziehen und die Ergebnisse der Signaturprüfung für die Nutzungsdaten durch den Intermediär einzusehen. Eine Verschärfung gegenüber der bei OSCI 1.2 bloß optionalen Signierung des Laufzettels ist deren zwingende Signierung beim EGVP mit einer fortgeschrittenen elektronischen Signatur.[615] Die Benutzung einer fortgeschrittenen anstatt einer qualifizierten elektronischen Signatur dürfte sich in diesem Fall historisch daraus erklären, dass diese Signatur automatisch vom System erzeugt wurde, ohne dass ein menschliches Tätigwerden erforderlich war. Die noch nach dem Signaturgesetz bestehende Voraussetzung an qualifizierte elektronische Signaturen, dass diese mit sicheren Signaturerstellungseinheiten erzeugt werden mussten, die unter anderem gemäß § 17 Abs. 2 SigG vor der Erzeugung einer Signatur die Erstellung anzeigten, schloss eine rein automatisierte Erzeugung von qualifizierten elektronischen Signaturen ohne menschliche Kontrolle aus. Nach der eIDAS-Verordnung besteht dieses Erfordernis an qualifizierte Signaturerstellungseinheiten im Sinne von Art. 29 eIDAS-VO fort. Nach Anhang II Abs. 2 eIDAS-VO dürfen qualifizierte elektronische Signaturerstellungseinheiten nicht verhindern, dass dem Unterzeichner die zu unterzeichnenden Daten vor dem Unterzeichnen angezeigt werden.

610 *Bundesrechtsanwaltskammer*, beA-Verschlüsselungsverfahren.
611 Für RSA empfiehlt dieses aktuell eine Schlüssellänge von mindestens 2000 Bit (*Bundesamt für Sicherheit in der Informationstechnik*, BSI-TR-02102-1, 37) und für AES eine Schlüssellänge von 128, 192 oder 256 Bit (*Bundesamt für Sicherheit in der Informationstechnik*, BSI-TR-02102-1, 22).
612 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 13.
613 *OSCI Leitstelle*, OSCI-Transport 1.2 Entwurfsprinzipien, 25.
614 *Governikus GmbH & Co. KG*, Governikus-Prüfprotokoll, 20.
615 *NotarNet GmbH*, Eingangsnachweis, 1.

Mangels entgegenstehender Angaben ist zu erwarten, dass auch das besondere elektronische Anwaltspostfach diesen Laufzettel zur Protokollierung von Nachrichtenversand und -empfang sowie erfolgten Signaturprüfungen und deren Ergebnissen nutzen wird.

Eine anfangs in den Gesetzesentwürfen zur Förderung des elektronischen Rechtsverkehrs noch enthaltene Funktion zur automatischen Versendung eines (elektronischen) Empfangsbekenntnisses durch das Postfach des Rechtsanwalts, der eine Zustellung gegen Empfangsbekenntnis erhält, ist hingegen entfallen.[616] Diese Funktionalität stieß von Anfang an seitens der Anwaltschaft auf großen Widerstand, so hatten sich in ihren jeweiligen Stellungnahmen zu den Gesetzesentwürfen beispielsweise die Bundesrechtsanwaltskammer[617] und der deutsche Anwaltverein[618] gegen eine solche Funktion ausgesprochen. Als Argument gegen die Funktion wurde unter anderem ein größeres Haftungsrisiko für Rechtsanwälte herangezogen, da diese nach der bisherigen berufsrechtlichen Rechtsprechung erst dann ein Empfangsbekenntnis zurücksenden dürften, wenn sie die Frist auch in ihrem Fristenkalender notiert hätten.[619]

6.1.3 Integration in SAFE und Trusted Domains

Mit der Integration in SAFE[620] bietet das EGVP die Möglichkeit, die Kommunikationsinfrastruktur – insbesondere die Intermediäre und die Authentifizierungsserver (in der SAFE-Terminologie als Identity Provider bezeichnet)[621] – statt unter der Kontrolle einer einzigen zentralen Instanz zu halten, dergestalt aufzuteilen, dass bestimmte Nutzergruppen ihre eigene Infrastruktur pflegen und kontrollieren können, ohne dass hierdurch die Kommunikation im Gesamtsystem erschwert werden würde.[622] Möglich wird dies durch die Bereitstellung abgetrennter sogenannter *Trusted Domains*, die über standardisierte Kommunikationswege in Verbindung miteinander stehen und Nachrichten austauschen können. Durch die Hinzufügung einer Trusted Domain zu einer Benutzerkennung kann das System EGVP Nachrichten an die in ihm hinterlegten Server der jeweiligen Trusted Domain weiterleiten, die dann die weitere Verarbeitung einschließlich Zuordnung, Prüfung und Zustellung der Nachricht übernehmen.

616 *Bundesrechtsanwaltskammer*, das beA und die BRAK, Abschnitt „BRAK fördert und unterstützt“; vgl. hierzu auch oben unter 3.1.7.
617 *Backs/Kühnelt/Sandkühler/Schmid u. a.*, BRAK-Stellungnahme Nr. 6/2012
618 So beispielsweise in *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 14/2012, 8 und *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012 13 f.
619 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 12.
620 Vgl. hierzu auch bereits oben unter 3.1.6.
621 *Ehrmann/Wöhrmann/Streckel/Krause*, 19.
622 *Ehrmann/Wöhrmann/Streckel/Krause*, 11.

Mit dem besonderen elektronischen Anwaltspostfach soll die Bundesrechtsanwaltskammer nach dem durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten neu eingefügten § 31a Abs. 1 BRAO von diesem System Gebrauch machen, indem sie eine Postfachinfrastruktur für Mitglieder der Rechtsanwaltskammer schafft. Die Bundesregierung betrachtet den hierdurch erteilten Auftrag an die Bundesrechtsanwaltskammer als Ausfluss der anwaltlichen Selbstverwaltung.[623] Auch eine Kommunikation zwischen Nutzern des besonderen elektronischen Anwaltspostfachs ist hiermit möglich.[624] Dies stellt eine Veränderung gegenüber der bisherigen Nutzungsmöglichkeit des EGVP dar, da das EGVP Nutzern in der Rolle des Bürgers (wozu auch anwaltliche Nutzer zählen) bisher nur die Kommunikation mit Gerichten ermöglichte, nicht jedoch mit anderen EGVP-nutzenden Bürgern.

6.1.3.1 Authentifizierung

Bei der Frage der Authentifizierung sind genau genommen zwei Fälle zu unterscheiden: Die Authentifizierung durch sichere Anmeldung am System sowie die Authentifizierung gegenüber dem Nachrichtenempfänger durch elektronische Signaturen. Die Anmeldung am System und das Öffnen des eigenen Postfachs setzt beim EGVP-Client eine kryptografisch abgesicherte Anmeldung über ein (Hardware- oder Software-)Zertifikat voraus, das durch eine PIN-Eingabe gesichert ist.[625] Empfohlen wird in der Anwenderdokumentation ausdrücklich die Benutzung eines Softwarezertifikats, um die Erzeugung nicht personengebundener Postfächer für Vertretungsfälle zu ermöglichen.[626] Ungeklärt war demgegenüber beim EGVP-Client noch die Frage, wie mit EGVP-Nachrichten umgegangen werden konnte, die bereits durch ein Gericht versandt worden und im EGVP-Postfach eines Anwalts eingegangen waren. Im Falle der Abwesenheit des Postfachinhabers wäre in solchen Fällen kein Zugriff auf das Postfach und somit auch keine Kenntnisnahme von den Nachrichten durch Vertreter möglich. In der Praxis dürfte sich mancher Nutzer damit beholfen haben, das zum Zugang zum Postfach benötigte Zertifikat schlicht an Kollegen weiterzugeben, um unbemerkte Rechtsfolgen durch im Vertretungsfall eingegangene, aber nicht abrufbare elektronische Nachrichten zu umgehen. Auch für das besondere elektronische Anwaltspostfach ist eine solche Anmeldung mit zwei getrennten Sicherungsmitteln (sogenannte Zwei-Faktor-Authentifizierung)

623 Dies ergibt sich aus den Antworten der Bundesregierung auf eine kleine Anfrage, BT-Drs. 18/9994, 2 f.
624 *Bundesrechtsanwaltskammer*, Teilnehmer am ERV, Abschnitt „Rechtsanwälte“.
625 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 40, 42.
626 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 40.

erforderlich.[627] Das Problem einer Weitergabe von Sicherungsmitteln an Dritte hat man hier dadurch zu entschärfen versucht, dass eine Anmeldung an das beA auch anderen Personen als dem Inhaber des Postfachs gestattet werden kann, wobei es ein ausdifferenziertes Berechtigungssystem mit einzeln vergebbaren Berechtigungen für verschiedene Handlungen geben soll.[628] Technisch soll der Zugriff durch Dritte beim beA durch ein Hardware-Sicherheitsmodul realisiert werden, mit dem die Befugnisse des sich anmeldenden Nutzers überprüft werden können.[629] Diese Formulierung der Bundesrechtsanwaltskammer scheint auf die Verwendung eines physischen (d.h. Hardware-)Tokens zur Authentifizierung hinzudeuten, unklar ist hierbei jedoch, wie sich diese zur persönlichen Authentifizierug eines Dritten gegenüber dem System verhält. Für letztere wird in der Beschreibung des beA die Verwendung eines Hardware- oder Softwarezertifikats als Voraussetzung verlangt. Denkbar wäre insofern, dass bei der Anmeldung von Personen, die nicht Postfachinhaber sind, darüber hinaus die Verwendung eines weiteren Sicherungsmittels, in das die einzelnen vergebenen Befugnisse kodiert sind, verlangt wird.

Die Unterstützung elektronischer Signaturen im Sinne des nunmehr aufgehobenen und durch die eIDAS-Verordnung ersetzten Signaturgesetzes fand sich bereits im Standard OSCI 1.2. Die Signaturen werden in unterschiedlichen Qualitätsstufen (fortgeschrittene und qualifizierte elektronische Signaturen[630]) unterstützt und sowohl auf Ebene der Inhaltsdaten als auch auf der der Nutzungsdaten angeboten.[631] Die Möglichkeit der Signaturnutzung findet sich auch beim EGVP sowie dem beA. Im Gegensatz zu den von OSCI 1.2 angebotenen Verschlüsselungsmethoden für Inhaltsdaten sind die Signaturverfahren jedoch auch bei EGVP und beA optional.[632] Beim EGVP wurde die Benutzung einer qualifizierten elektronischen Signatur allerdings zumindest vor dem 1. Januar 2018 empfohlen, da eine solche auch Zulässigkeitsvoraussetzung einer fristwahrenden Schriftsatzeinreichung bei den teilnehmenden Gerichten bis zu diesem Zeitpunkt war.[633] Als ausreichend wurde hier allerdings – trotz des insofern irreführenden Wortlautes von § 130a Abs. 1 a.F., nach dem die Signatur „das Dokument“ erfassen soll – eine Containersignatur betrachtet, bei der mehrere Dokumente zusammengefasst und dann gemeinsam signiert werden.[634] Dies erscheint

627 *Bundesrechtsanwaltskammer*, Zugang zum beA, Abschnitt „Anmeldung, Login“.
628 *Bundesrechtsanwaltskammer*, Zugriffsrechte.
629 *Bundesrechtsanwaltskammer*, Sichere Anmeldung.
630 Dies umfasst selbstverständlich auch qualifizierte elektronische Signaturen mittels Zertifikaten von akkreditierten Zertifizierungsdiensteanbietern, die zum Teil als akkreditierte Zertifikate bzw. akkreditierte elektronische Signaturen bezeichnet werden, technisch aber keine anderen Anforderungen stellen als qualifizierte elektronische Signaturen.
631 *OSCI Leitstelle*, OSCI-Transport 1.2 Spezifikation, 18 f.
632 Für das EGVP vgl. hierzu *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 29 sowie *Berlit*, JurPC Web-Dok. 13/2006, Rn. 22.
633 Z.B. nach § 130a ZPO a.F., vgl. hierzu oben unter 3.1.3.
634 *Müller*, 130.

jedoch folgerichtig, da die Signatur des Containers durch die Bestätigung der Authentizität der darin enthaltenen Dokumente im Verbund auch die Authentizität jedes einzelnen Dokuments bestätigt, sofern der Verbund zur Prüfung noch rekonstruierbar ist.

Für das besondere elektronische Anwaltspostfach ergibt sich die Freiwilligkeit der Benutzung einer qualifizierten elektronischen Signatur aus den durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten geänderten Normen wie beispielsweise § 130a Abs. 3 und 4 Nr. 2 ZPO oder den deckungsgleichen Vorschriften in anderen Prozessordnungen.[635] Hiernach ist eine elektronische Einreichung ab dem Wirksamkeitsbeginn der entsprechenden Normen mit dem 1.1.2018 dann formwahrend, wenn sie mit einer qualifizierten elektronischen Signatur eingereicht wird, oder von der verantwortenden Person signiert und über einen sicheren Einreichungsweg versandt wurde (Abs. 3). Auf eine qualifizierte elektronische Signatur kommt es demnach nach dem ERV-Gesetz bei Einreichung über einen sicheren Einreichungsweg wie das beA gerade nicht mehr an, es reicht vielmehr bereits die bloße textuelle Wiedergabe des Namens als Signatur (einfache elektronische Signatur).[636] Hiermit soll dem Umstand Rechnung getragen werden, dass die aufgezählten Übertragungswege ein höheres Maß an Sicherheit bieten sollen als eine einfache E-Mail, und zugleich die qualifizierte elektronische Signatur vermieden werden. Zu beachten ist jedoch, dass der Verzicht auf die qualifizierte elektronische Signatur nur dann greift, wenn die Dokumente vom Postfachinhaber, d.h. dem registrierten Rechtsanwalt selbst, versendet werden.[637] Dies gilt jedenfalls dann, wenn man in der Formulierung des § 130a Abs. 3 ZPO n.F. bzw. der entsprechenden Normen anderer Prozessordnungen das „und“ so liest, dass auch die Einreichung „von der verantwortenden Person“ erfolgen muss. Eine andere Lesart, nach der sich das Merkmal der „verantwortenden Person“ nur auf die Signatur beschränkt, erscheint jedoch nicht ganz fernliegend. Die Gesetzesbegründung scheint die erste Lesart zwar zu bestätigen, da dort davon die Rede ist, dass eine Identität der vom System als Absender ausgewiesen Person mit der das elektronische Dokument verantwortenden Person feststellbar sein müsse, um eine wirksame Einreichung zu bewirken.[638] Bei genauerer Betrachtung sagt jedoch auch diese Formulierung nur aus, dass die Signatur auf den Postfachinhaber lauten muss, nicht jedoch, dass der letztendliche Versendevorgang auch durch diesen erfolgen muss. Damit würde die Rechtslage faktisch der bisher für analoge Einreichungen geltenden entsprechen, nach der der Rechtsanwalt Schriftstücke unterschreibt, und diese durch Kanzleimitarbeiter versendet werden. Die tatsächliche Auslegung dieser Norm in der Praxis wird den Gerichten überlassen bleiben. Bis zu einer diesbezüglichen

635 § 46c ArbGG, § 65a SGG, § 55a VwGO und § 52a FGO.
636 Vgl. hierzu oben unter 2.3.2.
637 *Bundesrechtsanwaltskammer*, Nachrichtenerstellung und Versand.
638 BT-Drs. 17/12634, 25.

Entscheidung dürfte sich eine gewisse Rechtsunsicherheit ergeben, der anwaltliche Nutzer durch das vorsorgliche Anbringen einer qualifizierten elektronischen Signatur begegnen können.

6.1.3.2 Verwaltung von Schlüsseln und Identitäten der Teilnehmer

Teil des EGVP ist ein Teilnehmerverzeichnis, in dem alle registrierten Teilnehmer des Systems auffind- und gegebenenfalls erreichbar sind. Dies ergibt sich daraus, dass für das EGVP die Hinterlegung eines Authentifizierungsschlüssels im System erforderlich ist, mit dem sich der Postfachinhaber gegenüber dem Intermediär als berechtigt ausweisen kann. Die Auflistung der Nutzer in dem Verzeichnis ist damit abschließend, ein Versand an Personen oder Einrichtungen, die nicht im Verzeichnis auffindbar sind, ist nicht möglich.[639] Dem Vorteil einer eindeutigen Adressierung der Teilnehmer im System und der Vermeidung von Tippfehlern seitens des Nutzers steht die Gefahr gegenüber, unter mehreren gleichnamigen Nutzern den falschen auszuwählen. Auch bloße Bedienungsfehler in Form eines „Verklickens“ sind nicht völlig auszuschließen, dies stellt jedoch ein Grundproblem grafischer Benutzeroberflächen von Softwareprodukten dar, das in gewissem Maße systemimmanent und unvermeidbar ist. Ein (originäres) Manko des EGVP ist jedoch die fehlende Erkennbarkeit, ob ein Postfach tatsächlich noch vom Inhaber eingesehen wird oder lediglich ein Überbleibsel eines früheren Versuchs mit dem EGVP darstellt. Eine Abhilfemöglichkeit, die allerdings ebenfalls ein Tätigwerden des jeweiligen Inhabers eines verwaisten oder nicht mehr gewünschten Postfachs erfordert, ist eine Löschungsmöglichkeit. Mit einem Löschformular auf der EGVP-Homepage können Nutzer ihren EGVP-Zugang und damit auch ihre Adressierbarkeit über das System deaktivieren.[640] Beim beA relativiert sich dieses Problem dadurch, dass schlicht jeder Rechtsanwalt auch ohne Willensakt ein besonderes elektronisches Anwaltspostfach zugewiesen bekommt, an das nach dem Stichtag auch fristauslösende Zustellungen erfolgen können und werden. Hierdurch werden genau genommen gleich zwei Probleme des EGVP umgangen – zum einen ist jedem Nutzer nur noch genau ein (beA-)Postfach zugeordnet, so dass keine Unsicherheit bezüglich etwaiger Testpostfächer oder vom Nutzer vergessener Postfächer entsteht. Zum anderen erfolgt eine Löschung des beA-Postfachs automatisch durch die BRAK, wenn die Zulassung zur Anwaltschaft erlischt, einschließlich im Falle des Todes des Benutzers.[641]

---

639 Vgl. hierzu *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation 71.

640 Das Löschungsformular findet sich unter http://www.egvp.de/serviceformular/index.php, zuletzt aufgerufen am 18.12.2017.

641 *Bundesrechtsanwaltskammer*, Grundlegende Fragen, Frage 8.

6.1.4 Verwaltung des Systems und Kosten

Das EGVP ist ein Projekt, das als Pilotprojekt von Bundesverwaltungsgericht, Bundesfinanzhof, dem Bundesamt für Sicherheit in der Informationstechnik und der Bundesländer Hessen und Bremen initiiert wurde und durch eine mehrheitlich durch die öffentliche Verwaltung kontrollierte GmbH & Co. KG betrieben wird.[642] Damit stellt das EGVP ein Angebot der öffentlichen Verwaltung dar, dessen primärer Fokus klar auf den Interessen von Justiz und Verwaltung liegt. Dies mag mit der ursprünglichen Intention für das System zu tun haben, durch Vorantreiben der Digitalisierung in Verwaltung und Justiz Einspareffekte zu erzielen. Bei der Anwaltschaft hat diese Verbindung jedoch zum Teil zu Verstimmungen geführt. So wurde teilweise eine mangelnde Nutzerfreundlichkeit des Systems aus anwaltlicher Sicht darauf zurückgeführt, dass die Entwicklung des Systems sich in erster Linie an den Bedürfnissen der Justiz orientiere.[643] Das besondere elektronische Anwaltspostfach wird demgegenüber im Auftrag und unter der Kontrolle der Bundesrechtsanwaltskammer entwickelt und geführt, die als Selbstverwaltungsorgan der Anwaltschaft Anlass zur Erwartung gibt, dass sie vorrangig die Interessen der Anwaltschaft bei der Ausgestaltung des Postfachs berücksichtigt. Auch bestehen keine ernsthaften Zweifel dahingehend, dass die Bundesrechtsanwaltskammer nicht das notwendige Sicherheits- und Vertraulichkeitsniveau für ein Anbieten des elektronischen Rechtsverkehrs bieten könnte. Denn zum einen begibt sich die Bundesrechtsanwaltskammer durch das Anbieten des besonderen elektronischen Anwaltspostfachs in die Rolle eines Telemedienanbieters, womit sie den Dienste durch technische und organisatorische Maßnahmen gegen Kenntnisnahme Dritter schützen und unter anderem den Datenschutz und die Störungssicherheit gewährleisten muss.[644] Durch die angestrebte vollständige Ende-zu-Ende-Verschlüsselung beim beA sind bei technisch korrekter Umsetzung weder die Bundesrechtsanwaltskammer oder der von ihr beauftragte technische Dienstleister noch Dritte tatsächlich nicht im Stande, die Inhalte der Kommunikation mitzulesen, ohne im Besitz des passenden privaten Schlüssels zu sein. Letzterer verbleibt aber nach der technischen Konzeption sowohl des EGVP als auch des darauf aufbauenden beA stets beim Inhaber des Postfachs. Selbst die Bundesrechtsanwaltskammer als Betreiberin des beA hätte somit selbst wenn sie es wollte keinen Zugriff auf die Klartextdaten.[645]

Es ist anzunehmen, dass seitens des Gesetzgebers nicht nur die konsequent scheinende Zuordnung

642 Vgl. hierzu oben unter 2.3.3 zur Geschichte des EGVP.
643 *Bundesrechtsanwaltskammer*, Vorschläge ERV, 2.
644 Vgl. hierzu oben unter 3.2.3.2.
645 Vgl. aber zur tatsächlichen Ausgestaltung der Verschlüsselung beim besonderen elektronischen Anwaltspostfach unten unter 7.2.2.

der anwaltlichen Kommunikation zum Träger anwaltlicher Selbstverwaltung maßgeblich war, sondern in erster Linie eine Umschichtung der Kosten von der öffentlichen Hand auf die konkret betroffene Interessengruppe. So diese Erwartung eine Rolle gespielt haben sollte, dürfte sie sich durch die praktische Umsetzung des besonderen elektronischen Anwaltspostfachs realisieren, da dieses von der Bundesrechtsanwaltskammer durch eine Umlage auf alle Kammermitglieder finanziert wird. Nach Angaben der Bundesrechtsanwaltskammer werden für die Bereitstellung des Gesamtsystems beA pro Jahr und Kammermitglied voraussichtlich 65 bis 70 Euro erhoben.[646] Dies ist zwar eine spürbare „Verteuerung“ gegenüber dem aus Nutzersicht kostenlosen EGVP, erscheint aber insbesondere für Rechtsanwälte nicht unverhältnismäßig teuer.

6.2 Weiterentwicklung des Systems und alternative Zugriffswege

Wie bereits gezeigt, ist das EGVP zumindest im hier zu Grunde gelegten Verständnis mehr als nur die für Bürger bereitgestellte EGVP-Client-Software, sondern vielmehr ein Kommunikationssystem, das auf dem Standard OSCI basiert. Dies bedeutet auch, dass es neben dem EGVP-Client auch andere, kompatible Softwareprodukte gibt, die mit anderer Software im EGVP-Netzwerk interoperabel ist. So gibt es beispielsweise eigene Produkte für Behördennetze und die Integration in anwaltliche Fachsoftware. Zum anderen hat sich das System EGVP im Laufe der Zeit auch gewandelt. Zum Teil wurden früher verfolgte Ansätze zu Nutzungsarten und Angebotsformen aufgegeben, weil sie sich in der Praxis als untauglich erwiesen haben oder weil sich durch Neuerungen wie das beA die Bedeutung und die Umsetzung des EGVP verändert hat. Wenngleich der Fokus dieser Arbeit auf dem verbreiteten EGVP-Client und dem besonderen elektronischen Anwaltspostfach liegt, soll dennoch hier kurz auf weitere Schnittstellen des Systems EGVP eingegangen werden.

6.2.1 EGVP Enterprise

EGVP Enterprise ist eine Software zur Integration einer Kommunikation über das EGVP in bestehene IT-Umgebungen. Ziel der Software ist es, professionellen Anwendern wie großen Firmen oder Kanzleien die Nutzung des EGVP zu ermöglichen, ohne sich hierzu auf den EGVP-Client mit seinen begrenzten Einbindungsmöglichkeiten in die eigene Softwareumgebung festlegen zu

646 *Bundesrechtsanwaltskammer*, Was kostet das beA?

müssen. EGVP Enterprise bietet hierzu einen Server, der als Mittler (Middleware) zwischen der eigenen Softwareumgebung und dem EGVP-System fungiert.[647] Hiermit ist es möglich, die eigene Softwareumgebung wie beispielsweise Mailprogramme im Grundsatz weiter nutzen zu können, wenn diese auf die Kommunikation mit dem EGVP Enterprise-Server angepasst wurden. Dadurch ergibt sich auch die Zielgruppe für so eine Umsetzung, da für kleinere Unternehmen oder Kanzleien in der Regel ein solcher technischer Aufwand wirtschaftlich nicht rentabel oder auch nur möglich ist. Hinzu kommt, dass die Nutzung des EGVP Enterprise-Servers gesondert bei der AG IT-Standards der Bund-Länder-Kommission beantragt werden muss.[648] Mit dem durch das ERV-Gesetz neu eingeführten besonderen elektronischen Anwaltspostfach hat sich der Fokus noch weiter von Nutzern in der freien Wirtschaft hin zu Behörden und Gerichten verschoben, da Teil des Konzeptes des besonderen elektronischen Anwaltspostfachs auch ist, dass neben dem Zugang über ein Webinterface eine Softwareschnittstelle (API) für Drittanbieter bereitgestellt wird, mit der diese eine Kommunikation über das beA in eigene Produkte, insbesondere Anwaltssoftware, integrieren können.[649] Zu den Nutzern von EGVP Enterprise zählt aber beispielsweise die Hessische Justiz, die das Produkt für die elektronische Kommunikation der Justiz benutzt.[650]

6.2.2 EGVP-Client

Auch der in Java programmierte EGVP-Client hat sich im Laufe der Zeit weiterentwickelt. Die diversen technischen Änderungen und Verbesserungen im Laufe der Jahre spiegeln sich auch in der steigenden Versionsnummer wider, die mit Stand Dezember 2016 aktuelle Version ist beispielsweise 3.0. Was die Betrachtung des Produktes EGVP-Client erschwert, ist die teilweise uneinheitliche Terminologie, die im Umgang mit ihm selber in der offiziellen Dokumentation verwendet wird. Insbesondere wird der EGVP Classic Client dort auch schlicht als EGVP bezeichnet, was eine saubere Trennung zwischen dem System EGVP, dem EGVP Classic Client und anderen Produkten wie EGVP Enterprise erschwert.

Durch die Pläne zur Einführung des besonderen elektronischen Anwaltspostfachs wurde beschlossen, den EGVP Classic Client nicht mehr weiterzuführen. Die Daten zur Abkündigung und zum später darauf folgenden Supportende für den Client wurden im Laufe des Jahres 2016 mehrfach geändert.[651] Sicher scheint, dass der EGVP Classic Client in Zukunft nicht mehr

647 *Ministerium der Justiz und für Europa Baden-Württemberg*, EGVP.
648 *egvp.de*, Änderungen zum 1.1.2016.
649 *Bundesrechtsanwaltskammer*, Browser oder Kanzleisoftware.
650 *Hessisches Ministerium der Justiz*, Länderbericht 2016, 5.
651 *Deutscher Anwaltverein*, längere EGVP-Verfügbarkeit.

weitergepflegt werden soll. Geplant ist stattdessen ein Übergangsprodukt, das nur noch einen lesenden Zugriff auf die EGVP-Postfächer bieten soll. Für eine aktive Kommunikation über das EGVP-System ist demnach je nach Rolle der Nutzer ein unterschiedlicher Weg vorgesehen. Rechtsanwälte werden nach dem Start des besonderen elektronischen Anwaltspostfachs auf dieses verwiesen. Anwendern, die nicht zu den professionellen Einreichern im Sinne des ERV-Gesetzes gehören, soll demgegenüber ein Webbasierter EGVP-Client zur Verfügung gestellt werden, der jedoch nur die Einreichung elektronischer Dokumente ermöglicht, ohne zugleich ein empfangsbereites Postfach als Rückkanal zu eröffnen.[652] Für Behörden soll es weiterhin das Produkt EGVP Enterprise zur Integration in die eigene IT-Landschaft geben.[653]

Die erzwungene Migration auf das besondere elektronische Anwaltspostfach dürfte für die Nutzer durchaus Vorteile mit sich bringen. Zwar werden hierdurch zunächst einmal gewohnte Arbeitsabläufe in den Kanzleien in Frage gestellt. Allerdings gilt dies vorrangig für die Nutzer, die bisher den EGVP-Classic Client ohne Einbindung in eine anwaltliche Fachsoftware benutzt haben, da von den Anbietern anwaltlicher Fachsoftware bereits Produkte verfügbar sind, die eine Interaktion mit dem besonderen elektronischen Anwaltspostfach ermöglichen. Für diese Nutzer dürfte damit mit dem Wechsel zum beA kaum eine Umstellung verbunden sein. Zudem weist die Integration des EGVP-Classic Clients durchaus Schwierigkeiten auf, beispielsweise ist ein Versenden von (normalen) E-Mails aus dem Client unter bestimmten Umständen nicht möglich, was beispielsweise auch den Versand von Fehlermeldungen des Programms an die Supportadresse der für den Support zuständigen Firma Westernacher betrifft.[654] Auch war zumindest nach der offiziellen Dokumentation eine Lauffähigkeit des EGVP-Clients zwar unter Windows und Linux, nicht aber unter – dem im Vergleich zu Linux deutlich weiter verbreiteten – MacOS von Apple gewährleistet.[655] Dem gegenüber soll das besondere elektronische Anwaltspostfach auch unter MacOS X lauffähig sein.[656] Unklar ist jedoch noch, ob sich diese Voraussetzungen nur auf die Nutzung des Webinterfaces beziehen (hierauf deutet der Hinweis, dass eine Nutzung auch mit anderen Browsern und Betriebssystemen möglich ist hin), oder ob hiervon auch die auf dem Rechner zu installierende Java-Software Client Security[657] erfasst wird.

Positiv ist auch hervorzuheben, dass im Gegensatz zum EGVP ein erklärtes Entwicklungsziel des besonderen elektronischen Anwaltspostfachs eine barrierefreie Nutzungsmöglichkeit nach den

652 *Barthel*, 16.
653 *Governikus GmbH & Co. KG*, 25. EDVGT.
654 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 9.
655 *Governikus GmbH & Co. KG*, EGVP-Anwenderdokumentation, 8 f.
656 *Bundesrechtsanwaltskammer*, Unterstützte Browser und Betriebssysteme.
657 Vgl. hierzu *Bundesrechtsanwaltskammer*, Technische Fragen sowie *Bundesrechtsanwaltskammer*, Erstregistrierung.

Kriterien des Behindertengleichstellungsgesetzes für barrierefreie Informationstechnologie (BITV 2.0) für blinde bzw. sehbehinderte Nutzer ist.[658] Dies entspricht auch der Vorgabe in § 31a Abs. 1 BRAO, der durch das ERV-Gesetz neu eingefügt wurde und nach dem das besondere elektronische Anwaltspostfach barrierefrei ausgestaltet sein soll.[659]

7 Erfüllung der Anforderungen an den elektronischen Rechtsverkehr durch das EGVP

Nachdem nun im 5. Kapitel Kriterien für den elektronischen Rechtsverkehr im Sinne dieser Betrachtung herausgearbeitet wurden und in Kapitel 6 das elektronische Gerichts- und Verwaltungspostfach als System für den elektronischen Rechtsverkehr näher betrachtet wurde, soll die Eignung des EGVP als eine mögliche Umsetzung des elektronischen Rechtsverkehrs nach den erarbeiteten Kriterien untersucht werden. Hierbei wird das zuvor beschriebene Verständnis des EGVP als System und nicht als (einzelnes) Softwareprodukt zugrunde gelegt. Gleichwohl müssen an dieser Stelle die für Benutzer zur Verfügung stehenden Clientprogramme – insbesondere elektronische Anwaltspostfach und dessen Vorgänger EGVP-Classic-Client – betrachtet werden. Dies ergibt sich zum einen daraus, dass das System EGVP verschiedene Sicherheitsstufen und Sicherheitsfunktionen bereitstellt, deren Benutzung jedoch zum Teil nicht verpflichtend ist, sondern vielmehr den Anforderungen des Client-Programms überlassen ist. Zum anderen lassen sich bestimmte benutzerbezogene Kriterien wie die Ergonomie der Benutzeroberfläche, die Interoperabilität und auch die Kostenstruktur nur an konkreten Produkten, nicht aber am Gesamtsystem betrachten.

7.1 Datenschutz

Wie oben gezeigt, speist sich das Datenschutzrecht zunächst aus einer Vielzahl von Normen unterschiedlicher Stufen in der Normenpyramide. Maßgebliche Rechtsquelle ist für die Beurteilung der Datenschutzkonformität ist jedoch ab dem 25. Mai 2018 die Datenschutzgrundverordnung, deren Anforderungen der elektronische Rechtsverkehr somit ab diesem Zeitpunkt genügen muss.

Bei der Beurteilung der stattfindenden Verarbeitungen personenbezogener Daten ist zu trennen

658 *Bundesrechtsanwaltskammer*, Das Postfach, Infokasten „Das beA ist barrierefrei“.

659 Vgl. hierzu auch die Begründung im Regierungsentwurf (BT-Drs. 17/12634, 21), in der explizit auf die Umsetzung der UN-Behindertenrechtskonvention sowie der barrierefreie Informationstechnologieverordnung verwiesen wird.

zwischen Daten des Mandanten, für die regelmäßig eine konkludente oder ausdrücklich erklärte Einwilligung vorliegen wird, und Daten von anderen Beteiligten, für die dies nicht erwartet werden kann.[660] Nach dem obigen Befund ergibt sich eine grundsätzliche Anwendbarkeit der Datenschutzgrundverordnung auch für den Bereich der Mandatsbearbeitung. Für die Verarbeitung personenbezogener Daten im Rahmen des elektronischen Rechtsverkehrs (und damit mittels Datenverarbeitungsanlagen) werden und in die vom Betroffenen keine Einwilligung vorliegt, wird regelmäßig Art. 6 Abs. 1 lit. f DSGVO als taugliche Rechtfertigung zur Verfügung stehen, so lange im Einzelfall die Interessen der Betroffenen nicht überwiegen, woran allerdings im Interesse eines effektiven Rechtsschutzes eher hohe Anforderungen gestellt werden sollten.

Eine andere Frage betrifft jedoch die Umstände der Datenverarbeitung, für die Art. 32 DSGVO technische und organisatorische Maßnahmen beschreibt, die bei der Umsetzung eines angemessenen Schutzniveaus helfen. In Art. 32 Abs. 1 lit. a DSGVO wird ausdrücklich Verschlüsselung als eine solche Maßnahme genannt. Wie oben dargestellt, sollte nach der hier vertretenen Ansicht eine Verschlüsselung nach dem Stand der Technik für den elektronischen Rechtsverkehr angestrebt werden. Hieran ändert sich auch dadurch nichts, dass durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs die verpflichtende elektronische Datenübertragung allgemein bekannt sein könnte, und insofern über das Merkmal der Umstände der Datenverarbeitung in Art. 32 Abs. 1 DSGVO eine Verringerung der Schutzbedürftigkeit der personenbezogenen Daten erfolgen könnte. Dies ist nämlich schon deshalb zweifelhaft, weil nicht jedem juristischen Laien die Verpflichtung zur elektronischen Einreichung von Schriftsätzen durch seinen Anwalt bekannt sein dürfte. Zum anderen sieht das ERV-Gesetz verschiedene Einreichungswege mit unterschiedlichen Sicherheitsniveaus vor, so dass aus der Erteilung eines Mandats nach Beginn des verpflichtenden elektronischen Rechtsverkehrs nicht darauf geschlossen werden kann, dass der Mandant auch mit allen danach zulässigen Einreichungswegen einverstanden ist.

Das Vorliegen und die Qualität der Verschlüsselung im EGVP bzw. beA wird im Folgenden thematisiert.

7.2 Integritätsschutz und Schutz vor unbefugter Kenntnisnahme

Wie im Rahmen der vorliegenden Betrachtung herausgearbeitet wurde, stellt die Sicherstellung der

660 Siehe hierzu oben unter 5.2.

Integrität und Vertraulichkeit von Nachrichten eine der großen Herausforderungen bei der digitalen Speicherung und Übertragung von Daten dar. Sie ist dabei wie gezeigt nicht bloß zufälliger Reflex, sondern vielmehr als Kehrseite des Vorteils einer verlustfreien Veränderung, Übertragung und Duplizierung digitaler Daten integraler Bestandteil moderner elektronischer Kommunikation. Für die Sicherstellung der Integrität und Vertraulichkeit von elektronischen Nachrichten haben sich insbesondere Verfahren zur Verschlüsselung und zu elektronischen Signaturen entwickelt, auf deren Umsetzung im Rahmen des EGVP und des beA nun eingegangen werden soll.

7.2.1 Transportverschlüsselung

Wie gezeigt wurde, stellt eine Transportverschlüsselung das unmittelbarste und grundlegendste Verfahren der Verschlüsselung von Daten bei elektronischer Kommunikation dar. Sie wird auch nicht durch eine Verschlüsselung von Inhaltsdaten entbehrlich, weil durch Transportverschlüsselung weitere Gefahren wie das „Kapern“ der Verbindung und Absenden eigener Nachrichten auf dem durch Dritte etablierten Kanal (sog. Man-in-the-middle-Angriff) und die Auswertung von Kommunikationsmetadaten, aus denen ebenfalls datenschutzrelevante Erkenntnisse abgeleitet werden können,[661] durch unberechtigte Dritte unterbunden werden können. Aus dem gleichen Grund macht die Benutzung einer elektronischen Signatur eine Transportverschlüsselung nicht entbehrlich. Denn die elektronische Signatur schützt lediglich vor der Bedrohung durch das Absenden gefälschter Nachrichten oder das unbefugte Verändern echter Nachrichten durch unbefugte Dritte, nicht aber vor einem Ausspähen der Nachrichten und der an den Kommunikation beteiligten Parteien.

Das System EGVP verwendet für die Verbindung zwischen Nutzer und Intermediär eine Transportverschlüsselung in Form einer SSL-Implementierung. Wenngleich über die Details der Implementierung wie verwendete Protokollversion keine verbindlichen Informationen erhältlich sind, ist doch bereits die Verwendung einer Transportverschlüsselung ein wünschenswerter Schritt. Etwaige Probleme durch bekannt werdende Lücken in den verwendeten Protokollen wie etwa den aus Sicht der IT katastrophalen Heartbleed-Bug in OpenSSL[662] können (und müssen) durch das beständige Überwachen und anpassen der Protokolle an den Stand der Technik erfolgen. Sie werden in ihrem Ausmaß jedoch durch die ebenfalls verwendete Inhaltsverschlüsselung abgemildert. Wie beim EGVP-Client wird auch beim besonderen elektronischen Anwaltspostfach eine

661 Hierzu zählen beispielsweise die Informationen dazu, wer zu welchem Zeitpunkt mit wem kommuniziert hat.
662 Vgl. hierzu bereits oben unter 4.8.2 Fn. 478.

Transportverschlüsselung eingesetzt werden.[663] Auch hier sind keine weiteren Details über die konkrete Implementierung bekannt. Aufgrund der Verwendung des OSCI-Standards und der Anlehnung an das EGVP ist aber davon auszugehen, dass faktisch die gleichen Verfahren wie beim EGVP zum Einsatz kommen. Insoweit gilt das oben gesagte auch hier.

Eine kritische Schwachstelle in der Konzeption des besonderen elektronischen Anwaltspostfachs hat sich kurz vor Beginn der passiven Nutzungspflicht zum 1. Januar 2018 ergeben. Am 22. Dezember 2017 musste das besondere elektronische Anwaltspostfach, das erst kurz zuvor zur fakultativen Nutzung durch die Anwaltschaft freigegeben worden war, vorübergehend wegen Sicherheitsbedenken abgeschaltet werden.[664] Die Bundesrechtsanwaltskammer hatte zunächst ab diesem Tag vermeldet, dass aufgrund eines Problems mit einem abgelaufenen Zertifikat für die intern vom beA benutzte TLS-Verschlüsselung die Installation eines neuen Zertifikats auf den Nutzerrechnern erfolgen müsse, wofür sie ein neues Zertifikat zur Verfügung stellte. Im weiteren Verlauf stellte sich jedoch heraus, dass der vermeintlich (relativ) harmlose Ablauf der Zertifikatsgültigkeit nicht das Hauptproblem war, sondern die BRAK vielmehr mit dem für alle beA-Nutzer gleichen öffentlichen Zertifikat zugleich den privaten Schlüssel im beA-Installationspaket mitgleifert hatte.[665] Als Problemlösung empfahl die BRAK den Nutzern daraufhin in einem weiteren, mittlerweile jedoch zurückgezogenen Sondernewsletter, ein neues, selbstsigniertes Zertifikat zu installieren. Da jedoch auch bei diesem Zertifikat der private Schlüssel wieder enthalten war, und es sich bei dem neuen Zertifikat zudem um ein root-Zertifikat handelte, mit dem auch weitere TLS-Zertifikate beglaubigt werden konnten, hätte dies dazu geführt, dass jeder Angreifer mit dem privaten Schlüssel aus dem – für jedermann öffentlich abrufbaren – beA-Installationspaket eine bösartige Website hätte gestalten können, die jedoch aufgrund des von allen beA-Nutzern akzeptierten Zertifikats diesen als vertrauenswürdig dargestellt worden wäre.[666] Einem Missbrauch in Form von Phishing-Angriffen, beispielsweise durch das Nachbilden einer gefälschten Online-Banking-Seite oder gar eines gefälschten besonderen elektronischen Anwaltspostfachs wäre somit Tür und Tor geöffnet gewesen. Als Konsequenz der Enthüllungen durch das CCC-Mitglied Markus Drenger und den hieraufhin erfolgenden öffentlichen Druck nahm die Bundesrechtsanwaltskammer das beA mit Meldung vom 27. Dezember 2017 nicht wieder in Betrieb und stellte eine Aufarbeitung der Sicherheitsprobleme in Aussicht.[667] Hierzu gehörte auch ein umfassender Security-Audit durch das Unternehmen Secunet AG, der einige weitere

663 *Brosch/Fiebig*, BRAK-Magazin 4/2015, 10, 11.
664 Vgl. hierzu *Bundesrechtsanwaltskammer*, Wartungsarbeiten am beA, in der allerdings nur von vereinzelten Verbindungsproblemen die Rede war.
665 *Borchers*, Heise-Newsticker 22.12.2017 mit Updates vom 23. Dezember 2017.
666 *Böck*, BRAK verteilt HTTPS-Hintertüre.
667 *Bundesrechtsanwaltskammer*, bea vorerst offline.

Sicherheitsrisiken zu Tage brachte. Zu den kritischsten Lücken gehörten eine Missbrauchsmöglichkeit des beA als Cloud-Speicher für beliebige Dateien[668], eine Möglichkeit zum Auslesen der Metadaten fremder Nachrichtenanhänge[669], eine Änderungsmöglichkeit von signierten XML-Nachrichten durch Innentäter[670] und veraltete Softwarekomponenten in der beA Client Security.[671] Von diesen im Gutachten als betriebsverhindernd beschriebenen Schwachstellen wurden jedoch im Verlaufe des Audits durch den Dienstleister ATOS zwei geschlossen. Von den beiden verbleibenden kritischen Schwachstellen wurde die Änderungsmöglichkeit signierter XML-Nachrichten nach Fertigstellung des Gutachtens von ATOS behoben. Das Beheben der verbleibenden betriebsverhindernenden Schwachstelle (Ziffer 3.5.4, veraltete Softwareelemente) wurde zusammen mit dem Beheben weiterer – jedoch nicht aller – weniger kritischer Schwachstellen von der BRAK zur Bedingung gemacht, zum 4. Juli 2018 die beA Client Security wieder zum Download anzubieten und damit die Voraussetzung für die Inbetriebnahme des beA zum 3.9.2018 zu schaffen.[672] Mit einem Sondernewsletter vom 20. August 2018 vermeldete die Bundesrechtsanwaltskammer schließlich, dass nach Aussage der Firma Secunet alle verbleibenden Schwachstellen, deren Behebung die Bundesrechtsanwaltskammer zur Voraussetzung der Wiederinbetriebnahme des beA gemacht hatte, beseitigt seien.[673]

Bedenken blieben hinsichtlich der nicht vorhandenen Ende-zu-Ende-Verschlüsselung bestehen. So wird im Gutachten festgestellt, dass das beA hinter den kryptografischen Möglichkeiten zurückbleibt und sich stellenweise stattdessen auf organisatorischen sowie physikalischen Schutz wichtiger Systemkomponenten beschränke.[674] Hierin wurde jedoch von der BRAK kein Hindernis für einen erneuten Livegang gestehen.

Das beA nahm schließlich am 3. September 2018 den Betrieb wieder auf. Die in § 31a Abs. 6 BRAO festgelegte passive Nutzungspflicht lebte hiermit ebenfalls wieder auf.

7.2.2 Ende-zu-Ende-Verschlüsselung

Eine oft als Alleinstellungsmerkmal präsentierte Eigenart des EGVP ist die benutzte Ende-zu-Ende-Verschlüsselung, die eine Entschlüsselung nur durch den berechtigten Empfänger, nicht jedoch

668 *secunet Security Networks AG*, beA-Abschlussgutachten, Ziffer 3.5.1
669 *secunet Security Networks AG*, beA-Abschlussgutachten, Ziffer 3.5.2
670 *secunet Security Networks AG*, beA-Abschlussgutachten, Ziffer 3.5.3
671 *secunet Security Networks AG*, beA-Abschlussgutachten, Ziffer 3.5.4
672 *Bundesrechtsanwaltskammer*, Presseerklärung 19/2018.
673 *Bundesrechtsanwaltskammer*, beA-Sondernewsletter, Abschnitt „Los geht‘s“.
674 *secunet Security Networks AG*, beA-Abschlussgutachten, S. 11.

durch Dritte erlaubt, wobei ein Zugriff selbst durch Dritte im Lager des Dienstebetreibers, die Zugriff auf die technische Infrastruktur, auf der der Postfach gehostet wird haben, ausgeschlossen ist. Hierbei ist zu unterscheiden zwischen der Sicherheit des Systems einerseits und der Sicherheit der Schlüssel andererseits. Denn eine Ende-zu-Ende-Verschlüsselung, die zwar formell die Verschlüsselung an nur einen Adressaten erlaubt, bei deren Umsetzung aber nicht zugleich gewährleistet ist, dass nur an diesen Adressaten verschlüsselt wird, kann nicht als echte Ende-zu-Ende-Verschlüsselung betrachtet werden, wenn der private Schlüssel des Adressaten systembedingt noch anderen Parteien zugänglich ist. Vielmehr muss das Gesamtsystem die Vertraulichkeit der Kommunikation zu schützen in der Lage sein.

Für den EGVP-Classic Client dürfte eine echte Ende-zu-Ende-Verschlüsselung gegeben sein. Trotz mehrjähriger Nutzung des Systems in der Praxis und der kritischen Begutachtung durch Experten sind bisher keine ausnutzbaren Schwachstellen oder gar ein tatsächliches Durchbrechen der Verschlüsselung beim EGVP bekannt geworden. Der vom EGVP-Client verwendete Verschlüsselungsalgorithmus AES-256 für die Ende-zu-Ende-Verschlüsselung entspricht dem Stand der Technik.[675] Auch die Schlüsselverwaltung lässt keine offensichtlichen Schwachstellen erkennen, insbesondere erfolgt die Erzeugung des privaten Schlüssels auf dem Benutzerrechner (bei der zuletzt empfohlenen Benutzung eines Softwarezertifikats) oder bei einem zertifizierten Trustcenter in Form eines Hardwaretokens (bei Verwendung einer Chipkarte). Die Speicherung der öffentlichen Schlüssel ist zumindest unter Sicherheitsgesichtspunkten bei einem korrekt umgesetzten Public-Key-Verfahren irrelevant, da aus einem öffentlichen Schlüssel der private Schlüssel nicht ableitbar ist. Die Schlüsselverwaltung und Überprüfung von Identitäten erfolgt innerhalb der Trusted Domain durch den Identity Provider, hierzu werden mehrere offene Kommunikations- und Sicherheitsprotokolle benutzt.[676] Hierdurch dürften zwei wesentliche Sicherheitskriterien für IT-Systeme, nämlich die Anpassung an neue Erkenntnisse und Bedrohungslagen sowie die öffentliche Begutachtung und Überprüfung von Sicherheitstechnologien, gewährleistet sein.

Für das besondere elektronische Anwaltspostfach sollten die obigen Erwägungen grundsätzlich auch gelten, da es das gleiche System wie das EGVP benutzt und sowohl während des Gesetzgebungsverfahrens[677] als auch während der Konzeption und der Testphase des beA durch die

675 Siehe hierzu Abschnitt 6.1.1.

676 So kommen für SAFE offene Standards, die von der non-profit-Organisation OASIS, die sich für offene Standards in der Informationsgesellschaft einsetzt und der auch große IT-Unternehmen wie IBM und Microsoft angehören, zum Einsatz. Zu den verwendeten Sicherheitsstandards gehören WS-Policy, SecurityPolicy, PolicyAssertions sowie WS-Trust, WS-Federation und WS-Security, vgl. *Apitzsch/Hartnick/Krause/Lüttich u. a.*, SAFE-Schnittstellenspezifikation S.52 ff.

677 Siehe hierzu z.B. den Regierungsentwurf des ERV-Gesetzes, BT-Drs. 17/12634, 47.

Bundesrechtsanwaltskammer[678] eine Ende-zu-Ende-Verschlüsselung zugesagt wurde. Fragwürdig erscheint in dieser Hinsicht jedoch die Umsetzung der ebenfalls in Aussicht gestellten verschiedenen Zugangsberechtigungen. Nach den Informationen der BRAK sollen diese durch ein sogenanntes Hardware-Sicherheitsmodul (HSM) in Form einer „Umverschlüsselung" erfolgen.[679] In dieser Aussage wird zum Teil eine Abweichung vom Versprechen einer Ende-zu-Ende-Verschlüsselung gesehen, weil die Umverschlüsselung auf den Servern der Bundesrechtsanwaltskammer stattfinden soll.[680] Wäre dies der Fall, könnte man nicht mehr von einer Ende-zu-Ende-Verschlüsselung sprechen, ohne sich dem Vorwurf der Täuschung auszusetzen. Denn in dem Moment, in dem die Bundesrechtsanwaltskammer auf Servern in ihrem Hoheitsbereich technisch zur Entschlüsselung und Neuverschlüsselung von Nachrichten in der Lage ist, könnte sie faktisch auch Einsicht in die Daten nehmen. Eine Umverschlüsselung setzt nach dem bisherigen Stand der Technik eine Entschlüsselung und Neuverschlüsselung des Klartextes einer Nachricht voraus. Würde die Bundesrechtsanwaltskammer demgegenüber einfach die verschlüsselte Nachricht für Empfänger A zusätzlich mit dem Schlüssel von Empfänger B verschlüsseln, könnte Empfänger B lediglich die für Empfänger A verschlüsselte Nachricht erhalten, nicht jedoch den Klartext, da hierfür der Schlüssel von Empfänger A fehlt. Entsprechend müsste die Bundesrechtsanwaltskammer zur Entschlüsselung der Nachricht entweder über den (privaten) Schlüssel von Empfänger A verfügen, oder das beA so gestalten, dass pauschal alle Nachrichten zusätzlich mit einem zweiten (öffentlichen) „Generalschlüssel" verschlüsselt werden, dessen privates Gegenstück die Bundesrechtsanwaltskammer unter ihrer Kontrolle hält.

Für eine abschließende Bewertung der Sicherheit der behaupteten Ende-zu-Ende-Verschlüsselung ist die Quellenlage allerdings nicht ausreichend. Es wäre in jedem Fall – gerade bei einem so sensiblen Thema wie der Vertraulichkeit anwaltlicher Kommunikation – wünschenswert, wenn eine transparentere Kommunikation des Bundesrechtsanwaltskammer über die technischen Spezifikationen des beA erfolgen würde. So gibt es mit der Informationsseite der BRAK zum beA[681] einen lobenswerten Ansatz, deren Inhalte allerdings bei genauer Betrachtung oft beklagenswert vage bleiben, was die konkrete Gestaltung des beA anbelangt. Insofern ist den Vorschlägen zu folgen, als vertrauensbildende Maßnahme und zur Qualitätssicherung ein Gremium mit Mitgliedern aus verschiedenen Vereinen, Körperschaften und Kanzleien zu bilden, das über die Umsetzung des besonderen elektronischen Anwaltspostfach wacht.[682]

678 *Bundesrechtsanwaltskammer*, Sichere Nachrichtenübermittlung.
679 *Bundesrechtsanwaltskammer*, beA-Verschlüsselungsverfahren.
680 *Hecksteden*, Ende-zu-Ende-Verschlüsselung.
681 Abrufbar unter http://bea.brak.de, zuletzt abgerufen am 18.12.2017.
682 *Volk/Burianski/Redeker/Schafhausen u. a.*, DAV-StN. Nr. 6/2016, 10.

7.3 Authentizitätsschutz

Zum Schutz der Authentizität der übermittelten Nachrichten bietet das EGVP die Möglichkeit, seine Nachrichten mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Gemäß dem Signaturgesetz war hierbei Voraussetzung, dass die Nutzer über getrennte Sicherungsmittel verfügen, die sie unter ihrer alleinigen Kontrolle halten können. Dieses Erfordernis wird nunmehr durch die eIDAS-Verordnung aufgeweicht, da Art. 3 Nr. 11 eIDAS-VO für fortgeschrittene und damit auch für qualifizierte elektronische Signaturen nur noch verlangt, dass der Unterzeichner die Signaturerstellungsdaten mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

Mit der Abkündigung des EGVP-Clients ändert sich die Gewichtung der qualifizierten elektronischen Signatur für das System EGVP. Denn an Stelle des EGVP-Clients treten auf Anwaltsseite das beA und für andere Interessenten das Web-EGVP. Für das besondere elektronische Anwaltspostfach wird entsprechend der Regelungen des ERV-Gesetzes keine elektronische Signatur mehr erforderlich sein. Auch das Web-EGVP wird, soweit erkennbar, keine besonderen Vorrichtungen für das Anbringen einer qualifizierten elektronischen Signatur durch den Einreicher mitbringen. Eine Gewährleistung der Authentizität durch die qualifizierte elektronische Signatur ist somit nicht sichergestellt.

Zwar wird beim beA das fakultative Anbringen von qualifizierten elektronischen Signaturen an den versandten Dateien technisch möglich bleiben, da für das beA keine Beschränkungen der übermittelbaren Dateitypen bis auf den Ausschluss ausführbarer Dateien aus Virenschutzgründen[683] vorgesehen sind. Die praktische Bedeutung dieser Möglichkeit dürfte jedoch mangels einer gesetzlichen Verpflichtung hierzu stark zurückgehen.

Das Anbringen einer qualifizierten elektronischen Signatur könnte jedoch durch die flankierenden Sicherheitsvorkehrungen des beA entbehrlich sein. Denn der dem EGVP und seiner konkreten Ausgestaltung beA zu Grunde liegende OSCI-Standard verlangt, dass die Nachrichten einschließlich ihrer Metadaten vom Client mit einer (fortgeschrittenen) elektronischen Signatur versehen werden.[684] Beim EGVP erfolgt die erste Signatur der gesamten Nachricht – unabhängig davon ob der Benutzer eine qualifizierte elektronische Signatur an den Inhaltsdaten anbringen möchte oder nicht – bereits beim Absenden der Nachricht durch den EGVP-Client. Fraglich ist, ob

683 So wird bei *Bundesrechtsanwaltskammer*, Nachrichtenerstellung und Versand darauf hingewiesen, dass es Einschränkungen nur Dateien mit Endungen, die eindeutig auf Schadsoftware schließen lassen, geben wird. Die Sinnhaftigkeit dieser Maßnahme darf indes getrost in Frage gestellt werden, vgl. hierzu unten unter 7.5.

684 *OSCI Leitstelle*, OSCI-Transport 1.2 Spezifikation, 19.

dies beim beA auch bereits clientseitig durch die Client Security (also den Teil der Software, die außerhalb des Webbrowsers auf dem Clientrechner läuft und die Sicherheitsfunktionen bereitstellt) geschieht, oder erst auf den Servern der BRAK innerhalb des Anwaltspostfachs. Sollte letzteres der Fall sein, bestünde eine größere Angriffsfläche, da die Nachricht auf dem Weg vom Webbrowser des Benutzerrechners zum beA verändert werden könnte.

Allerdings halten sich die faktischen Möglichkeiten der Veränderung in Grenzen, da die Inhaltsdaten der Nachricht bereits beim Verlassen des Clientrechners (also noch vor Eingang ins beA) verschlüsselt werden. Zu einer gezielten sinnvollen Manipulation der Nachricht wäre daher die Kenntnis des privaten Schlüssels des Nutzers erforderlich, da ohne diesen nur zufällige Änderungen an der Nachricht, die aber mit überwiegender Wahrscheinlichkeit die Lesbarkeit der Nachricht komplett zerstören würden, erfolgen könnten. Damit dürfte das vielversprechendste Mittel zur böswilligen Veränderung die Kompromittierung des Rechners des Benutzers sein, die zugleich aber praktisch auch alle anderen Sicherheitsmaßnahmen einschließlich einer qualifiziert elektronischen Signatur und einer Ende-zu-Ende-Verschlüsselung aushebeln könnte. So könnte beispielsweise theoretisch ein Angreifer, der Zugriff auf den Rechner, auf dem die Signatur stattfinden soll hat, dem Nutzer falsche Daten zur Unterschrift „unterschieben“, wenn dieser einen Signaturvorgang anstoßen will. Auch ist auf diesem Wege die Veränderung der zu signierenden Daten möglich, beispielsweise indem die zu signierenden Daten vor dem Erfolgen der Signatur heimlich ausgetauscht werden. Das Grundproblem, das solcherlei Angriffe ermöglicht, ist die Benutzung der qualifizierten elektronischen Signatur in einer potentiell unsicheren Umgebung wie nicht speziell abgesicherten PCs.[685]

Da dieser Aspekt jedoch ein grundsätzliches Problem von Sicherheitstechnologien, die in unsicheren Umgebungen eingesetzt werden können, ist, kann dies nicht gegen den Verzicht der qualifizierten elektronischen Signatur bei der Gestaltung des Postfachs sprechen. Die Sicherheit der Authentizität hängt beim besonderen elektronischen Anwaltspostfach vielmehr an der Verschlüsselung, die bei der Kommunikation zwischen dem Rechner des Nutzers und der Portalseite des beA oder – bei Verwendung einer Anwaltssoftware mit beA-Funktionalität – dem Intermediär verwendet wird. Durch die Gestaltung mittels einer SSL-gesicherten Verbindung sowie einer Inhaltsverschlüsselung in Verbindung mit einem Freischaltungsverfahren, das nur Rechtsanwälte berücksichtigen dürfte aber nach den hier aufgestellten Kriterien hinreichende Gewähr für einen wirksamen Auhentizätsschutz bestehen. Bei einem gesteigerten Bedürfnis nach Fälschungssicherheit kann zudem weiterhin eine qualifizierte elektronische Signatur (fakultativ)

685 Vgl. hierzu *Fox*, DuD 1999, 508, 510.

benutzt werden. Eine Auswertung der Signatur ist hierbei ohnehin lediglich im Streit- oder Schadensfall erforderlich, so dass hierdurch kein grundsätzlich größerer Aufwand für die Gerichte entsteht.

7.4 Konsistenz der Daten

Wie oben unter 5.1.3 besprochen, ist eine Voraussetzung für sicheren elektronischen Rechtsverkehr die Gewährleistung der Konsistenz der Daten. Im Rahmen dieser Betrachtung ist damit das Zusammenpassen von Inhalts- und Metadaten gemeint, um beispielsweise Täuschungen oder Irrtümer über die Identität der Kommunikationsteilnehmer oder über die Zeitpunkte, zu denen Kommunikationshandlungen erfolgten, zu vermeiden. Dabei kann die qualifizierte elektronische Signatur, die einem Dokument (oder mehreren Dokumenten in Form einer Containersignatur) anhaftet, diese Funktion nicht erfüllen, weil hiermit lediglich bestätigt wird, dass der Inhalt seit dem Signaturzeitpunkt unverändert ist (Integrität der Nachricht) und die Nachricht von dem Inhaber des Signaturschlüssels so signiert wurde (Authentizität der Nachricht). Die hierin noch nicht enthaltene Information ist jedoch, ob der tatsächliche Absender der Nachricht mit dem scheinbaren Absender der Nachricht identisch ist. Diese Frage kann eine (qualifizierte) elektronische Signatur der Inhaltsdaten nicht beantworten, da die entsprechenden Informationen in den Metadaten der Nachricht (analog zum Header einer E-Mail) enthalten sind.

Um die Konsistenz der übertragenen Daten zu gewährleisten, benutzt das EGVP verschiedene Technologien. So können vom EGVP-Client des Absenders versandte Nachrichten einschließlich der Metadaten für den Transport elektronisch signiert werden. Der empfangende Server (und jedes weitere System im EGVP-Verbund das die Nachricht empfängt) überprüft diese Signatur und erstellt über das Ergebnis der Signaturprüfung einen Vermerk auf dem sogenannten Laufzettel, der wiederum mit dem Signaturschlüssel des überprüfenden System (fortgeschritten) signiert wird.[686] Den Signaturen werden auch Zeitstempel beigefügt, die vom Intermediär stammen und somit eine Manipulation beispielsweise der Absende- oder Empfangszeitpunkte ausschließen sollen. Hiermit wird sichergestellt, dass Nutzer die Metadaten nicht unbemerkt verändern können. Selbst wenn ein bösgläubiger Nutzer Manipulationen an seinem EGVP-Client vornimmt, die ihm erlauben, Absendernamen und Absendezeitpunkt frei zu wählen, würde diese Manipulation bereits beim ersten Intermediär, bei dem die Nachricht eingeht, aufgedeckt werden. Denn bezüglich des

686 *OSCI Leitstelle*, OSCI-Transport 1.2 Spezifikation, 19.

Absendernamens würde der Intermediär eine Diskrepanz zu dem verwendeten EGVP-Account feststellen und protokollieren. Auch beim Versendezeitpunkt würde sich beim Intermediär eine Diskrepanz zeigen und protokolliert werden, wenn ein Auseinanderfallen von (angeblichem) Versendezeitpunkt und Zeitpunkt, zu dem der Intermediär die Nachricht erhält, vorläge, da diese Kommunikation praktisch ohne Verzögerung erfolgt. Dieses Verfahren ist als sicher zu betrachten, der Intermediär ist eine vertrauenswürdige Instanz für die Generierung von Zeitstempeln. Insbesondere kein Argument hiergegen ist es, dass lediglich fortgeschrittene elektronische Signaturen anstatt qualifizierter elektronischer Signaturen benutzt werden, da eine automatische Signatur durch den Intermediär mit einer qualifizierten elektronischen Signatur aufgrund der nötigen Personenbezogenheit rechtlich nicht zulässig wäre. Technisch kann eine fortgeschrittene elektronische Signatur aber einer qualifizierten elektronischen Signatur ebenbürtig sein, die gesteigerten Anforderungen an die qualifizierte elektronische Signatur werden bei der Verwendung nicht zur Ersetzung einer eigenhändigen Unterschrift sondern bei der technischen Beglaubigung eines automatischen Vorgangs gerade nicht benötigt.

Das besondere elektronische Anwaltspostfach verwendet grundsätzlich das gleiche Verfahren, da es auch die EGVP-Infrastruktur und -protokolle nutzt. Insofern kann auch bei diesem die Konsistenz der Daten als gesichert angenommen werden.

Das Sonderproblem von Medienbrüchen durch die Übertragung analoger Dokumente in digitale durch Scannen[687] stellt sich beim EGVP auch. Es ist allerdings kein dem System immanentes Problem, sondern tritt bei jedem Bedarf, analoge Daten in digitale zu übertragen, auf. Für anwaltliche Nutzer dürfte diese Problematik rein faktisch eine untergeordnete Bedeutung haben, da regelmäßig bereits wegen berufsrechtlicher Vorgaben Originaldokumente aufbewahrt werden bzw. wegen der eigentumsrechtlichen Zuordnung den Mandanten zurückgegeben werden müssen. Fehler beim Scannen durch veränderte oder fehlende Daten können so zwar auch auftreten, lassen sich jedoch regelmäßig durch eine korrekte Neudurchführung des Scanvorgangs heilen. Eine Beachtung technischer Richtlinien wie der TR-RESISCAN erscheint demnach für anwaltliche Nutzer des elektronischen Rechtsverkehrs als zwar nicht schädlich, aber auch als nicht unbedingt erforderlich. Um in den Genuss der Echtheitsvermutung gemäß § 437 ZPO auch für Scans zu kommen, muss der Scan ohnehin durch einen Träger der öffentlichen Gewalt erfolgen, § 371b ZPO, der im Zweifel selbst den Stand der Technik beachten wird. In der Regel dürfte dies durch Beachtung der Scanvorgang aus der TR-RESISCAN erfolgen.

687 Vgl. hierzu oben unter 5.1.4.

7.5 Interoperabilität

Für die Gewährleistung der im Rahmen dieser Betrachtung geforderten Interoperabilität bringt das EGVP bereits gute Voraussetzungen mit. Zum einen ist der EGVP-Client in der für verschiedenste Plattformen verfügbaren Programmiersprache Java geschrieben, so dass – theoretisch – eine Lauffähigkeit auf einer Vielzahl von Betriebssystemen mit geringem Aufwand realisierbar wäre. Tatsächlich war die Zusage, unter welchen Betriebssystemen der EGVP-Client lauffähig ist, jedoch beschränkt auf Windows sowie Linux, letzteres in Form nur der (allerdings im deutschsprachigen Raum recht verbreiteten) Distribution openSUSE. Bemerkenswert ist an dieser Gestaltung, dass damit mit MacOS ein Betriebssystem nicht unterstützt wird, das aufgrund seiner größeren Verbreitung eigentlich noch vor Linux als Zielsystem in Frage käme.[688]

Das besondere elektronische Anwaltspostfach hingegen verfolgt einen anderen Ansatz: Statt einer Software, die auf dem Computer des Nutzers läuft und auf eine Kompatibilität mit diesem angewiesen ist, nutzt das beA ein Webinterface, das im Grundsatz nur einen kompatiblen Webbrowser auf dem Rechner des Nutzers benötigt. Dies wird jedoch wieder eingeschränkt durch das Erfordernis, eine Softwarekomponente (als Client Security bezeichnet) auf dem lokalen Rechner zu installieren, die die Ver- und Entschlüsselung von Nachrichten durchführt.[689] Die Client Security benutzt wie bereits das EGVP Java als Programmiersprache, wodurch aller Wahrscheinlichkeit nach die (relative) Plattformunabhängigkeit der Software gesichert werden soll. Die Benutzung einer vom Browser entkoppelten Software für die sicherheitskritischsten Funktionen erscheint konsequent, da man nur in einem geschlossenen System die Sicherheit der hierin erfolgenden Vorgänge gewährleisten kann. Die Verschlüsselung im Webbrowser selbst anzubieten, dürfte sich zum einen aufgrund der vielen verschiedenen Produkte auf dem Markt, zum anderen aufgrund der hierin immer wieder enthaltenen Sicherheitslücken nicht als realistische Alternative angeboten haben. Die Kapselung der Sicherheitsfunktionen in einer Software und die Bündelung mit einer hierfür getesteten Java-Version ist insofern aus sicherheitstechnischer Sicht zu begrüßen.

Auch die Kompatibilität hat sich trotz dieser Gestaltung im Vergleich zum EGVP verbessert. Im Gegensatz zum EGVP wird für das beA eine Lauffähigkeit auch auf MacOS in Aussicht gestellt, so dass die zum EGVP diesbezüglich geäußerte Kritik hierauf keine Anwendung findet.

688 Nach Angaben der Firma Netmarketshare, die Statistiken über Systeme, die das World Wide Web nutzen sammelt, hatte Linux im September 2016 einen globalen Marktanteil von 2,23 %, MacOS X 10.11 hingegen mit 4,07 % einen beinahe doppelt so großen Anteil (https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=212&qpnp=1&qptimeframe=M, zuletzt abgerufen am 18.12.2017).

689 *Bundesrechtsanwaltskammer*, Erstregistrierung.

Bezüglich der unterstützten Dateiformate ist die Gestaltung des beA selbst zurückhaltend, für die zulässigen Formate wird auf die entsprechenden Rechtsverordnungen der Länder verwiesen.[690] Als Sicherheitsfunktion des beA wird jedoch genannt, dass bestimmte „Dateiendungen […], die eindeutig auf eine Schadsoftware hinweisen“,[691] von der Übertragung durch das beA ausgenommen werden sollen. Dies ist aus mehreren Gründen fragwürdig. Denn zum einen gibt es keine Dateiendungen, die *eindeutig* auf Schadsoftware schließen lassen – die Tarnung als nützliche Dateien liegt gerade in der Natur der meisten Schadsoftware. So verwenden die meisten Schadprogramme unmittelbar vom Betriebssystem ausführbare Dateiendungen wie *.exe*, *.com* oder *.scr*, die unter Windows-Betriebssystemen beliebigen ausführbaren Code enthalten können.[692] Gleichzeitig können natürlich diese Dateiendungen ebenso harmlose und nützliche Programme enthalten, ein Anwendungsfall für .exe-Dateien ist für den E-Mail-Versand beispielsweise das Versenden selbstextrahierender Archive, bei denen der Empfänger keine spezielle Software zum Entpacken benötigt. Zudem kann die Endung von Dateien „verschleiert“ werden, indem diese beispielsweise mit einem Archivprogramm in ein gepacktes Format (beispielsweise .zip oder .rar) umgewandelt werden. Auch dieses Vorgehen ist sowohl bei Nutzsoftware als auch bei Schadsoftware anzutreffen, eine insofern nötige Mitwirkungshandlung des Opfers bei Schadsoftware kann zumindest bei unbedarften Benutzern durchaus erwartet werden[693] und dürfte die Verbreitung von Schadsoftware nicht in relevanter Weise eingeschränkt haben. Zweitens kann Schadsoftware unabhängig von der Dateiendung in verschiedensten Dokumenten enthalten sein, solange diese aktive Komponenten enthalten. Dies betrifft beispielsweise auch Makros in Office-Dateien (beispielsweise Word-Dokumente oder Excel-Tabellen), mit denen bei Ausführung durch den Nutzer entweder selbst ein Schadenseffekt hervorgerufen wird oder – wie beispielsweise bei einer gezielt auf Unternehmen gerichteten Schadsoftwarekampagne im Dezember 2016 – durch das Makro Schadsoftware von einem Server nachgeladen und auf dem Rechner des Ziels ausgeführt wird.[694] Dem Ansatz, Dateien nach der Dateiendung herauszufiltern, ist jedoch zuzugeben, dass er aufgrund der verwendeten Verschlüsselung der einzig praktikable Ansatz sein dürfte, um überhaupt die Gefahr durch Schadsoftware zu reduzieren. Wenngleich die Effektivität in Frage steht, dürfte dieser Ansatz andererseits auch zu keinen relevanten Nachteilen für den Nutzer führen. Ein Ansatz

690 *Bundesrechtsanwaltskammer*, Nachrichtenerstellung und Versand; gemeint sein dürfte hier die Rechtsverordnung nach § 130a Abs. 2 ZPO n.F. sein, die die Bundesregierung mit Zustimmung des Bundesrates erlassen darf.
691 *Bundesrechtsanwaltskammer*, Nachrichtenerstellung und Versand.
692 Dies spiegelt auch die größere Verbreitung von Windows-Betriebssystemen auf dem Markt wieder, da die allermeiste Schadsoftware „in freier Wildbahn“ für eben diese Betriebssysteme geschrieben ist.
693 Sehr verbreitet sind beispielsweise .zip-Dateien mit aufmerksamkeitserregenden Dateinamen wie *Rechnung-[Datum].zip*, die freilich in der Regel Schadsoftware enthalten, die bei Ausführung der entpackten Datei durch den Nutzer ihre Wirkung entfalten kann; vgl. zu dieser Problematik *Verbraucherzentrale.de*, Trojaner.
694 *Scherschel*, Goldeneye.

wie bei De-Mail, die Nachrichten auf Servern des Providers zu entschlüsseln und auf Schadsoftware zu untersuchen, wäre zwar bei der Bekämpfung dieser (etwas) effektiver, jedoch wurde dieser Ansatz verschiedentlich aus Gründen des Datenschutzes und der Datensicherheit kritisiert.[695]

7.6 Verfügbarkeit

Eine Schwachstelle des EGVP-Systems in der bisherigen Umsetzung war die Verfügbarkeit. So gab es immer wieder Ausfälle des Systems, die zum Teil geplant (durch Wartungen, Updates etc.), zum Teil aber auch ungeplant waren.[696] Wenngleich die bisherigen Ausfälle für die betroffenen Nutzer sicherlich ärgerlich waren, dürften sie jedoch mangels Nutzungsverpflichtung und der insgesamt überschaubaren Anzahl von EGVP-Nutzern bisher nur verhältnismäßig geringe Auswirkungen gehabt haben. Etwas anderes wird jedoch für die verpflichtende Nutzung gelten, bei der Ausfälle potentiell alle Anwälte betreffen, die im Ausfallzeitraum Schriftsätze einreichen wollen bzw. müssen. Die Bundesrechtsanwaltskammer hat für das beA angekündigt, mehrere über das Land verteilte Hochleistungsserver zu benutzen, um die Zuverlässigkeit des Systems zu gewährleisten.[697] Hierbei ist aber zu berücksichtigen, dass diese Aussage schon der Kompetenzverteilung beim elektronischen Rechtsverkehr nach nur das besondere elektronische Anwaltspostfach als einen Teil der EGVP-Kommunikationsinfrastruktur betreffen kann. Gerade für Ausfälle im Bereich der Gerichte kann die Bundesrechtsanwaltskammer keine Aussage treffen, da sie auf diese keinen Einfluss hat. Somit ist über die Aussagen zur Zuverlässigkeit des beA hinaus erforderlich, dass auch die Gerichte ihre Infrastruktur entsprechend aufstocken und auf den elektronischen Rechtsverkehr und das hierdurch erzeugte Datenaufkommen vorbereiten. Für Ausfälle indes bietet das ERV-Gesetz mit Regelungen wie in § 130d S. 2 ZPO n.F. eine juristische Lösung für Systemausfälle in Form einer Rückfallmöglichkeit auf die Einreichung „nach den allgemeinen Vorschriften“, worunter hier die Einreichung auf dem Postweg bzw. per Telefax verstanden wird, die nach § 130d S. 3 ZPO n.F. glaubhaft gemacht werden muss.[698] Nach der Gesetzesbegründung soll diese Vorschrift auch dann Anwendung finden, wenn die Störung in der Sphäre des Rechtsanwalts liegt.[699] Dies ist zu begrüßen, da es damit die möglichen negativen Auswirkungen durch den zwingenden

695 Vgl. hierzu oben unter 2.3.5.
696 Vgl. hierzu beispielsweise die Kritik von *Vossius*, DNotV-StN. vom 29.2.2012, 8; aktuelle Meldungen zum EGVP, über die auch geplante oder ungeplante Systemausfälle kommuniziert werden, finden sich unter http://www.egvp.de/meldungen/index.php, zuletzt abgerufen am 18.12.2017.
697 *Bundesrechtsanwaltskammer*, Zuverlässigkeit.
698 BT-Drs. 17/12634, 27.
699 BT-Drs. 17/12634, 27.

elektronischen Rechtsverkehr für manche Nutzer zusätzlich abfedert und einen Interessenausgleich zwischen Justiz und Anwaltschaft bzw. den Rechtssuchenden schafft.

Ein Problem, was hierdurch nicht abgefangen wird, ist jedoch die Verfügbarkeit von ausreichend dimensionierten Internetverbindungen.[700] Da das ERV-Gesetz für alle Anwälte, ungeachtet ihrer technischen Ausrüstung und der Internetverfügbarkeit am Kanzleiort gilt, könnten hierdurch besondere Härten für einige Anwälte entstehen. Für gerade im ländlichen Bereich bisher immer noch verbreitete unterdimensionierte Internetanschlüsse kann sowohl dem EGVP als auch dem beA zu Gute gehalten werden, dass diese eine Größenbeschränkung von (derzeit) 30 MB pro Datei vorsehen.[701] Dieses Limit kann jedoch seinerseits wieder Probleme verursachen, weil durchaus Konstellationen, in denen größere Dateien (beispielsweise großformatige Scans von Bauzeichnungen, CAD/CAM-Designs[702], hochauflösende Fotos, Videoaufnahmen von Überwachungskameras und dergleichen) übertragen werden müssen. Gravierender noch sind Fälle, in denen gar keine nutzbare Internetverbindung verfügbar ist. Eine nur vorübergehende Unmöglichkeit im Sinne des § 130d S. 2 ZPO n.F. wird hier nicht anzunehmen sein, da eine strukturell fehlende Internetanbindung regelmäßig ein langfristiges Problem ist, dem im Extremfall allenfalls durch eine Verlegung des Kanzleistandortes oder kostenintensive Investitionen wie beispielsweise in eine Satelliteninternet-Anbindung abzuhelfen ist. Interessengerecht wäre es hier, auch für solche Fälle eine Ausnahmeregelung gesetzlich festzuschreiben. Es ist schlicht nicht ersichtlich, weshalb ein Anwalt der nur vorübergehend den elektronischen Rechtsverkehr nicht nutzen kann, gegenüber einem Anwalt, der dies strukturell bedingt nicht vermag, bevorteilt werden soll. Für die Justiz ergäbe sich hierdurch auch kein großer Mehraufwand, wenn man davon ausgeht, dass zum Startzeitpunkt des beA nur noch eine äußerst geringe Anzahl von Nutzern betroffen sein dürften, und da Vorkehrungen zur analogen Kommunikation per Briefpost oder Telefax ohnehin aufrecht erhalten werden müssen. Dem steht das Risiko gegenüber, dass einzelne Betroffene auf dem Klagewege versuchen könnten, gegen die Verpflichtung zur Nutzung des elektronischen Rechtsverkehrs vorzugehen.

Ein weiteres Verfügbarkeitsproblem wurde zudem im Rahmen der ursprünglich ab 1. Januar 2018 geplanten passiven Nutzungspflicht des beA offenbar. Durch die außerplanmäßige Abschaltung des beA[703] war es faktisch seit dem 22. Dezember 2017 nicht mehr möglich, Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis zu nehmen. Um aufgrund dieser Diskrepanz

700 Siehe zu dieser Problematik bereits oben unter 5.4.2.
701 Zum beA hierzu *Bundesrechtsanwaltskammer*, Technische Fragen, Frage 4.
702 CAD (Computer Aided Design) und CAM (Computer Aided Manufacturing) bezeichnen Technologien zum computergestützten Gestalten und Fertigen von Objekten.
703 Vgl. hierzu auch oben unter 7.2.1.

zwischen rechtlicher Verpflichtung und tatsächlicher Möglichkeit Rechtssicherheit zu erlangen, hatte der Berliner Anwalt Janne Andreas Jacoby am 6. Januar 2018 eine Klage auf einstweiligen Rechtsschutz beim Berliner Anwaltsgerichtshof erhoben, die jedoch mit Beschluss vom 6. August 2018 als unzulässig zurückgewiesen wurde.[704] Der Anwaltsgerichtshof führte in seinem Beschlussaus, dem Antragsteller fehle bereits das erforderliche Rechtsschutzbedürfnis, da bereits ein Fall der Unmöglichkeit vorliege.[705] Die Entscheidung wurde unter anderem vom Antragsteller selbst dahingehend kritisiert, dass auch gegen einen offensichtlich rechtswidrigen Verwaltungsakt oder nichtigen Verwaltungsakt ein Rechtsschutzbedürfnis bestehe; andererseits begrüße er jedoch die durch den Beschluss eingetretene Rechtssicherheit.[706]

In der Tat zeigt dieser Geschehensablauf sehr plastisch, welche Probleme im Rahmen mit der Nutzungsverpflichtung entstehen können. Zwar lässt sich regelmäßig über Gesetzesauslegen und rechtliche Konstruktionen wie Unmöglichkeit am Ende zu einer sach- und interessengerechten Lösung kommen. Allerdings ist durch die – im konkreten Fall auch mit sieben Monaten für ein Verfahren im einstweiligen Rechtsschutz auch nicht geringe – Verfahrensdauer eine Phase der Rechtsunsicherheit gegeben, die geeignet ist Nutzer eines ohnehin neuen und kritisch betrachteten Systems weiter zu verunsichern. Dies stützt ebenfalls die These, dass für einen Erfolg des elektronischen Rechtsverkehrs mit den Gerichten eine transparente und schnelle (Krisen-)Kommunikation mit den Nutzern unabdingbar ist.

7.7 Kosten

Wie bereits oben unter Kapitel 5.5 herausgearbeitet können die Kosten für ein Verfahren mit Anschluss- und Benutzungszwang wie den elektronischen Rechtsverkehr im Hinblick auf die Berufsfreiheit gemäß Art. 12 GG relevant werden, woran allerdings strenge Anforderungen zu stellen sind. Für das EGVP in der Form vor Inkrafttreten des ERV-Gesetzes spielt dies keine Rolle, da die Benutzung freiwillig ist. Von einem mittelbaren Benutzungszwang wird man ebenfalls nicht ausgehen können, da ein Grund für den Erlass des ERV-Gesetzes gerade die beklagte geringe Nutzung des elektronischen Rechtsverkehrs war. Zudem wird der EGVP-Client kostenlos angeboten. Mittelbare Kosten entstehen hier jedoch durch das Erfordernis einer Signaturkarte mit entsprechenden Zertifikaten (die kostenpflichtig beantragt werden müssen und nur eine limitierte Laufzeit haben) sowie einer Signaturgesetzkonformen Signatureinheit.

704 *Lorenz*, beA-Nutzungspflicht.
705 AGH Berlin, Beschluss vom 6. August 2018, II AGH 2/18.
706 *Lorenz*, beA-Nutzungspflicht

Mit dem Inkrafttreten der Verpflichtung zum elektronischen Rechtsverkehr und dem besonderen elektronischen Anwaltspostfach ändert sich diese Lage zumindest für professionelle Einreicher. So wird der kostenlose EGVP-Client aufgrund der Abkündigung nicht mehr verfügbar sein, an seine Stelle tritt mit dem Web-EGVP ein allein an nicht-professionelle Einreicher gerichtetes kostenfreies Angebot, das jedoch nur Nachrichten senden, nicht jedoch solche empfangen können wird.[707] Für das besondere elektronische Anwaltspostfach wird pauschal von jedem in Deutschland zugelassenen Rechtsanwalt von der Bundesrechtsanwaltskammer eine Gebühr eingezogen, die voraussichtlich 65 bis 70 Euro pro Jahr betragen wird.[708] Gegen die Gebührenpflicht wurde bereits von mindestens einem Anwalt Klage erhoben, der damit gegen die (erste) Gebühr in Höhe von 63 Euro vorgehen wollte, die von der für ihn zuständigen Rechtsanwaltskammer Hamm erhoben wurde.[709] Der Bundesgerichtshof in Anwaltssachen hat die Berufung gegen ein abweisendes Urteil des Anwaltsgerichtshofs Hamm mit der Begründung zurückgewiesen, dass der Bescheid rechtmäßig ergangen sei, da insbesondere die Finanzierung des besonderen elektronischen Anwaltspostfachs eine Aufgabe sei, die den Rechtsanwaltskammern durch das ERV-Gesetz zugewiesen worden sei.[710] Auch eine Verletzung von Art. 12 GG sei nicht gegeben, da das Ziel der Förderung des elektronischen Rechtsverkehrs vernünftige Gründe des Allgemeinwohls darstelle, die eine Beschränkung der Berufsausübung zu rechtfertigen geeignet seien.[711] Schließlich stünden den Kosten auch anwaltsseitig langfristig Einsparungen gegenüber, zumal die Anwaltschaft die Kosten nicht allein trage, sondern auch die Justiz erhebliche Investitionen tätigen müsse.[712]

Dieser Einschätzung des Bundesgerichtshofs in Anwaltssachen ist beizupflichten. Wenngleich auch ein Abstellen auf die geringe Höhe des Beitrags eine ungerechtfertigten Eingriff in den Schutzbereich von Art. 12 GG schon fernliegend erscheinen lässt,[713] dürfte es jedenfalls für die Akzeptanz des elektronischen Rechtsverkehrs förderlich sein, auf alle geäußerten Bedenken des Klägers einzugehen. Insofern beweist das Urteil durchaus Augenmaß.

Auch bezüglich der mittelbaren Kosten für den elektronischen Rechtsverkehr lassen sich die Argumente für die Umlage teilweise nutzbar machen. So dürften die meisten Kanzleien bereits mit einer wie auch immer gearteten IT-Infrastruktur ausgestattet sein. Durch den Wegfall des Erfordernisses der qualifizierten elektronischen Signatur ist eine Investition in Signaturkarte mit Zertifikaten und Signaturerstellungseinheit nicht mehr zwingend erforderlich, gleichwohl kann eine

707 Sieh dazu oben unter 6.2.2.
708 *Bundesrechtsanwaltskammer*, Was kostet das beA?
709 *Deutscher Anwaltverein*, Digitale Anwaltschaft News vom 17.2.2016.
710 BGH, Urteil vom 11. Januar 2016, Az. AnwZ (Brfg) 33/15 = openJur 2016, 319, Rn. 15 f.
711 BGH, Urteil vom 11. Januar 2016, Az. AnwZ (Brfg) 33/15 = openJur 2016, 319, Rn. 18.
712 BGH, Urteil vom 11. Januar 2016, Az. AnwZ (Brfg) 33/15 = openJur 2016, 319, Rn. 19.
713 Vgl. hierzu oben unter 5.5.

solche natürlich (weiterhin) benutzt werden, wodurch etwaige frühere Investitionen hierin nicht als verloren betrachtet werden sollten. Auch steht den (anwaltlichen) Nutzern frei, andere Einreichungswege als das besondere elektronische Anwaltspostfach zu nutzen, wodurch aber gegebenenfalls ebenfalls Kosten entstehen können, beispielsweise in Form von Übermittlungsentgelten für De-Mail-Nachrichten.

7.8 Ergonomie

Ein beim EGVP-Client zuweilen beklagter Missstand war die mangelnde Benutzerfreundlichkeit.[714] Teilweise wurde der Justiz vorgeworfen, sich generell zu wenig um die Nutzerfreundlichkeit des elektronischen Rechtsverkehrs zu sorgen und die Interessen der Nutzer außerhalb der Justiz außen vor zu lassen.[715] Für den EGVP-Client ist dieser Befund durchaus nachvollziehbar – die Benutzeroberfläche soll zwar Mailprogrammen nachgebildet sein, wirkt aber überfrachtet und präsentiert dem Nutzer zum Teil für ihn irrelevante Informationen. Ein Teil der mangelnden optischen Attraktivität mag hierbei der Benutzung von Java für das Frontend geschuldet sein, da sich in Java geschriebene Programme als Kehrseite ihrer Plattformunabhängigkeit mit den vorgefertigten Designelementen oft nur schlecht in das Oberflächendesign des verwendeten Betriebssystems einfügen. Auch eine Barrierefreiheit des EGVP-Clients ist zumindest für blinde oder sehbehinderte Benutzer nicht gegeben.[716] Die Bund-Länder-Kommission hat sich allerdings im Rahmen eines Themenpapiers zum Thema Barrierefreiheit in der Justiz verpflichtet, eine barrierefreie Gestaltung des EGVP zu erreichen.[717] Im Hinblick auf die Abkündigung des EGVP-Clients ist allerdings anzunehmen, dass die Umsetzung dieser Zielvorgabe mit neuen Produkten wie dem Web-EGVP für Bürger erreicht werden soll.

Für das beA ist insofern zu begrüßen, dass durch den durch das ERV-Gesetz eingefügten § 191a Abs. 1 GVG ein Anspruch auf barrierefreie Einreichung und barrierefreien Zugang zu Dokumenten für blinde oder sehbehinderte Personen ermöglicht wird. Für das beA bestimmt § 31a Abs. 1 S. 2 BRAO, dass dieses barrierefrei ausgestaltet sein soll. Die Bundesrechtsanwaltskammer hat diese Vorgaben umgesetzt, indem sie das Unternehmen, das mit der technischen Realisierung des beA beauftragt wurde, verpflichtet hat, im Selbsttest nach der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV 2.0) ein Ergebnis von

714 So z.B. *Hoffmann/Borchers*, CR 2014, 62, 66.
715 *Bundesrechtsanwaltskammer*, Vorschläge ERV, 1 f.
716 *Boysen*, DVBS-Sachverständigenstellungnahme vom 12. April 2013 Abschnit III. 1.
717 *Bund-Länder-Kommission für Informationstechnik in der Justiz*, Barrierefreiheit, 11.

mindestens 90 Punkten (gut zugänglich) für das beA zu erreichen.[718] Diese Gewährleistung kann allerdings natürlich nur für die Weboberfläche des beA gelten, nicht jedoch für Drittprodukte, die dieses nutzen. Mangels einer Verpflichtung zur Nutzung der Software eines Drittanbieters und der Kostenfreiheit der Webinterface-Benutzung (über die Umlage hinaus, die jeder Anwalt ungeachtet seiner Nutzung des beA zu zahlen hat), dürfte hierin jedoch kein juristisches, sondern allenfalls ein marktwirtschaftliches Problem liegen. Insofern ist die Barrierefreiheit des beA uneingeschränkt zu begrüßen. Gleichwohl befreit das nicht von dem Erfordernis an die Bundesrechtsanwaltskammer, auch Rückmeldungen von Nutzern einzuholen und diese für die weitere Ausgestaltung des Produktes zu berücksichtigen.

Auch die Benutzerfreundlichkeit des beA für Anwender ohne Behinderung scheint im Vergleich zum EGVP-Client deutlich zugenommen zu haben. Ausweislich der von der Bundesrechtsanwaltskammer zur Verfügung gestellten Screenshots[719] verfügt das beA über eine aufgeräumt wirkende Benutzeroberfläche mit einer klaren Formensprache und einer freundlichen Gestaltung. Die Anzahl der Bedienelemente ist gegenüber dem EGVP-Client ebenfalls deutlich reduziert worden. Der unbestreitbare Vorteil des beA ist in dieser Hinsicht, dass durch die eingeschränkte Zielgruppe (zugelassene Rechtsanwälte) eine kompromisslos auf deren Bedürfnisse zugeschnittene Benutzerführung realisierbar ist. Die tatsächliche Benutzerfreundlichkeit kann indes nur im Produktivbetrieb von anwaltlichen Nutzern beurteilt werden. Auch insofern ist der Bundesrechtsanwaltskammer anzuraten, frühzeitig und regelmäßig Feedback von den Nutzern einzuholen, um eine möglichst praxisgerechte Gestaltung zu erreichen.

7.9 Haftungsrisiken

Eine große Sorge vieler Anwälte im Zusammenhang mit der Einführung des verpflichtenden elektronischen Rechtsverkehrs waren hierdurch entstehende neue Haftungsrisiken. Insbesondere wurde hierbei auf mögliche Fristversäumnisse durch den elektronischen Rechtsverkehr abgestellt, die zu Haftungskonstellationen führen können.[720] In der Tat gab es bereits in der Zeit vor Erlass des ERV-Gesetzes Fälle, in denen die (freiwillige) Benutzung des elektronischen Rechtsverkehrs in Form des EGVP zu Haftungsfällen führte. Ein besonders öffentlichkeitswirksamer Fall war durch ein Fristversäumnis entstanden, weil ein Bundesland trotz vorhandenem EGVP-Postfach des

718 *Bundesrechtsanwaltskammer*, Das Postfach, Infokasten „Das beA ist barrierefrei“.
719 *Bundesrechtsanwaltskammer*, Screenshots.
720 *Redeker/Conrad/Härting/Huppertz u. a.*, DAV-Stellungnahme 64/2012, 5 f.

angeschriebenen Gerichts den elektronischen Rechtsverkehr zum Zeitpunkt der Einreichung einer Berufungsbegründung durch einen Anwalt (noch) nicht eröffnet hatte.[721] Ein Teil der Öffentlichkeitswirksamkeit dieses Falles rührte auch daher, dass die resultierende Schadenssumme fast 70 Millionen Euro betrug. In der Literatur wurde dieser Fall ausführlich besprochen und als Argument dafür gesehen, dass dringend eine einheitliche, für den anwaltlichen Nutzer transparente Eröffnung des elektronischen Rechtsverkehrs erfolgen müsse.[722] Das Haftungsrisiko aufgrund des beklagten „Flickenteppichs", also der uneinheitlichen Akzeptanz von elektronischen Einreichungen im Bundesgebiet, sollte sich indes durch das ERV-Gesetz drastisch reduziert haben. Aufgrund der Regelungen im ERV-Gesetz ist nunmehr klargestellt, dass eine fakultative Nutzung des ERV mit den neuen Einreichungswegen pro Bundesland frühestens zum 1.1.2018 und eine verpflichtende Nutzung frühestens ab dem 1.1.2020 möglich ist.[723] Allerdings bleibt bei dieser Gestaltung das Problem der unterschiedlichen Umsetzung in den Ländern bestehen. Nutzern ist deshalb anzuraten, die Umsetzung in den Bundesländern, mit deren Gerichten sie elektronisch kommunizieren wollen, vorab zu prüfen und gegebenenfalls vorsichtshalber auf die althergebrachten Einreichungswege auszuweichen, zumindest solange der verpflichtende elektronische Rechtsverkehr im jeweiligen Bundesland noch nicht eröffnet ist.

Für vorübergehende technische Ausfälle der ERV-Infrastruktur sieht das ERV-Gesetz in den jeweiligen prozessualen Regelungen (z.B. § 130d S. 2 ZPO n.F.) die Möglichkeit vor, auf die bisher zulässigen Einreichungswege wie Post oder Telefax auszuweichen.[724] Dies dürfte aufgrund der Weite der Vorschrift auch das Haftungsrisiko für derartige Konstellationen stark begrenzen, zumal auch Störungen in der Spähre des anwaltlichen Nutzers erfasst werden. Problematisch könnten in diesem Zusammenhang jedoch zu spät bemerkte Störungen sein, da in diesen Fällen eventuell nicht mehr genug Zeit für eine Ersatzeinreichung per Post oder – in Extremfällen – auch nur per Telefax bliebe. Faktisch kann dies auf eine Verkürzung der Frist hinauslaufen, da Anwälte so sicherheitshalber elektronische Einreichungen nicht unter völliger Ausschöpfung der Fristen vornehmen, sondern einen gewissen Zeitpuffer für gegebenenfalls notwendige Ersatzeinreichungen vorsehen sollten. Dies entspricht jedoch der bereits für das Telefax etablierten Rechtsprechung, die den Verschuldensmaßstab bei einer Fristversäumung danach beurteilt, wie knapp an die Frist herangearbeitet wurde.[725] Es wird insofern abzuwarten bleiben, als wie zuverlässig sich die einzelnen Einreichungswege in der Praxis herausstellen. Auch hier ist im Eigeninteresse der Justiz

721 OLG Düsseldorf, Urteil vom 24. Juli 2013, Az. VI-U (Kart) 48/12 = openJur 2013, 32422.
722 *Sandkühler*, KammerMitteilungen Rechtsanwaltskammer Düsseldorf 1/2014, 45 f.
723 Vgl. oben unter 3.1.7
724 Vgl. hierzu oben unter 7.6.
725 *Greger* in *Zöller*, § 233 ZPO Rn. 23, Stichwort „Telefax".; vgl. hierzu bereits oben unter 5.7.1.

daran, dass sich die bisherigen Aufwendungen für den elektronischen Rechtsverkehr amortisieren, darauf hinzuarbeiten, eine möglichst hohe Zuverlässigkeit der Einreichungen via EGVP und beA anzustreben, um Nutzer nicht auf andere Einreichungswege abzudrängen.

Schließlich wurde kurz nach Wiedereinführung der passiven Nutzungspflicht des beA eine neue Problematik bekannt, die Auswirkungen auf die anwaltliche Haftung haben könnte. So ist es zum Zeitpunkt der letzten Überarbeitung dieser Arbeit nach wie vor möglich, über die Berechtigungsseite innerhalb des beA-Interfaces zu erkennen, welche Anwälte ihr beA bereits initialisiert haben und somit überhaupt in der Lage sind, gegen sie erfolgte Zustellungen zur Kenntnis zu nehmen.[726] Dies hat für die anwaltlichen Nutzer zwei sehr konkrete potentielle Folgen: Zum einen begeht ein Nutzer, der das beA nicht spätestens zum 3. September 2018 in Betrieb genommen hat, einen Verstoß gegen in § 31a Abs. 6 BRAO festgelegte berufsrechtliche passive Nutzungspflicht. Diese kann gemäß § 113 BRAO durch anwaltsgerichtliche Maßnahmen geahndet werden. Zum anderen öffnet dieser Nutzer sich für Angriffe der Gegenseite, indem diese die mangelnde Fähigkeit, Zustellungen zur Kenntnis zu nehmen, durch eine rechtlich ebenfalls seit dem 3. September 2018 mögliche Zustellung vom Anwalt zum Anwalt über das beA ausnutzt. Hierdurch könnte beispielsweise ein Fristablauf in Gang gesetzt werden, in der Hoffnung, dass die Gegenseite mangels Kenntnisnahme die Frist versäumt. Einige sehen sogar eine berufsrechtliche Pflicht, diese Versäumnis der Gegenseite auszunutzen.[727] Hieran bestehen jedoch erhebliche Zweifel, da die Pflicht zur Kollegialität ebenfalls Teil des anwaltlichen Berufsrechts ist. Nach § 25 BORA ist der Anwalt gehalten, Kollegen vertraulich auf Berufspflichtverstöße hinzuweisen, es sei denn, die Interessen des Mandanten oder eigene Interessen erfordern eine Reaktion in anderer Weise. Die Vorschrift dient insbesondere auch dem Schutz des Vertrauens in die Anwaltschaft, da offene Hinweise auf mögliche Berufspflichtverletzungen nicht nur das Vertrauensverhältnis zwischen gegnerischem Anwalt und dessen Mandanten untergraben könnte, sondern auch das Vertrauensverhältnis zwischen dem so handelnden Anwalt und seinem Mandanten.[728] Dem gegenüber steht zwar eine zivilrechtliche Pflicht aus dem Mandatsvertrag, den Mandanten bestmöglich zu vertreten, diese ist jedoch nicht per se berufsrechtlich sanktionierbar.[729] Für eventuelle Schadensersatzansprüche, die aus einem nicht erfolgten Ausnutzen dieser beA-Schwachstelle gegenüber der Gegenseite resultieren, wird beim Verschuldensmaßstab auch die Pflicht zur anwaltlichen Kollegialität sowie die Neuheit des beA insgesamt berücksichtigt werden müssen. Im Ergebnis ist deshalb eine berufsrechtliche Pflicht zur Ausnutzung der unterbliebenen

726 Vgl. zu diesem Problem bereits *Lorenz*, beA-Anmeldung.
727 *Lorenz*, beA-Anmeldung
728 *Brüggemann* in *Feuerich*/*Weyland*, § 25 BORA Rn. 1.
729 *Träger* in *Feuerich*/*Weyland*, § 43 BRAO Rn. 23.

Anmeldung eines gegnerischen Anwalts an das beA – jedenfalls sofern diese Information über die entsprechende Funktion des beA erlangt wurde – abzulehnen. Nach der hier vertretenen Ansicht wäre ein Ausnutzen der durch das beA erzeugten Unsicherheit und der bei manchen sicherlich auch bestehenden Nutzungsunsicherheit zwar nicht unzulässig, eine Pflicht hierzu kann berufsrechtlich jedoch nicht hergeleitet werden.

8 Fazit und Ausblick

Der elektronische Rechtsverkehr ist ein Thema, was insbesondere in der Anwaltschaft viele – zum Teil auch sehr emotionale – Reaktionen hervorgerufen hat. Das Spektrum reicht dabei von völliger Ablehnung zu offener Begeisterung. Im Folgenden soll ein Fazit aus der vorangegangenen Betrachtung zum elektronischen Gerichts- und Verwaltungspostfach gezogen und Ratschläge für eine künftige Weiterentwicklung gegeben werden. Dabei werden drei Themenblöcke, die als Fazit dieser Arbeit stehen sollen, voneinander unterschieden.

8.1 Elektronischer Rechtsverkehr als unvermeidbare Modernisierung

Unsere heutige Zeit ist geprägt von rapidem technischen Fortschritt, dem das Recht allzu oft nur nachzueilen scheint. Juristen werden zuweilen als Bremser des Fortschritts betrachtet, da die Möglichkeiten, die neue Technologien und Medien uns eröffnen (das tatsächliche „können“) zuweilen durch rechtliche Vorgaben (das rechtliche „dürfen“) beschränkt werden. Dass diese Diskrepanz nicht zwingend etwas Negatives sein muss, weil das Recht als Korrektiv für die ansonsten drohende Umsetzung alles Machbaren in einer blinden Technikgläubigkeit dienen kann und muss, wird dabei zuweilen vergessen. Einen gewissen Anteil hat die Rechtswissenschaft, die oft in Traditionen verhaftet scheint und von manchen deswegen als strukturell fortschrittsfeindlich wahrgenommen wird, sicherlich auch selbst. Umso wichtiger ist es, sich technischen Neuerungen nicht völlig zu verschließen, sondern diese in einem vernünftigen Rahmen nutzbar zu machen. Die Abwägung zwischen Fortschritt und Bewahrung etablierter Prinzipien kann dabei niemals schematisch erfolgen, sondern muss stets mit Augenmaß auf den Einzelfall getätigt werden. Ein Sichverschließen vor jeglicher Digitalisierung wäre angesichts der Durchdringung der Gesellschaft von modernen Technologien verfehlt. Eine Justiz, die noch auf verstaubte Akten auf Papier setzt

und sich schwer tut mit der Einordnung neuer Kommunikationsmittel, droht schnell vom Bürger, der beruflich und privat modernste Informationstechnik nutzt und dessen Leben immer mehr von der internetgestützten Kommunikation bestimmt wird, nicht mehr ernst genommen zu werden. Auch die Kosten, die durch eine redundante Vorratshaltung von Papierakten entstehen, werden angesichts langer Verfahrensdauern und unterbesetzter Gerichte schwerer vermittelbar. Und auch für die Anwälte, die immer öfter über eine moderne IT-Ausstattung in ihren Kanzleien verfügen, drohen die Gerichte technisch völlig abzuhängen. Andererseits darf auch nicht der Fehler begangen werden, in blinde Technikgläubigkeit zu verfallen und – mitgerissen von den Verlockungen der modernen IT-Welt – nicht auf jene mahnenden Stimmen zu hören, die vor Gefahren neuer Techniken warnen.

Die Einführung des elektronischen Rechtsverkehrs war eine unvermeidbare Entwicklung, die eine konsequente Weiterentwicklung aus Technologien und Phänomenen darstellt, die sich über einen langen Zeitraum entwickelt haben. Für die Gestaltung des elektronischen Rechtsverkehrs jedoch gab und gibt es viele Möglichkeiten. Die gewählte Gestaltung sollte im Idealfall einen Ausgleich schaffen zwischen Modernität und Stabilität. Dies zu erreichen, ist nicht nur Aufgabe des Gesetzgebers, sondern auch der Justiz und der (anwaltlichen) Anwender.

8.2 Elektronischer Rechtsverkehr als Gesellschaftsaufgabe

Da eine Entscheidung des Gesetzgebers für den elektronischen Rechtsverkehr eine logische Folge der bisherigen technischen Entwicklung ist, stellt sich in erster Linie die Frage nach dessen konkreter Ausgestaltung. Der Zugang zum Recht ist ein elementarer Grundwert unserer Gesellschaft, der auch im Grundgesetz verankert ist. Ohne ihn kann eine freiheitliche, demokratische Gesellschaft nicht funktionieren. Die Art des Zugangs darf deswegen nicht Einzelnen überlassen werden, sondern sie muss als Sachverhalt, der potentiell alle betrifft auch unter Berücksichtigung aller Stimmen gestaltet werden. Das Gesetz zur Förderung des elektronischen Rechtsverkehrs ist bereits insoweit einzigartig, als sowohl verschiedene Bundesländer als auch die Bundesregierung verschiedene Gesetzesentwürfe zur Diskussion gestellt haben. Im Gesetzgebungsverfahren haben sich die verschiedensten Interessengruppen beteiligt. Herausgekommen ist ein Gesetz, das viele – wenn auch nicht alle – Kritikpunkte beherzigt und im Großen und Ganzen einen sinnvollen Ausgangspunkt für eine modernere Justiz schafft. Die Gestaltung, die ein Nebeneinander verschiedener Einreichungswege erlaubt, ist ein Beispiel für

diesen offenen Ansatz. Auch Kritikpunkten wie dem automatischen elektronische Empfangsbekenntnis und den fehlenden Absicherungen für den Fall von Systemausfällen wurde abgeholfen. Mit dem Bekenntnis zur Barrierefreiheit der Verfahren für den elektronischen Rechtsverkehr wurde zudem ein wichtiger weiterer Schritt hin zu einer Teilhabe möglichst vieler Personen am Rechtsverkehr geschaffen.

Zum Anschluss- und Benutzungszwang für professionelle Einreicher, der mitunter am stärksten polarisierte und seitens der Anwaltschaft überwiegend ablehnend gesehen wurde, ist eine differenzierende Sicht geboten. Zwar ist das Argument, dass ein gut funktionierender und tatsächlich Ersparnisse bringender elektronischer Rechtsverkehr schon genug Nutzer überzeugen werde, gut nachvollziehbar. Andererseits handelt es sich hier um ein typisches Henne-Ei-Problem, da ein so komplexes System auch immer auf die Rückmeldungen seiner Benutzer angewiesen ist. Erkennt man an, dass der elektronische Rechtsverkehr grundsätzlich wünschenswert ist, wie auch die meisten Kritiker das tun, so muss man wohl auch gemeinsam Investitionen in diesen tätigen. Denn es wäre wohl im Sinne keines Nutzers, den elektronischen Rechtsverkehr scheitern zu sehen, womöglich mit der Folge, dass durch diesen Schlag über Jahre keine neuen Vorstöße in dieser Richtung mehr gewagt werden würden.

Aufgrund der Neuheit des elektronischen Rechtsverkehrs darf sich jedoch niemand auf dessen Einführung ausruhen. Vieles ist – auch prinzipbedingt – noch ungeklärt. Es müssen nun Erfahrungen mit dem elektronischen Rechtsverkehr gesammelt werden, bei denen abermals in erster Linie die Benutzer gefragt sind, die am stärksten vom elektronischen Rechtsverkehr betroffen sind.

8.3 Evaluierung des elektronischen Rechtsverkehrs

Wie bei jeder neuen Technologie ist auch beim elektronischen Rechtsverkehr noch nicht abschließend absehbar, welche langfristigen Folgen er haben wird. Insbesondere aufgrund des Nebeneinanders verschiedener Einreichungswege wurde eine Konkurrenzsituation bezüglich der besten Technik für den elektronischen Rechtsverkehr geschaffen. Welches Verfahren sich am Ende durchsetzen wird, oder ob gar alle in gleichem Umfang nebeneinander bestehen bleiben werden, wird die Zeit zeigen. Das besondere elektronische Anwaltspostfach genießt in dieser Konstellation allerdings einen erheblichen Vorteil, da die Kosten hierfür ohnehin von jedem Anwalt eingezogen werden, selbst wenn dieser einen anderen Einreichungsweg nutzt. Durch die enge Bindung an die Anwaltschaft ist wohl zu erwarten, dass sich das besondere elektronische Anwaltspostfach gegen

Konkurrenzsysteme wie De-Mail durchsetzen wird. Dies wird auch bekräftigt durch die von manchen Kritikern geäußerten Datenschutzbedenken ob der nicht durchgehenden Verschlüsselung bei De-Mail. Dieser Vorteil des beA könnte allerdings dahinschmelzen, wenn nicht durch die Bundesrechtsanwaltskammer noch stärker transparent gemacht wird, wie die Ende-zu-Ende-Verschlüsselung konkret umgesetzt ist und in welchem Verhältnis sie zur Umverschlüsselung der Postfächer für die Benutzung durch freigegebene Dritte steht. Auch das Sicherheitskonzept insgesamt wird sich in der Zukunft im täglichen Betrieb beweisen müssen, ebenso wie die Zuverlässigkeit der technischen Infrastruktur. Die Rechtsprechung wird sich überdies mit einer Fülle neuer Fragestellungen betreffend den elektronischen Rechtsverkehr konfrontiert sehen. Insbesondere Fragen betreffend die Authentizität und Integrität elektronisch versandter Nachrichten müssen ob des Verzichts auf eine zwingende qualifizierte elektronische Signatur beantwortet werden, wenngleich die Anwaltschaft bei dieser Frage eine eigene Steuerungsmöglichkeit durch freiwilliges Anbringen einer entsprechenden Signatur hat. Die Lösung dieser Fragestellungen wird einen maßgeblichen Einfluss auf die Akzeptanz und damit den Erfolg der einzelnen Systeme für den ERV haben.

Um diesen Unwägbarkeiten und möglichen Entwicklungen zu begegnen, ist zu empfehlen, die weitere Entwicklung des elektronischen Rechtsverkehrs genau zu beobachten und bei eventuellen Fehlentwicklungen schnell einzugreifen. Eine Beteiligung verschiedener betroffener Gruppen hierbei – beispielsweise in Form eines Evaluationsgremiums – ist nicht nur wünschenswert, sondern für den Erfolg des elektronischen Rechtsverkehrs unerlässlich. Hierzu gehört auch ein transparentes Vorgehen, das in der Vergangenheit bei Problemen mit dem beA bedauerlicherweise nicht immer gegeben war. Für einen erfolgreichen elektronischen Rechtsverkehr mit den Gerichten ist es aber unerlässlich, wenn die Beteiligten – allen voran die Bundesrechtsanwaltskammer – aus vergangenen Kritikpunkten lernen und eine offene Fehlerkultur etablieren.

ISBN 978-3-7376-0712-4