MICHAEL KNOPP / DANIEL WILKE / GERRIT HORNUNG / PHILIP LAUE

Grunddienste für die Rechtssicherheit elektronischer Kommunikation

Rechtlicher Bedarf für eine gewährleistete Sicherheit

Elektronische Kommunikation hat für den Rechtsverkehr zunehmend an Bedeutung gewonnen. Doch nach wie vor bestehen große Unsicherheiten und Missbrauchsrisiken, die eine weitgehende Gleichstellung mit analogen Medien verhindern. Aus diesem Grund werden rechtlich anerkannte und leicht verfügbare Diensteangebote zur Herstellung einer ausreichenden Sicherheit benötigt. Der folgende Beitrag soll hierzu den Bedarf und auch rechtliche Verpflichtungen darstellen, vorhandene Ansätze aufzeigen und kurz auf europarechtliche Probleme einer diesbezüglichen Regulierung hinweisen.

I. Risiken des elektronischen Rechts- und Geschäftsverkehrs

Der elektronische Rechts- und Geschäftsverkehr ist mit zahlreichen Risiken behaftet, die bislang nur über umständliche Verfahren oder auch gar nicht beseitigt werden können. Vielfach ist für die Kommunikationspartner ungewiss, ob Rechte oder Ansprüche, die durch elektronische Kommunikation erworben werden, durchsetzbar sein werden. Die Gründe liegen im Wesentlichen in den Schwierigkeiten, sich über elektronische Kommunikationsvorgänge der Identität oder bestimmter Eigenschaften des Kommunikationspartners zu versichern und Inhalte oder Kontexte der elektronischen Kommunikation einem sicheren Beweis zugänglich zu machen.[1] Darüber hinaus ist die Gewährleistung der Vertraulichkeit der Kommunikation eine Schwäche elektronischer Kommunikation, die die Abwicklung bestimmter Teile des Rechtsverkehrs über dieses Medium ohne weitere Sicherheitsmaßnahmen eigent-

1) So bereits *Hammer/Schneider*, in: Hammer, Sicherungsinfrastrukturen, 1995; zu den spezifischen Risiken des Internet und der Rolle der Technikgestaltung *Roßnagel*, in: Klumpp/Kubicek/Roßnagel, next generation information society, 2003, S. 423, 425 f., 428 ff.

■ Michael Knopp, Daniel Wilke, LL.M. und Dr. Gerrit Hornung, LL.M. sind wissenschaftliche Mitarbeiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel; Philip Laue, LL.M. ist Rechtsanwalt in der Kanzlei Graf von Westphalen in Köln. Als Mitarbeiter der Projektgruppe haben sie an der „Studie Rechtsfragen" des E-Government 2.0 Projekts „Bürgerportale" mitgewirkt.

lich ausschließt.[2] Hiervon betroffen sind viele Beratungsdienste von Berufsgruppen, die Geheimhaltungs- oder Schweigepflichten unterliegen. Technische Lösungsmöglichkeiten existieren für die meisten dieser Schwierigkeiten in allen Sicherheitsgraden und Varianten, doch selbst solche mit bestehendem Rechtsrahmen wie etwa qualifizierte elektronische Signaturen setzen sich nur mühsam durch. In der Regel nimmt die Praxis die Gefahren hin, solange ihre Verwirklichung in einem wirtschaftlich erträglichen Ausmaß und das Risiko kalkulierbar bleibt. Im Schadensfall ist ein Schadensersatz häufig schwer zu erlangen[3] und nicht alle Schäden, etwa solche durch bekannt gewordene vertrauliche Inhalte, lassen sich finanziell ausgleichen. Doch mit der immer weiter steigenden Bedeutung des Mediums steigen auch die Risiken durch immer ausgefeiltere Missbrauchsstrategien und erweisen sich als Hindernisse für die weitere Entwicklung.[4] Es entsteht ein Bedarf an IT-Grunddiensten, die Risiken sicher ausschließen, rechtliche Sicherheit vermitteln und für den Nutzer leicht zu bedienen sind, ohne dass er sich mit der Problematik näher auseinandersetzen muss.

II. Grunddienste sicherer elektronischer Kommunikation

Aus den größten und folgenschwersten Risiken ergeben sich schnell die gesuchten Grunddienste, die für einen sicheren Rechts- und Geschäftsverkehr benötigt werden. Für die Sicherung von Integrität und Authentizität elektronisch übermittelter Erklärungen steht mit qualifizierten elektronischen Signaturen bereits eine solche Grunddienstinfrastruktur bereit.[5] Ein weiteres Bedürfnis besteht in dem Nachweis der Identität und Authentizität im Verlauf eines Kommunikationsvorgangs, nicht zuletzt auch bezogen auf den Empfänger. Erfolgt die Kommunikation – i.S.d. Datenschutzes positiv zu bewerten – pseudonym, besteht der Bedarf nach einem einerseits restriktiven, andererseits aber auch faktisch durchführbaren Aufdeckungsverfahren und einem durchsetzbaren Aufdeckungsanspruch.[6] Ohne diese ist kein Anspruch durchsetzbar, da der Anspruchsgegner sonst nicht ermittelt oder bezeichnet werden kann. Neben der Identität spielen häufig auch bestimmte Eigenschaften eine Rolle, deren Zutreffen sicher nachgewiesen sein muss. Dies betrifft z.B. Altersangaben, um Minderjährige zum einen zu schützen und zum anderen die Gültigkeit von Verträgen zu sichern. Gerade für die Anbieter jugendschutzrelevanter Dienste besteht ein permanentes Risiko, wegen unzureichender Verifikationsverfahren etwa nach § 184c StGB oder § 23 JMStV strafrechtlich belangt oder wettbewerbsrechtlich abgemahnt zu werden.[7] Doch auch der Nachweis anderer Berechtigungen, wie etwa Vertretungsberechtigungen oder Qualifikationsnachweise sind häufig Voraussetzungen für einen risikofreien Vertragsschluss. Eine Infrastruktur zur Sicherung der Vertraulichkeit ist ein weiterer notwendiger Grunddienst, gerade für die Geheimhaltungs- oder Schweigepflichten unterliegenden Berufsgruppen.

Die Beweisschwierigkeiten im Zusammenhang mit elektronischen Medien reduzieren sich nicht auf den Integritätsnachweis elektronischer Dokumente. Der elektronische Zugang bedarf ebenso einer nicht auf die Mitwirkung des Empfängers angewiesenen Beweismöglichkeit. Gerade für den elektronischen Geschäftsverkehr ist es zudem oft von Bedeutung, nicht nur die einzelnen Erklärungen im Verlauf eines Vertragsschlusses nachzuweisen, sondern auch die Geschäftsgrundlage oder den Kontext der Erklärungen. Ein wichtiges Beispiel ist die Beschaffenheit einer Informations- oder Angebotsseite sowie der Benutzerführung eines Teledienstes zu einem bestimmten Zeitpunkt. Zu ermöglichen ist also der Nachweis des kompletten Ablaufs eines elektronischen Kommunikationsvorgangs. Zuletzt ist ein weiterer Grunddienst zur Erhaltung der Beweiskraft der elektronischen Beweismittel erforderlich, der diese sicher aufbewahrt und zuverlässig konserviert.[8] Zusammengefasst ergeben sich folgende Grunddienste:

- Vertraulichkeitssicherung,
- Authentizitäts- und Integritätssicherung,
- Authentifizierung der Kommunikationsteilnehmer und Nachweis bestimmter Eigenschaften,
- sichere Nachweismöglichkeit des gesamten Kommunikationsvorgangs für alle Beteiligten,
- Nachweismöglichkeiten für den Zugang,
- pseudonyme Kommunikationsdienste und ein interessengerechtes Aufdeckungsverfahren,
- Aufbewahrung elektronischer Nachweise.

Ein weiterer Grunddienst besteht in der Sicherung gegen den Missbrauch der bei der elektronischen Kommunikation entstehenden Daten. Für die Wahrung von Datenschutzzielen und -vorschriften existieren bereits Gütesiegel.[9] Auf dieses Themenfeld soll hier jedoch nicht eingegangen werden, um den Rahmen dieser Darstellung nicht zu sprengen.

III. Rechtlich begründeter Bedarf und Ansätze einer garantierten Sicherheit

Das Angebot entsprechender Dienste ist zunächst kein technisches Problem, sieht man von den Schwierigkeiten mit der Interoperabilität verschiedener proprietärer Lösungen ab. Vielfach existieren sogar entsprechende Angebote. Für Nutzer und Anbieter ist jedoch deren rechtliche Bewertung, also die Geeignetheit zur Erfüllung rechtlicher Anforderungen, ungewiss. Der Nutzen der vorhandenen Angebote wird hierdurch stark gemindert. An der Entwicklung sicherer Dienste und ihres Rechtsrahmens wird jedoch geforscht und es existieren verschiedene Ansätze zur Umsetzung. Ein wichtiger Ansatz liegt z.B. in dem Bürgerportalprojekt des Bundes.[10]

1. Vertraulichkeit

Die Vertraulichkeit der Kommunikation ist grundsätzlich durch Art. 10 GG geschützt und ein allgemeines Bedürf-

2) Am Beispiel E-Mail *Eckert*, IT-Sicherheit, 4. Aufl. 2006, S. 135.
3) Hierzu etwa *Spindler*, MMR 2008, 7, 9.
4) Zu den Vertrauensverlusten und zur sicherheitsbedingten Zurückhaltung von Nutzern *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz, Informationelles Vertrauen für die Informationsgesellschaft, 2008, S. 17, 18 ff.
5) Zu den Grundlagen *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*), s. unter: http://www.bsi.de/esig/index.htm.
6) Für pseudonyme Signaturzertifikate *Roßnagel*, NJW 2001, 1817, 1821.
7) Zu den Anforderungen an die Altersverifikation s. auch *BGH* MMR 2008, 400 m. Anm. *Liesching* und *Waldenberger* – „über 18.de"; *Niedersächsisches OVG* JMS-Report 1/2008, 8 ff.
8) Zum Problem und zu den Möglichkeiten der Beweiserhaltung s. *Fischer-Dieskau*, Das elektronisch signierte Dokument als Mittel zur Beweissicherung, 2006, S. 144 ff.; *Roßnagel/Fischer-Dieskau/Jandt/Knopp*, Langfristige Aufbewahrung elektronischer Dokumente, 2007, S. 28; *Horst/Pordesch/Gondrom/Brandner*, in: Roßnagel/Schmücker (Hrsg.), Beweiskräftige elektronische Archivierung, 2006, S. 37 ff.
9) S. hierzu aber unter: https://www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm.
10) Das Bürgerportalprojekt ist Teil der High-Tech-Strategie und des E-Government-Programms 2.0 des Bundes; *Stach*, DuD 2008, 184; *dies.*, in: Zechner, Handbuch E-Government, 2007, S. 155; weitere Informationen unter: http://www.buergerportale.de.

nis. Gerade in Bezug auf das meistgenutzte elektronische Kommunikationsmittel, die E-Mail, ist sie jedoch derzeit faktisch kaum gesichert. Die elektronischen Postfächer der meisten Anbieter sind lediglich passwortgeschützt. Der Einblick auf dem Übermittlungsweg ist zwar aufwendig, aber auch durch Dritte möglich. Zusätzlich besteht für Mitarbeiter der Provider, der Betreiber von Routern und Administratoren nicht selten ein relativ leichter Zugriff.[11] Bestimmte Kommunikationsvorgänge erfordern jedoch einen besonderen Schutz der Vertraulichkeit durch mindestens einen der Kommunikationspartner. Die Berufsgruppe der Anwälte wird z.B. durch § 43a Abs. 2 Satz 1 BRAO zur Verschwiegenheit verpflichtet.[12] Für den Umgang mit fremden Gesundheitsdaten durch Krankenkassen und Ärzte verpflichten § 9 BDSG und die jeweiligen Berufsordnungen zu Maßnahmen, die Vertraulichkeit der Kommunikation solcher Daten zu schützen. Ebenso erfordert die Wahrung des Sozialgeheimnisses nach § 35 SGB I und § 78a SGB X einschließlich Nr. 4 des Anhangs zu § 78a SGB X Maßnahmen zum Vertraulichkeitsschutz. Wollen diese Berufsgruppen oder andere zum Schutz Verpflichtete vertrauliche Inhalte elektronisch kommunizieren, so bedürfen sie der Rechtssicherheit darüber, ob die gewählten Schutzmechanismen ausreichen, ihre gesetzliche Verpflichtung zu erfüllen. Außerdem dürfen die verwendeten Schutzmaßnahmen nicht den Empfänger vor Probleme stellen.

Die Gewährleistung von Vertraulichkeit bei der E-Mail-Kommunikation ist ein wesentlicher Baustein des Bürgerportalprojekts. Zu den Anforderungen, die private Diensteanbieter erfüllen müssen, um ihre Dienste als Bürgerportale bezeichnen zu dürfen, gehört die Verschlüsselung der Nachrichten bei der Übertragung und die Möglichkeit des Absenders, dem Empfänger den Abruf der Nachricht nur nach einer sicheren Authentifizierung zu gestatten. Eine Ende-zu-Ende-Verschlüsselung durch den Nutzer, die auch der Anbieter nicht aufheben kann, ist ebenfalls möglich, wird aber nicht durch die Bürgerportale selbst angeboten.

2. Dauerhaft beweisbare Integrität und Authentizität von elektronischen Erklärungen

Bei herkömmlich auf elektronischem Weg geschlossenen Rechtsgeschäften ist es beinahe schon eine typische Eigenschaft, dass hierbei entstandene Ansprüche mangels Beweisbarkeit nicht durchgesetzt werden können. Zur Abwehr eines solchen Anspruchs muss der Anspruchsgegner lediglich substanziiert darlegen, dass die maßgeblichen Erklärungen nicht durch ihn oder nicht mit dem behaupteten Inhalt abgegeben wurden.[13] Einen Anscheinsbeweis bei lediglich durch Nutzernamen und Passwort geschützten Authentifizierungsmechanismen oder ungesicherten elektronischen Dokumenten hat die Rechtsprechung zu Recht abgelehnt.[14] Besonders bei Geschäften, die individualisierte Vorleistungen erfordern, z.B. Maß- oder Sonderanfertigungen, entsteht durch diese faktische Durchbrechung des Grundsatzes „pacta sunt servanda" ein hohes Risiko für den Geschäftspartner, der auf die Wirksamkeit des Vertrags vertraut. Weitere Beispiele sind Geschäfte, deren termin- und absprachegerechte Erfüllung entscheidend ist, etwa Fixgeschäfte. Solange keine Dienste zur Verfügung stehen, die den Beweis des Vertragsschlusses zuverlässig ermöglichen, lässt sich dieses Problem nur durch Medienbrüche, Vorleistungen über Treuhänder oder die Vermeidung einer bestimmten Risikohöhe lösen. Für den elektronischen Rechtsverkehr wirkt dies als Hemmnis.

Erfolgt der Vertragsschluss durch den Austausch eigenständiger Willenserklärungen in Form elektronischer Dokumente, steht in Form qualifizierter elektronischer Signaturen ein Sicherungsmittel zur Verfügung, das alle Anforderungen ohne weiteres erfüllt. Der Beweiswert der Erklärungen ist in diesem Fall sogar durch eine gesetzliche Beweisregel festgelegt (§ 371a ZPO)[15] und die Anforderungen an qualifizierte elektronische Signaturen sowie die Aufsicht über deren Einhaltung sind ausführlich durch das Signaturgesetz samt zugehöriger Verordnung und deren Anhang bestimmt. Bei den zahlreichen Rechtsgeschäften, die unter Nutzung von Auktionsportalen oder Online-Bestelldiensten stattfinden, erfolgen Angebot und Annahme jedoch innerhalb fester Prozesse per Mausklick und ohne Signatureinsatz, sodass hierbei für mehr Rechtssicherheit andere Lösungen erforderlich sind.[16]

3. Nachweis über Geschäftsvorgänge

Am Anfang steht hier eine sichere Authentifizierung, die mindestens auf Besitz und Wissen aufbaut. Um eine dauerhafte Beweisbarkeit und nicht nur eine momentane Sicherheit zu erhalten, kann dieser Anmeldevorgang durch einen vertrauenswürdigen dritten Diensteanbieter in einem zertifizierten Prozess aufgezeichnet und durch den Einsatz qualifizierter Signaturen mit Zeitstempeln gesichert werden. Vor allem bei elektronisch abgewickelten Fernabsatzgeschäften ist für die Durchsetzbarkeit der jeweils erworbenen oder die Abwehr unberechtigter Ansprüche oftmals jedoch nicht nur das Vorliegen und die Nachweisbarkeit zweier übereinstimmender Willenserklärungen entscheidend, sondern auch die Gestaltung des Geschäftsablaufs und des elektronischen Angebots. Aus § 312e BGB und der BGB-InfoV ergeben sich Gestaltungsanforderungen und Informationspflichten, deren Erfüllung oder Nichterfüllung Einfluss auf die Anspruchsdurchsetzung haben kann.[17] Aus diesem Grund ist es wichtig für den jeweiligen Beweisbelasteten, auch diese Umstände zum Zeitpunkt des Geschäftsabschlusses sicher nachweisen zu können. Hierzu bestehen bislang noch keine Initiativen, die eine beweissichernde Speicherung ermöglichen. Um wirksam zu sein, wird für diesen Zweck eine den Ablauf dokumentierende dritte Instanz benötigt.

Ein Ansatz zu einem solchen Diensteangebot wurde i.R.d. Trustcaps-Projekts aus technischer und rechtlicher Sicht

---

11) *Lindloff*, E-Mail-Kommunikation von Rechtsanwälten mit Mandanten und Gerichten, 2005, S. 63 ff.; *Krempl*, c't 26/2004, 100, 101; informativ auch der IT-Grundschutz-Katalog des *BSI*, s. unter: http://www.bsi.bund.de/gshb/deutsch/g/g02087.htm und http://www.bsi.bund.de/gshb/deutsch/g/g05077.htm; zum rechtlichen Schutz der E-Mail auch in Bezug auf Arbeitgeber *Härting*, CR 2007, 311.

12) Zur Schweigepflicht *Hartung*, Anwaltliche Berufsordnung, 3. Aufl. 2006, BRAO § 43a Rdnr. 21 ff., BerufsO § 2 Rdnr. 38; diese umfasst auch Sorgfaltspflichten zur Wahrung der Vertraulichkeit in der Kommunikation, die durch ungesicherte E-Mail-Kommunikation verletzt werden können; *Miedbrodt*, in: Roßnagel, Hdb. des Datenschutzrechts, 2003, Kap. 4.9 Rdnr. 40 m.w.Nw.; a.A. *Härting*, MDR 2001, 61; *ders.*, NJW 2005, 1248; *Axmann/Degen*, NJW 2006, 1457, 1458 unter Berufung auf den Wortlaut und das traditionelle Verständnis von § 43a BRAO; technisch umfassend, aber Handlungspflichten ablehnend *Lindloff* (o. Fußn. 11), S. 105 ff.

13) *LG Münster* BeckRS 2007 04441; *OLG Köln* MMR 2006, 321; *LG Köln* BeckRS 2006 07259; s. auch *Sosnitza*, VuR 2007, 143, 145.

14) *OLG Köln* MMR 2002, 813; *LG Magdeburg* CR 2005, 466, 467; *LG Bonn* MMR 2004, 179.

15) S. näher *Roßnagel/Fischer-Dieskau*, NJW 2006, 806 ff.

16) Bisher erfolgt hier lediglich eine Protokollierung.

17) Die Verletzung dieser Pflichten kann zur Verlängerung der Widerrufsfrist führen oder einen Schadensersatzanspruch auslösen, der mit dem Primäranspruch aufgerechnet werden kann, *Grüneberg*, in: Palandt, 65. Aufl. 2006, § 312e Rdnr. 11.

untersucht und entwickelt.[18] Die Vertrauenswürdigkeit und Verlässlichkeit eines solchen Dienstes ergibt sich für den Nutzer aber erst dann, wenn die Anerkennung der Beweissicherung durch diese dritte Instanz seitens der Rechtsprechung vorab als sicher gelten kann. Auch hier wäre eine Akkreditierung ein denkbares Mittel.

4. Sichere Bestätigung persönlicher Eigenschaften

Bei der sicheren Bestätigung persönlicher Eigenschaften kommt es dagegen häufig nicht auf die dauerhafte Nachweisbarkeit der erfolgten Bestätigung an, sondern lediglich auf die Sicherheit der Bestätigung im Zeitpunkt ihrer Erzeugung. Ein Beispiel ist die Altersverifikation im Bereich des Jugendschutzes.[19] Die o.g. Risiken der Anbieter bei Verwendung eines nicht ausreichenden Verifikationssystems begründen den Bedarf nach rechtlich anerkannten und sicheren Diensten.[20] Für die Altersverifikation steht beispielsweise die EC-Geldkarte zur Verfügung.[21] Es besteht zwar kein Anerkennungsverfahren, die *Kommission für Jugendmedienschutz* (*KJM*) erkennt jedoch nach Altersstufen differenzierende Jugendschutzprogramme für Telemedien nach § 11 JMStV an und beurteilt vorgelegte Verifikationssysteme.[22] Der neue elektronische Personalausweis wird eine pseudonyme Altersverifikation ermöglichen.[23] Die Notwendigkeit zur Bestätigung persönlicher Eigenschaften erschöpft sich jedoch nicht in der Altersverifikation. Auch Vertretungsbefugnisse, Gruppenzugehörigkeiten und der Familienstand sind Beispiele für mögliche relevante Eigenschaften. Entscheidend ist auch hier die Verlässlichkeit der Überprüfung der Eigenschaft durch die bestätigende Instanz. So können bestimmte Eigenschaften i.R.e. qualifizierten elektronischen Signatur über Attributszertifikate nachgewiesen werden (§§ 5 Abs. 2, 7 Abs. 2 SigG). Für bestimmte persönliche Eigenschaften, wie etwa auch das Alter, kann eine authentisierende Bestätigung auch über eine signierte Information eines Bürgerportal-Diensteanbieters erfolgen. Die Sicherheit ersterer Möglichkeit ergibt sich aus den gesetzlichen Regelungen, im zweiten Fall resultiert die Verlässlichkeit aus der erfolgten Akkreditierung.

5. Rechtssicherer elektronischer Zugang

Ein weiteres Problem stellt sich, wenn eine Rechtsposition vom Nachweis des (rechtzeitigen) Zugangs abhängig ist, etwa bei Widerrufserklärungen nach §§ 312d Abs. 1, 355 BGB oder Kündigungen. Sofern der Empfänger den Zugang nicht freiwillig und beweisbar bestätigt, besteht für die elektronische Kommunikation bislang keine Möglichkeit, einen beweissicheren Zugang zu bewirken.[24] Hierzu kann nur auf analoge Medien ausgewichen werden.[25] Daran ändern auch die Neuerungen in den Prozessordnungen nichts, die die elektronische Zustellung ermöglichen.[26] Diese sehen lediglich die Zustellung gegen eine freiwillige Empfangsbestätigung des Adressaten vor und weisen zudem teilweise einen beschränkten Empfängerkreis auf.

In der Einführung eines Dienstes, innerhalb dessen der Provider des Empfängers den Zugang bestätigt, und der Ermächtigung dieser Anbieter, auch förmliche Zustellungen elektronisch vorzunehmen, liegt ein weiterer Eckstein der Bürgerportale. Letzteres soll über eine entsprechende gesetzliche Verankerung und die Beleihung der Bürgerportalanbieter ermöglicht werden. Der Diensteanbieter des Empfängers soll auf Anfrage eine qualifiziert signierte Erklärung darüber erteilen, dass die Nachricht in das elektronische Postfach des Empfängers eingelegt worden ist. Ein solches Zustellungsverfahren oder Verfahren zur Zugangsbewirkung bietet sogar Vorteile gegenüber den meisten analogen, denn in die Erklärung über die Zugangsbewirkung wird der Hashwert der zugestellten Erklärung eingebunden, sodass auch der Nachweis über den Inhalt der zugegangenen Erklärung geführt werden kann. Hierfür ist nicht einmal die Kenntnisnahme des Inhalts durch Dritte erforderlich.

6. Pseudonymer Geschäftsverkehr

Das Angebot der Verwendung von Pseudonymen beim Geschäftsschluss ist eine grundsätzlich zu begrüßende Möglichkeit des elektronischen Geschäftsverkehrs. Vor allem für den Vorleistenden besteht hierbei jedoch auch ein beträchtliches Risiko, denn um seine Ansprüche anschließend im Streitfall durchsetzen zu können, benötigt er die wahre Identität und die Anschrift des Vertragspartners. Bislang besteht jedoch bei den meisten pseudonym angebotenen Diensten kein interessengerechter Auskunftsanspruch gegen den Anbieter und für diesen auch keine Prüfpflicht hinsichtlich der tatsächlichen Identität des Nutzers. Für die E-Mail-Kommunikation über Bürgerportaladressen könnte dieser Anspruch jedoch i.R.d. Bürgerportalregulierung eingeführt werden. Erforderlich ist ein Ausgleich der Interessen, also einerseits eine weitgehende Sicherung und Wahrung der Pseudonymität und andererseits die sichere Aussicht des Kommunikationspartners, im Streitfall das Pseudonym aufdecken zu können. Der Aufdeckungsanspruch muss daher an bestimmte Bedingungen, etwa das Glaubhaftmachen eines durchzusetzenden Anspruchs und das Nichtvorliegen offensichtlichen Rechtsmissbrauchs sowie an eine ausreichende Prüfung dieser Voraussetzungen geknüpft und restriktiv gehandhabt werden, um die Funktion der Pseudonyme nicht zu gefährden. Zu berücksichtigen ist aber auch, dass die Anbieter pseudonymer Dienste nur begrenzt mit einer Anspruchsprüfung belastet werden können.

7. Beweissichere Aufbewahrung

Der Bedarf nach Angeboten zur Gewährleistung einer beweissicheren Aufbewahrung elektronischer Dokumente ist die logische Konsequenz einer vermehrten Nutzung elektronischer Medien für die Abwicklung von Rechtsgeschäften. Verträge, Erklärungen, Bestätigungen werden häufiger elektronisch entstehen. Genau wie Papierdokumente sollten diese, um einen fortdauernden Nachweis zu ermöglichen, aufbewahrt werden. Für einen Teil dieser Dokumente existieren sogar gesetzliche Aufbewahrungspflichten, wie etwa für elektronische Rechnungen in § 14b UStG oder hinsichtlich der Buchführung in den §§ 238 ff. HGB und §§ 140 ff. AO.[27] Bei bedeutsamen Rechtsgeschäften ist von der Verwendung qualifizierter elektronischer Signaturen auszugehen, zumal unsignierte elektro-

---

18) *Kumbruck/Sacher/Stumpf*, DuD 2007, 362, 366.

19) *Erdemir*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 4 JMStV Rdnr. 53 ff., 60.

20) Zu den Anforderungen *Niedersächsisches OVG* K&R 2008, 123.

21) Informationen hierzu unter: http://www.geldkarte-jugendschutz.de.

22) S. zu den beurteilten Diensten und den Grundlagen unter: http://www.kjm-online.de.

23) Näher *Roßnagel/Hornung/Schnabel*, DuD 2008, 168, 169

24) *Makoski*, K&R 2007, 246, 247; *Herwig*, MMR 2001, 245, 246.

25) Etwa das einfache Einschreiben, das Einschreiben mit Rückschein oder die förmliche Zustellung. Ein Einschreiben verhilft allerdings ebenfalls nicht zum Beweis, dass tatsächlich eine Erklärung mit dem behaupteten Inhalt zugegangen ist.

26) Etwa § 5 Abs. 5 VwZG und die entsprechenden Landesgesetze, § 174 Abs. 3 und 4 ZPO.

27) Zu weiteren Aufbewahrungspflichten und deren Erläuterung s. *Roßnagel/Fischer-Dieskau/Jandt/Knopp* (o. Fußn. 8), S. 79 ff.

nische Dokumente praktisch keinen Beweiswert besitzen. Da die qualifizierten Zertifikate jedoch nach § 4 Abs. 1 SigV nur für fünf Jahre nach Schluss des Jahres, in dem die Zertifikatsgültigkeit abläuft, aufbewahrt werden und außerdem die Sicherheitseignung der verwendeten Hash- und Verschlüsselungsalgorithmen zeitlich begrenzt ist, sind aktive Maßnahmen zum Erhalt des Beweiswerts erforderlich.[28] Akkreditierte Zertifizierungsdiensteanbieter haben die von ihnen ausgestellten Zertifikate sogar für weitere 30 Jahre nach Ablauf der Gültigkeit in ihrem Verzeichnis zu führen (§ 4 Abs. 2 SigV). Doch auch hier bleibt das Aufbewahrungsproblem grundsätzlich bestehen. Die Maßnahmen umfassen zuerst die in § 6 Abs. 1 Satz 2 SigG, § 17 SigV geregelte Neusignierung. Zur Sicherung des Authentizitätsnachweises ist jedoch weiter die Aufbewahrung des Nutzerzertifikats und aller notwendigen Verifikationsdaten zu dessen Bestätigung erforderlich. Auch diese Bestandteile sind in eine Neusignierung einzubeziehen.[29]

Der Nutzer kann diese Maßnahmen selbst ergreifen, doch einfacher und wohl auch sicherer wäre die Nutzung entsprechender Diensteangebote Dritter. Allerdings sollte auch hier angesichts des u.U. erheblichen Schadensrisikos bei Verlust der Dokumente für den Nutzer erkennbar sein, ob der Anbieter zuverlässig ist und ein anerkanntes Verfahren anwendet. Im Rahmen der Bürgerportale sind Beweiserhaltungsmaßnahmen bezüglich Signaturen bislang nicht vorgesehen, wohl aber die sichere Aufbewahrung elektronischer Dokumente, die immerhin Zugriffsschutz und Schutz vor Verlust bietet.

IV. Gewährleistung der Sicherheit

Für die Nutzbarkeit all dieser Dienste ist es notwendig, dass ihre Sicherheit im Vorfeld nach feststehenden Standards bestätigt wird. Soll für den Nutzer Sicherheit bestehen, dass er durch die jeweiligen Dienste Nachweis über seine Kommunikation führen kann oder bestimmte Sorgfaltspflichten erfüllt, muss zum einen die rechtliche – vor allem die gerichtliche – Anerkennung eines ausreichenden Beweiswerts oder eines ausreichenden Sicherheitsniveaus vorhersehbar sein, zum anderen sollte diese Anerkennung nicht von einer immer neuen sachverständigen Prüfung abhängig sein. Erreicht wird dies am besten durch einen Anscheinsbeweis, sei er gesetzlich geregelt wie im Falle des § 371a ZPO für qualifizierte elektronische Signaturen oder aber Ergebnis der Rechtsprechung. Voraussetzung eines solchen Anscheinsbeweises ist aber das nachweisbare Vorliegen von Eigenschaften der Dienste, auf denen ein entsprechender Erfahrungssatz, etwa dass das Verfahren bei der Erstellung einer Zugangsbestätigung durch Bürgerportalanbieter hinreichend sicher ist, gründen kann.[30]

Grundlage eines solchen Erfahrungssatzes kann eine Akkreditierung der Dienste durch hierfür anerkannte Stellen sein sowie die Zertifizierung der verwendeten technischen Komponenten. Im Rahmen der Akkreditierung können die technische Sicherheit, die Organisation und die Zuverlässigkeit der Dienste bzw. ihrer Anbieter vor der Dienstaufnahme überprüft werden. Im Zusammenhang mit dem Akkreditierungsverfahren können außerdem ausreichende Anforderungen an die Dienste entwickelt werden. Für Bürgerportaldienste etwa wird eine rechtliche Regelung der Anforderungen und eines Akkreditierungsverfahrens angestrebt. Auf diese Weise ist eine Vorab-Prüfung gewährleistet, auf die die Rechtsprechung bei der Annahme eines Erfahrungssatzes für die Sicherheit der Dienste abstellen kann.

V. Fragen der europarechtlichen Zulässigkeit

Die staatliche Gewährleistung der Sicherheit der Grunddienste setzt eine Regulierung dieser Dienste und eine Überwachung der Tätigkeit voraus. Eine solche Regulierung ist, besonders im Umfeld elektronisch erbrachter und damit weitgehend ortsunabhängiger Dienste, auch an europäischem Recht zu messen. Neben der allgemeinen Dienstleistungs- und Niederlassungsfreiheit sind vor allem die Dienstleistungsrichtlinie (DLRL)[31] und die E-Commerce-Richtlinie (ECRL)[32] zu beachten.

1. E-Commerce-Richtlinie

Die ECRL fordert in Art. 4 Abs. 1 die Zulassungs- und Anmeldefreiheit von Diensten der Informationsgesellschaft. Im deutschen Recht wird diese Vorgabe durch § 4 TMG umgesetzt.[33] Die unter III.1. bis III.7. (s.o.) aufgezählten Dienste, also die im Bürgerportalvorhaben zusammengefassten Dienste zum Schutz der vertraulichen Kommunikation, zur Authentifizierung und zur nachweisbaren Zugangsbewirkung sowie der Protokollierungsdienst für die elektronische Geschäftsabwicklung werden elektronisch angeboten und erbracht werden. Sie erschöpfen sich auch nicht in der Signalübermittlung, sind also keine TK- oder tk-gestützte Dienste nach § 3 Nr. 24 und 25 TKG. Dies gilt auch für weite Teile eines Aufbewahrungsdienstes, wie er in III.7. (s.o.) skizziert ist. Es handelt sich somit zumindest beim Angebot der Dienste um Telemediendienste[34] und Dienste der Informationsgesellschaft. Daraus ergibt sich die Frage, ob die Regelung eines Akkreditierungsverfahrens und die Bestimmung der hierzu erforderlichen Anforderungen an die Dienste sowie das Anknüpfen bestimmter Rechtsfolgen an das Vorliegen einer Akkreditierung den Grundsatz der Zulassungsfreiheit durchbrechen und gegen Art. 4 Abs. 1 ECRL verstoßen.

Im Ergebnis ist dies zu verneinen. Von einem Zulassungsverfahren ist auszugehen, wenn die Tätigkeitsaufnahme von einer behördlichen Entscheidung abhängig gemacht wird. Bei einem freiwilligen Akkreditierungsverfahren, das der Qualitätssicherung dient, ist dies nicht der Fall. Die Akkreditierung entscheidet lediglich, ob der Antragsteller sich als auf diese Weise geprüft bezeichnen darf und ob bestimmte, an eine Akkreditierung anknüpfende Rechtsfolgen eintreten. Der Dienst kann jedoch auch ohne vorherige Akkreditierung angeboten werden. Diese Einschätzung wird auch durch Erwägungsgrund 28 ECRL bestätigt. Freiwillige Akkreditierungssysteme sollen demnach vom Grundsatz der Zulassungsfreiheit nicht berührt werden.

2. Dienstleistungsrichtlinie

Für die DLRL gilt ein ähnlicher Befund. Ihr Anwendungsbereich ist zwar eröffnet, da es sich bei den aufgeführten

28) *Horst/Pordesch/Gondrom/Brandner* (o. Fußn. 8), S. 37; *Fischer-Dieskau* (o. Fußn. 8), S. 162 ff.; *Roßnagel/Fischer-Dieskau/Jandt/Knopp* (o. Fußn. 8), S. 61.
29) *Fischer-Dieskau* (o. Fußn. 8), S. 208 ff.
30) *Prütting*, in: Lüke (Hrsg.), MüKo-ZPO, 2. Aufl. 2002, § 286 Rdnr. 55 ff.; *Förster*, in: Musielak, ZPO, 5. Aufl. 2007, § 286 Rdnr. 23 ff.
31) RL 2006/123/EG des Europäischen Parlaments und des Rates v. 12.12.2006 über Dienstleistungen im Binnenmarkt.
32) RL 2000/31/EG des Europäischen Parlaments und des Rates v. 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft [...] im Binnenmarkt (RL über den elektronischen Geschäftsverkehr).
33) *Mickelitz*, in: Spindler/Schuster (o. Fußn. 18), § 4 TMG Rdnr. 1 ff.
34) *Schmitz*, in: Spindler/Schuster (o. Fußn. 18), § 1 TMG Rdnr. 5 ff.

Diensten in der Regel um entgeltliche, selbstständige Tätigkeiten handelt. Die Ausnahmen des Art. 2 Abs. 2 DLRL betreffen diese nicht, mit Ausnahme der möglichen Bewirkung förmlicher Zustellungen, die mit einer Beleihung verbunden wäre und daher unter die Ausübung öffentlicher Gewalt nach Art. 2 Abs. 2 i) DLRL fiele. Gegenüber der ECRL ist die DLRL nach Art. 3 Abs. 1 DLRL subsidiär, soweit sich die Bestimmungen widersprechen. Dies schließt jedoch ihre Anwendbarkeit auf die hier besprochenen Dienste nicht aus, soweit keine Widersprüche, sondern weitergehende Regelungen vorliegen und soweit Teile der Dienste aus dem Anwendungsbereich der ECRL herausfallen.

Die DLRL untersagt den Mitgliedstaaten in Art. 9 Abs. 1 DLRL, die Aufnahme oder Ausübung einer Dienstleistungstätigkeit von einer Genehmigung abhängig zu machen, es sei denn, dies ist nach Art. 9 Abs. 2 DLRL gerechtfertigt. Eine Genehmigungsregelung ist nach Art. 4 Nr. 6 DLRL jedes Verfahren, das zur Einholung einer förmlichen oder stillschweigenden behördlichen Entscheidung verpflichtet. Zum Schutz des freien Dienstleistungsverkehrs geht die RL in Art. 16 sogar noch weiter und untersagt gegenüber Dienstleistungen, die aus anderen Mitgliedstaten angeboten werden, das Aufstellen einiger Anforderungen, darunter auch das Erfordernis, eine Genehmigung einzuholen, sich anzumelden oder zu registrieren (Art. 16 Abs. 2 b) DLRL). Auch hier gilt jedoch, dass die Akkreditierung für die Aufnahme oder Ausübung eines der genannten Dienste nicht verpflichtend, sondern freiwillig ist und lediglich zur Sicherung und zum Nachweis einer bestimmten Qualität erfolgt. In diesem Rahmen wird sie zur Qualitätssicherung in Art. 26 Abs. 1 DLRL zugelassen.[35] Dies würde sich erst dann ändern, wenn für einen breiten Anwendungsbereich die Verwendung nicht akkreditierter Dienste gesetzlich ausgeschlossen würde, sodass diese praktisch nicht mehr genutzt werden könnten. Eine solche Entwicklung ist absehbar jedoch nicht zu erwarten.

Auf eine Rechtfertigungsmöglichkeit nach Art. 9 Abs. 2 DLRL zumindest für Maßnahmen gegenüber sich niederlassenden Dienstleistungserbringern kommt es damit nicht mehr an. Das Postulat der Zulässigkeit von Akkreditierungsverfahren wird auch durch die ausdrückliche Erlaubnis dieses Mittels in anderen vergleichbaren Bereichen, vor allem durch die Signaturrichtlinie in Art. 3 Abs. 2 SigRL,[36] bestätigt.

VI. Zusammenfassung

Mit dem Signaturgesetz von 1997 wurde ein Anfang gemacht, um eine Infrastruktur zu schaffen, die einen sicheren elektronischen Rechts- und Geschäftsverkehr ermöglicht. Mit dem Fortschreiten der Entwicklung wird deutlich, dass Voraussetzung für eine weitere Verlagerung von Rechts- und Geschäftsprozessen auf elektronische Medien eine Ausweitung von Infrastrukturangeboten ist, die ähnlich der Signatur rechtlich anerkannt gegen technische Risiken Sicherheit verschaffen. Der beweisbare elektronische Zugang, die Sicherung von Authentizität und Vertraulichkeit in der E-Mail-Kommunikation und die sichere Aufbewahrung der entstehenden elektronischen Dokumente sind Beispiele solcher erforderlicher Grunddienste. Ähnlich wie bei elektronischen Signaturen sind jedoch ein Rechtsrahmen zur Festlegung des ausreichenden Sicherheitsniveaus und eine Kontrolle der Einhaltung erforderlich. Die Wahl von Zertifizierungs- und Akkreditierungsverfahren zur Qualitätssicherung erweist sich hierbei auch unter europarechtlichen Gesichtspunkten als beste Alternative.

35) *Ensthaler/Synnatzchke/Vogt,* in: Leible (Hrsg.), Die Umsetzung der Dienstleistungsrichtlinie – Chancen und Risiken für Deutschland, 2008, S. 237, 250; *Kommission der Europäischen Gemeinschaften,* Hdb. zur Umsetzung der Dienstleistungsrichtlinie, 2007, S. 79 f., abrufbar unter: http://ec.europa.eu/internal_market/services/services-dir/index_de.htm.

36) RL 1999/93/EG des Europäischen Parlaments und des Rates v. 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.