AUFSATZ

Christoph Engemann

Die Adresse des freien Bürgers: Digitale Identitätssysteme Deutschlands und der USA im Vergleich

Seit etwa 20 Jahren versuchen Nationalstaaten im Internet Systeme zu etablieren, die es erlauben, Menschen mit ähnlicher Zuverlässigkeit zu adressieren, wie es von den papierbasierten Identitätsdokumenten erwartet wird: Geburtsurkunden, Personalausweise, Pässe, Aufenthaltstitel usw. Die Zustellung solcher Dokumente ist zugleich elementare Voraussetzung gesellschaftlicher Inklusionsansprüche[1] und notwendige Bedingung des Regierens.[2] Ohne Adressen keine Bevölkerung, und eine Bevölkerung, die ihr Leben mehr und mehr im Internet vollzieht, wo staatliche Papierdokumente kaum Geltung haben, bedroht die Staatlichkeit und fordert entsprechend neue Gouvernementalitäten mit neuen Weisen, eine Bevölkerung zu adressieren, heraus. Eine solche, durch einen Medienwandel herbeigeführte Situation konfrontiert darüber hinaus die Staatlichkeit mit der eigenen Medialität und evoziert Fragen nach deren Status unter den Elementen des Regierungswissens. Die Frage stellt sich, welche politischen Projekte die Regierungen in Deutschland und den USA im genannten Zeitraum als Antwort auf diese Herausforderungen vorgebracht haben. Mit der Betonung auf politischen Projekten werden diese von den durch die Veröffentlichungen von Edward Snowden bekannt gewordenen Projekten der NSA und anderer Geheimdienste abgegrenzt. Letztere waren und sind im erheblichen Maße geheim, während die hier dargelegten Projekte in der Öffentlichkeit diskutiert und implementiert werden. Der Einbezug der sogenannten Öffentlichkeit eskaliert dabei über die im Folgenden identifizierten drei Etappen, in denen der Prozess der Stiftung digitaler Adressierungsmedien bis heute stattgefunden hat. Dabei wird außerdem gezeigt, dass dieser Prozess mit einer zunehmenden Reflexivität über die Medialität von Staatlichkeit selbst einhergeht.

Die Beschränkung auf die USA und Deutschland ist den pragmatischen Zwängen der Handhabbarkeit des Materials geschuldet. Dennoch lassen sich auch Aussagen über diese beiden Länder hinaus treffen: So sind die USA weiterhin das Zentrum der aktuellen Medienentwicklungen und dabei sowohl ökonomisch als auch regulativ global von Einfluss. Die Hardware digitaler Medien wird zwar in der Regel zusammengebaut (*Assembled in China*), aber überwiegend in Kalifornien entwickelt

1 Vgl. Derrida 2005, S. 55 & passim; Opitz 2012, S. 149 f. Derrida und Opitz beziehen ihre Diskussionen der Adressierbarkeit auf Menschen, dieses Problem betrifft aber auch feste und bewegliche Güter und damit das Statut des Eigentums, das innerhalb eines gegebenen Territoriums, unter anderem mittels Kataster, Verträgen, steueramtlichen Statistiken und Zollverfahren, organisiert wird. Vgl. Scott 1998; Torpey 1998.

2 Engemann 2012 a.

(*Designed in California*). Die wesentlichen Softwareprogramme und Protokolle werden in den USA entwickelt und standardisiert. Für Deutschland wiederum lassen sich sehr frühe und besonders ehrgeizige, aber dennoch erfolglose Versuche der Transposition von papierprozessierender zu digitaler Staatlichkeit konstatieren. Deren industriepolitische Motivationen galten und gelten der Europäischen Union als Wirtschafts- und Regierungsraum, ebenso aber dem globalen Exportmarkt. Neben Infineon, Siemens, Giesecke und Devrient – um nur einige Beispiele zu nennen – ist insbesondere die Bundesdruckerei in alle deutschen Projekte zur digitalen Identität involviert.[3] Diese werden zugleich international vermarktet: So liefert die Bundesdruckerei beispielsweise digitale Identitätslösungen an die Vereinigten Arabischen Emirate und Venezuela. Aber auch im europäischen Ausland sind deutsche Firmen tätig, so wie zum Beispiel bei der österreichischen BürgerCard, die in Teilen von Giesecke und Devrient geliefert wird. Nicht zuletzt engagiert sich die Bundesrepublik in den Gesetzgebungs- und Verordnungsverfahren der Europäischen Union zur digitalen Identität für Europa und sucht hier ihren Einfluss auf die Standards und Lösungen geltend zu machen.

Im Unterschied zur Kommunikationswissenschaft liegen in der deutschen medienwissenschaftlichen Debatte mit Ausnahme von Wolfgang Hagens medienhistorischer Studie zum Radio[4] bislang kaum vergleichende Untersuchungen zu den nationalen und nationalstaatlichen Unterschieden der Medienentwicklung vor. Dies geht sicher auf den zugleich komplexen wie zu befragenden Universalismus von Medienbegriffen zurück, aber auch auf die Schwierigkeit, die unterschiedlichen ökonomischen und rechtlichen Konfigurationen zu (er)kennen und in ihrem Einfluss einzugrenzen. Was der sozialwissenschaftliche Diskurs als Pfadabhängigkeiten bezeichnet,[5] die Einschränkung und Bindung der Dynamik sozialer und ökonomischer Prozesse durch historisch gewachsene formelle und informelle Regularien und Institutionen, stellt die Medienwissenschaften vor die komplexe Aufgabe, diese national gewachsenen technischen und sozialen Abhängigkeiten der Medialität ins Verhältnis zu den »medien-epistemologisch fundamentale[n] Unterschiede[n]«[6] zu setzen. Nicht immer werden sich Letztere so elegant in Gleich- und Wechselstrom aufheben lassen, wie Hagen das für die Radioentwicklung in den USA versus Europa zeigen kann.

In Hinblick auf die Entwicklung digitaler Identitätsmedien treten spätestens mit den Snowden-Veröffentlichungen Phänomene wie (National-)Staatlichkeit und Hoheitlichkeit in ihrer Medialität genauso wie in ihrer medienformativen Gewalt in Erscheinung. Man kann das wie der niederländische Medienwissenschaftler und Aktivist Geert Lovink als Bewegung der Medienwissenschaften »vom schizoiden,

3 Engemann 2011.

4 Vgl. Hagen 2005.

5 Für die Medienwissenschaft ist der inzwischen klassische Text zur Schreibmaschinentastatur von Paul David interessant: David 1985; siehe weiterhin: North 1990; Pierson 2005.

6 Hagen 2005, S. 163.

revolutionären zum paranoiden, reaktionären Pol«[7] begreifen oder einfach als Versuch, in der deutschen Medienwissenschaft konstitutive, aber zu wenig ausgewiesene Momente zu explizieren: Paranoia und Staatlichkeit.[8] Im vorliegenden Beitrag müssen diese Hinweise Desiderat bleiben, aber das hier präsentierte Material mag hinreichen, um die Unterschiede und gleichzeitigen Abhängigkeiten zwischen deutschen und amerikanischen Entwicklungen mindestens skizzenhaft anzuzeigen und die Prävalenz der angesprochenen Fragen zu verdeutlichen. Dabei wird sich auch der Zugewinn einer medienwissenschaftlichen Reflektion gegenüber den bislang unter anderem von Manuel Castells[9] und Saskia Sassen[10] vorgelegten Untersuchungen zum Schicksal der Staatlichkeit unter Bedingungen digitaler Netzwerke zeigen.

1. 1993-2000 – *Crypto-Wars*, *Clipper-Chip* und Signaturgesetz

1993 waren graphische Webbrowser[11] gerade zwei Jahre alt, die Anzahl der Internetnutzer war insgesamt klein und die kommerzielle Nutzung des Internets mehr die Ausnahme als die Regel. Dennoch fand bereits in diesem Jahr der erste nationalstaatliche Versuch statt, eine digitale Adressierbarkeit zu etablieren. Im April 1993 war die Clinton-Administration kaum vier Monate im Amt und ging mit ihrem ersten großen politischen Projekt an die Öffentlichkeit. Al Gore, der sich im Wahlkampf als »Erfinder des Internets« bezeichnet hatte, stellte die Public Encryption Management Initiative vor. Künftig sollten alle Telefone und alle Computer einen kryptographischen Chip enthalten, der sowohl die Verschlüsselung der Kommunikation als auch die Identifizierung der Kommunikationsteilnehmer ermöglichen würde. Damit wären zum einen die Sicherheit und Vertraulichkeit digitaler Kommunikation garantiert, zum anderen sind mit diesem System durch die Identifizierbarkeit der Beteiligten sichere ökonomische Transaktionen gewährleistet. Vorangegangen war dieser Initiative ein bereits auf das Ende der 1980er Jahre zurückgehender Konflikt um die Regulation der zugrunde liegenden kryptographischen Verfahren. Noch unter Ronald Reagan hatte zwischen National Security Agency (NSA), dem Pentagon, dem FBI und dem National Institute of Standards and Technology (NIST) eine Auseinandersetzung um die kommerzielle Nutzung der *Public-Key*-Kryptographie (PKI)[12] begonnen. Dem »Bedürfnis nach Privatsphäre« (*need*

7 Original in Englisch; Übersetzung C.E.

8 Lovink 2014. Zur Paranoia verdanke ich entscheidende Hinweise den bislang unveröffentlichten Vorträgen Elena Meilickes, gehalten am Graduiertenkolleg Mediale Historiographien Weimar; vgl. außerdem Schmidgen 2013; zur Staatlichkeit: Winthrop-Young 2012; Schröter 2014.

9 Castells 2004; Castells 2001.

10 Sassen 2008; Sassen 2000.

11 Webbrowser sind Programme wie Firefox, Internet Explorer oder Google Chrome, mit denen man das Internet nutzen kann.

12 Siehe die Darstellungen bei Schneier, Banisar 1997, S. 463 ff.; Levy 2001, S. 178-186, 226 ff.; Neymann 2001, S. 78 f. PKI wird in diesem Beitrag nicht näher erläutert. Siehe Kahn 1996.

for privacy) standen die »Bedürfnisse nach Durchsetzung der Strafverfolgung« (*needs for law enforcement*), mithin der Wunsch, abhören zu können, gegenüber.[13] Die NSA hatte am Übergang zu den 1990er Jahren einen *Skipjack* genannten kryptographischen Algorithmus entwickelt, der den widerstreitenden Interessen entgegenkommen sollte: *Skipjack* würde starke Verschlüsselung ermöglichen, aber zugleich eine definierte Hintertür zu Abhörzwecken bereithalten. *Capstone* und *Clipper* hießen die Mikrochips, in denen *Skipjack* implementiert wurde und die den Plänen der Clinton-Administration zufolge massenhafte Verbreitung finden sollten *Capstone* war für Computer vorgesehen, der *Clipper-Chip* hingegen für Telefone. Letzterer sollte für Al Gores Initiative namensgebend werden. In der vom Weißen Haus am 16. April 1993 verbreiteten Pressemitteilung heißt es: »Von staatlichen Ingenieuren ist nach den höchsten derzeit verfügbaren Standards ein Mikroprozessor namens ›Clipper-Chip‹ entwickelt worden«.[14] Die Besonderheit dieses Chips liege darin, die »Zweischneidigkeit der Verschlüsselung« umgehen zu können: »Verschlüsselung dient dem Schutz der Privatsphäre der Einzelnen und dem Rechtsschutz der Industrie, aber kann auch Kriminellen und Terroristen zu ihrer Abschirmung dienen«.[15]

Realisiert würde dieses über das in *Skipjack* eingebaute *Key-Escrow* genannte Verfahren der Schlüsselhinterlegung:

> »Jedes Gerät, das den Chip enthält, wird zwei einmalige Schlüssel bekommen, Chiffren, die autorisierte Regierungsstellen benötigen, um die Nachrichten, die mit dem Gerät verschlüsselt wurden, zu entziffern. Bei der Produktion der Geräte werden die beiden Schlüssel getrennt in zwei ›Key-Escrow‹-Datenspeichern hinterlegt, die vom Generalbundesanwalt eingerichtet werden. Der Zugang zu diesen Schlüsseln ist nur Regierungsbeamten mit einer legalen Autorisierung zum Abhören möglich.«[16]

Die *Clipper-Chip*-Initiative war also bereits 1993 der Versuch, einzulösen, was 20 Jahre später Edward Snowden als Realität offenbart hat: staatliche Hintertüren in möglichst vielen elektronischen Geräten. Mit dem entscheidenden Unterschied, dass dies in aller Öffentlichkeit und auf einer legalen Basis vollzogen werden sollte und nicht mittels geheimdienstlicher Interventionen auf Grundlage rechtlich fragwürdiger Präsidialdirektiven. Der Zugriff auf ein mit *Clipper* oder *Capstone* ausgestattetes elektronisches Gerät hätte der »legal authorization to conduct a wiretap« bedurft, also einer richterlichen Überwachungsanordnung. Ob diese Autorisierung in jedem Fall dem Äquivalent eines Durchsuchungsbefehls entsprochen hätte und somit der gerichtlichen Prüfung der Verhältnismäßigkeit unterlegen hätte, blieb in Al Gores Präsentation des Systems offen. Nicht nur hieran entzündete sich die Kritik gegen den *Clipper-Chip*, denn die amerikanische Öffentlichkeit lehnte die Idee eingebauter Abhörschnittstellen in elektronischen Geräten mit großer Mehrheit ab. Die Clinton-

13 Working Group on Data Security: www.epic.org/crypto/clipper/working_group.html (Zugriff vom 12.01.2015).

14 The White House, Statement by the Press Secretary vom 16. April 1993. www.epic.org/crypto/clipper/white_house_statement_4_93.html (Zugriff vom 20.06.2014); Übersetzung C.E.

15 Ebd.

16 Ebd.

Administration zeigte sich zunächst unbeeindruckt und stellte im Februar 1994 den auf dem *Clipper-Chip* aufbauenden *Digital Signature Standard* vor. Neben der Verschlüsselung der Daten sollten *Clipper* und *Capstone* damit auch der Authentisierung dienen:

> »[…] Absender und Empfänger einer elektronischen Nachricht werden verifizierbar. Eine solche Technologie wird für weite Bereiche der geschäftlichen Verwendung eine kritische nationale Informationsinfrastruktur sein. Ein digitaler Signaturstandard wird den Einzelnen in die Lage versetzen, Geschäfte elektronisch abzuschließen, statt signierte Papierverträge austauschen zu müssen.«[17]

Während auch die Nutzung dieses Verfahrens freiwillig bleiben sollte, wäre es doch faktisch über die Hinterlegung der Schlüssel bei staatlichen Stellen der Zustellung von offiziellen digitalen Identitäten gleichgekommen. Der öffentliche Druck jedoch wuchs, und in den folgenden drei Jahren wurden von der Clinton-Administration diverse Änderungen der *Clipper*-Initiative mit dem Ziel unternommen, öffentliche Akzeptanz für das Projekt zu gewinnen. Sollte das *Key-Escrow*, also die Hinterlegung der kryptographischen Nachschlüssel, zunächst noch bei zwei verschiedenen staatlichen Stellen erfolgen, so bot man der staatsskeptischen amerikanischen Öffentlichkeit in einem zweiten Schritt an, diese in die Kontrolle des privaten Sektors zu geben. Dennoch blieb insbesondere die amerikanische IT-Industrie auf Distanz und bangte um ihre Exportchancen, da Hardware, die offiziell eine Abhörschnittstelle für amerikanische Behörden enthielt, international nicht absetzbar gewesen wäre. Ende 1996 scheiterte das *Clipper-Chip*-Projekt dann endgültig. Die als *Crypto-Wars* bekannt gewordene *Clipper-Chip*-Kontroverse sollte neben dem »Hacker Crackdown«[18] von 1990 für die Politisierung des Internets in den USA entscheidend werden. Insbesondere etablierte sich die Electronic Frontier Foundation (EFF) als wichtiger netzpolitischer Akteur in den USA und stieg, ähnlich wie später der Chaos Computer Club in Deutschland, zur ersten Adresse einer Gouvernementalisierung auf, die Foucaults Definition gemäß, aber unter digitalen Bedingungen, dazu beiträgt, »zu definieren, was in die Zuständigkeit des Staates fallen darf und was nicht, was öffentlich und was privat ist, was staatlich und was nicht staatlich ist«.[19] Einer der Initiatoren der EFF fasste die zugrunde liegende Konfrontation folgendermaßen zusammen: »Das eigentliche Ziel des ›Key-Escrow‹ ist es, die Rechte des Staates über die Rechte des Einzelnen zu setzen. Das eigentliche Ziel starker Verschlüsselung auf der anderen Seite ist es, die Rechte des Einzelnen über die Rechte des Staates zu setzen«.[20]

So John Gilmore, der einer der prominentesten Vertreter der libertären Cypherpunks werden sollte, die die Kryptographie als Befreiungsinstrument von staatlicher

17 The White House, Statement of the Press Secretary vom 4. Februar 1994: www.epic.org/crypto/clipper/white_house_statement_2_94.html (Zugriff vom 20.05.2014); Übersetzung C.E.

18 Sterling 1992.

19 Foucault 2004, S. 134-172, hier S. 164.

20 Brin 1998, S. 103; Übersetzung C.E.

Überwachung sahen und kreativ deren Regulation und Kontrolle unterliefen.[21] Dem in *Clipper-Chip* und *Digital Signature Standard* evidenten staatlichen Adressierungsbegehren wurde hier die Kryptographie als Anonymisierungsmittel und somit Entzug staatlicher Adressierungspotenzen entgegengesetzt. Neben der Verschlüsselungssoftware PGP, deren Code und Verfahren strengen Exportbeschränkungen unterlagen, wurden hier bereits konzeptuell das heutige Bitcoin vorwegnehmende kryptographische Währungen debattiert, die staatsfreie Werttransfers erlauben sollten: »Starke Verschlüsselung existiert […] Was daraus hervorgehen wird, ist unklar. Aber ich denke, es wird eine Art von anarcho-kapitalitischem Marktsystem, das ich Krypto-Anarchie nenne (nur freiwillige Kommunikation, ohne Dritte, die sich einschalten)«.[22]

Nicht Dritte, wie Nationalstaaten es sind, würden die für zuschreibbares Handeln notwendigen Dokumentationssysteme stellen, sondern die jeweils miteinander Kommunizierenden selbst. Bereits 1991 hatte Gilmore die Kryptographie als Möglichkeit eines solchen Verweises des Staates aus den Beziehungen der Menschen gesehen: »Wir müssen gegenüber denjenigen rechenschaftsfähig sein, mit denen wir kommunizieren. Wir müssen gegenüber denjenigen rechenschaftsfähig sein, mit denen wir Geschäfte machen. Und die entsprechenden Technologien, die das durchsetzen können, müssen gebaut werden«. Spätestens nachdem mit dem *Clipper-Chip* die *Crypto-Wars* losbrachen, wurde die Frage anonymer Infrastrukturen sowohl in den großen Tageszeitungen[23] diskutiert als auch in der entstehenden Open-Source-Bewegung zu einem zentralen Arbeitsfeld. In dem 1994 veröffentlichten *A Cypherpunk's Manifesto* heißt es: »Wir, die Cypherpunks, widmen uns dem Aufbau anonymer Systeme«.[24] Auch wenn solche Utopien nicht allgemein Anklang gefunden haben, für die Verbreitung von Wissen über und Software für die Kryptographie sowie für die Liberalisierung der in den 1990er Jahren noch den Restriktionen des Kalten Krieges unterliegenden Kryptopolitik hat diese Bewegung dennoch eine wichtige Rolle gespielt. Hier liegt einer der Anfänge jener Entwicklungen, die die Kryptographie in den Stand eines gouvernementalen Problems erhoben haben, aus dem sie bis heute nicht mehr entlassen worden ist. Zugleich kamen in diesen Diskursen Fragen nach der Zuständigkeit des Staates sowohl für Identitätsdokumente als auch für die Register, die die zeitfeste und prüfbare Dokumentation von Handlungen untereinander ermöglichen, auf.

Digitale Identität im Deutschland der 1990er Jahre

Wesentlich unaufgeregter und weitgehend ohne öffentliche Beteiligung verlief die Entwicklung in Deutschland. Noch unter Helmut Kohl wurde ab 1995 von der schwarz-gelben Bundesregierung ein Gesetzespaket zur Implementierung einer kryptographischen *Public-Key*-Infrastruktur vorbereitet, die der eigenhändigen

21 Vgl. Levy 2001, S. 167, 207 f.; Übersetzung C.E.

22 May 1994; Übersetzung C.E.

23 Levy 1994; Übersetzung C.E.

24 Hughes1993; Übersetzung C.E.

Namensunterschrift der Bundesbürger die Möglichkeit rechtlich äquivalenter digitaler Signaturen zur Seite stellen sollte. Am 11. Dezember 1996 wurde das sogenannte Signaturgesetz im Bundestag auf den Weg gebracht und schließlich am 22. Juli 1997 als Teil des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)[25] verabschiedet. Auf denselben kryptographischen Prinzipien der asymmetrischen Verschlüsselung wie das *Clipper-Chip*-System beruhend, sollte diese Gesetzgebung sowohl die Authentifizierbarkeit der Bürger als auch die zuverlässige Verschlüsselung von Daten im Internet ermöglichen. Ein *Key-Escrow*-System und kryptographische Hintertüren waren dagegen nicht vorgesehen. Zudem sollten keine Chips in Telefone oder Computer eingebaut werden, sondern die Authentifizierung und Verschlüsselung mittels Chipkarten und Lesegeräten realisiert werden. Von der Bundesregierung als weltweit erstes Gesetz dieser Art beworben,[26] wurden mit dem Signaturgesetz die Grundlagen für die rechtliche Anerkennung von digitalen Daten als gerichtsfeste Dokumente geschaffen:

§ 2 Absatz 1: Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.[27]

Der Staat bietet den Bürgern ein digitales Siegel an, mit dem sie Daten in Dokumente verwandeln können. Einmal digital signiert, verweist dieses Dokument innerhalb der kryptographischen öffentlichen Verschlüsselungsinfrastruktur auf ein bestimmtes Individuum, das als Inhaber des jeweiligen Signaturschlüssels registriert ist. Da zugleich eine mathematische Verweiskaskade der Signaturschlüssel auf die staatlichen Schlüssel besteht, zeichnet ein solcher Bürger jeweils seinen Namen im Namen des Staates.[28] Digitale Signaturen unterhalten dabei zu ihren Dokumenten eine besonders intensive Beziehung, denn aus dessen Daten wird eine »Hashwert« genannte Prüfsumme berechnet (von *hashing* = zerhacken). Anschließend wird dieser Digest mit dem privaten Schlüssel des Signierenden verschlüsselt und zugleich mit einem Zeitstempel versehen. Die entstehende Chiffre ist die digitale Signatur. Eine digitale Signatur wird also – anders als eine eigenhändige Signatur – nicht unter das Dokument gesetzt, sondern aus dessen Daten gebildet. Zugleich ermöglicht das digitale Siegel des Dokuments die Überprüfung von möglicherweise nachträglich vorgenommenen Änderungen. Dazu wird auf Empfängerseite aus dem entschlüsselten Dokument der Hashwert erneut berechnet und mit dem verschlüsselten Hashwert verglichen. Sind beide Werte gleich, so ist das Dokument unverfälscht übertragen worden und entspricht dem Dokument, das vom Sender signiert wurde.

25 Bundesregierung, Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste, Bgbl. I, S. 1870.

26 Vgl. Schulte 2003, S. 636.

27 Bundesregierung, Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste, Bgbl. I, S. 1873.

28 Vgl. Engemann 2011.

Im deutschen Recht können digitale Signaturen Individuen oder Organisationen[29] zugeordnet werden, und zumindest für Erstere müssen sie als digitale Namen gelten. Insofern ist der Effekt der Signaturgesetzgebung die Sicherstellung der Identität zwischen dem individuellem Namen und den digital signierten Dokumenten: Auf der medientechnischen Ebene ist das Dokument der Name. Das Dokument existiert nicht ohne den staatlich zugestellten digitalen Namen, und dieser Name tritt nur dort hervor, wo ein Dokument generiert wird.

Praktische Anwendung fanden die Regelungen des Signaturgesetzes allerdings kaum. Ursachen dafür waren Unsicherheiten bezüglich der Rechtsfolgen, hohe Kosten bei der Einrichtung und Unterhaltung der notwendigen Infrastrukturen sowie eine Marktentwicklung, die zum Leidwesen deutscher Bürokratenträume auch jenseits digitaler Signaturen dynamisch blieb. Wer eine digitale Signatur nutzen wollte, musste sich eine entsprechende Chipkarte und ein Lesegerät auf eigene Kosten beschaffen und sah sich dann sowohl von Seiten der Privatwirtschaft als auch der öffentlichen Verwaltungen einer verschwindend geringen Zahl von Angeboten gegenüber.

2. 2000-2010 – Kartenstrategien und Identirati

Nach dem Ende der *Crypto-Wars* mit dem Scheitern der *Clipper-Chip*-Initiative wird weder von der Clinton-Administration noch von der darauf folgenden Bush-Regierung ein ernsthafter Versuch unternommen, staatliche Identitätsdokumente im Internet zu etablieren. Gegenüber der Öffentlichkeit überlässt der amerikanische Staat in der gesamten ersten Dekade des 21. Jahrhunderts die Lösung des Zuordnungsproblems (von digitalen Daten zu Individuen) der Privatwirtschaft und der interessierten Öffentlichkeit. Anders verläuft die Entwicklung in Deutschland und Europa, wo digitale Signaturen und Chipkarten ein wesentliches und zentrales Politikfeld werden sollten. Mit dem Regierungswechsel 1998 ist es nun eine rot-grüne Koalition, die die Implementierung des Signaturgesetzes vorantreibt, um den bestehenden »circulus vitiosus«[30] zwischen fehlender kritischer Masse und fehlenden Anwendungen zu brechen. Vor dem Hintergrund der niedrigen Akzeptanz digitaler Signaturen und dem Wegfall von Grenzkontrollen im Schengen-Raum wird seit Ende der 1990er Jahre an einer Neugestaltung des Personalausweises gearbeitet. Die Ereignisse des 11. September 2001 führen dann zum am 9. Januar 2002 erlassenen »Gesetz zur Bekämpfung des internationalen Terrorismus«, welches »Regelungen für den künftigen digitalen Personalausweis«[31] beinhaltet. Bevor dieser jedoch konkret geplant wird, werden an anderer Stelle Fakten geschaffen: Rot-Grün versucht die Biopolitik in Deutschland auf digitale Beine zu stellen und beschließt 2002 und 2003 die Einführung des sogenannten JobCard-Verfahrens und einer elektro-

29 Im Kontext der elektronischen Gesundheitskarte ist dies für Kliniken und Apotheken der Fall (siehe unten); auch Engemann 2012 b, S. 149-175.

30 Hornung 2005, S. 40.

31 Ebd., S. 47 ff.

nischen Gesundheitskarte. Das JobCard-Verfahren geht auf einen Vorschlag der Hartz-Kommission zurück. Schon auf der Titelseite des als Hartz-Bericht bekannt gewordenen Dokuments, das den Fahrplan für die umstrittene, Agenda 2010 genannte Reform des Sozialstaates abgab, findet sich die Abbildung einer Signaturkarte. In den Empfehlungen der Kommission heißt es dann: »Es wird eine Signaturkarte für den Abruf von Verdienst- und Arbeitsbescheinigungen durch die jeweils zuständige Stelle […]entwickelt […]. Der Einsatz der Signaturkarte wird zu einer erheblichen Kostensenkung im Bereich der Verwaltung und der Unternehmen führen«.[32] Die etwa 35 Millionen sozialversicherten Menschen in Deutschland sollten also die Arbeits- und Verdienstbescheinigungen für die Arbeitslosen- und Rentenversicherung mithilfe digitaler Signaturen vermittelt bekommen.[33] Ein Jahr später beschließt die rot-grüne Koalition das »Gesetz zur Modernisierung der gesetzlichen Krankenversicherung«[34] (GMG) mit noch weit ambitionierteren Zielen. Unter dem neu eingeführten § 67 Elektronische Kommunikation des durch das GMG novellierten Fünften Sozialgesetzbuchs (SGB V) heißt es:

(1) Zur Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung soll die *papiergebundene Kommunikation* unter den Leistungserbringern so bald und so umfassend wie möglich durch die elektronische und maschinell verwertbare Übermittlung von Befunden, Diagnosen, Therapieempfehlungen und Behandlungsberichten, die sich auch für eine einrichtungsübergreifende fallbezogene Zusammenarbeit eignet, ersetzt werden.[35]

Papier, materielle Voraussetzung der Akte, die den Aufstieg der frühmodernen Staatlichkeit ermöglicht,[36] findet hier explizit Erwähnung im Gesetzestext. Nach bis heute geltender Rechtslage möge es so bald und so umfassend wie möglich ersetzt werden. Auf Grundlage digitaler Signaturen soll nicht nur der gesamte Schriftverkehr im medizinischen Bereich auf die digitale Form umgestellt werden, sondern auch jeder Bürger eine elektronische Gesundheitskarte erhalten.[37] Die 80 Millionen gesetzlich Krankenversicherten in Deutschland sollten mit dieser ihre elektronische Gesundheitsakte selbst verwalten können. Alle medizinischen Daten wie Diagnosen, Verschreibungen, Röntgenbilder usw. würden, in einer Telematik-Infrastruktur verschlüsselt, zur Speicherung kommen und über das Internet zugreifbar sein. Sämtliche Schreibvorgänge und Veränderungen in der elektronischen Gesundheitsakte wären wiederum über digitale Signaturen nach dem Signaturgesetz dokumentiert worden. Während die Versicherten mit ihrer elektronischen Gesundheitskarte Lese-

32 Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit: Moderne Dienstleistungen am Arbeitsmarkt, S. 27. www.bmwa.bund.de/Navigation/Service/bestellservice,did=12168.html (Zugriff vom 10.01.2015).

33 Ebd.; vgl. Hornung 2005, S. 46; Engemann 2012 a.

34 Bundesregierung, Gesetz zur Modernisierung der gesetzlichen Krankenversicherung. www.bmgs.bund.de/downloads/GKV_Modernisierungsgesetz.pdf (Zugriff vom 12.01.2015).

35 Ebd.; Hervorhebung C.E.

36 Vgl. Vismann 2000, S. 137; Müller 2012, S. 56.

37 Vgl. Hornung 2005, S. 41 & passim; Engemann 2012 b.

und teilweise auch Schreibzugriff auf diese lebensbegleitende Dokumentation ihres Körpers hätten, ist für Mediziner, Apotheker und Psychologen ein ihre Approbation belegender Heilberufsausweis vorgesehen, für Praxen, Kliniken und Apotheken außerdem eine Institutionenkarte und für die im Gesetz »berufsmäßige Gehilfen« genannten Pflegeberufe ein spezieller Berufsausweis. Als zu erwartende Größenordnung wurden 280.000 Ärzte, 56.000 Zahnärzte, 46.000 Apotheker und 570.000 Personen des Pflegepersonals im klinischen Bereich genannt.[38] Zugleich ging der Deutsche Pflegerat von 2,4 Millionen Beschäftigten im Pflegebereich aus, die einen Berufsausweis erhalten müssen.[39] Da im Gegensatz zur Ärzteschaft, den Apothekern und den Psychotherapeuten keine Kammern für die unter »berufsmäßige Gehilfen« gezählten Personen existierten, wurde die Einrichtung eines elektronischen Gesundheitsberuferegisters beschlossen. Zwei Jahre nach dem Erlass der Gesetzgebung zur elektronischen Gesundheitskarte ging die Bundesregierung im März 2005 mit ihrer eCard-Strategie an die Öffentlichkeit. Diese sah vor, dass

> »[…]die Elektronische Gesundheitskarte, der Digitale Personalausweis, das JobCard-Verfahren und die Elektronische Steuererklärung – eng aufeinander abgestimmt werden. Gleiche Standards und die breite Verwendbarkeit der Chipkarten […]. Ferner werden durch die Eckpunkte die elektronische Authentisierung (Identifizierung des Nutzers) und die qualifizierte elektronische Signatur (Äquivalent zur manuellen Unterschrift) zur Verwendung auf den Chipkarten vereinheitlicht«.[40]

In gewisser Weise wurden damit elektronische Gesundheitskarte und Personalausweis gleichgestellt. Beide enthalten die dem jeweiligen Individuum zugeordnete digitale Signatur und sollen es ermöglichen, im Internet Dokumente zu signieren. Die staatliche Aktenführung eines Individuums wäre damit vom Papier loszulösen und in digitalen Medien durchzuführen. Die Umsetzung dieser ehrgeizigen Strategie dauerte jedoch sehr viel länger als von den Initiatoren erwartet: Weder wurde die elektronische Gesundheitskarte, wie ursprünglich im Gesetz vorgesehen, zum 1. Januar 2006 eingeführt, noch gab es vor Ablauf der Dekade den elektronischen Personalausweis oder kam das JobCard-Verfahren zur Einführung. Das ist einerseits auf erhebliche Widerstände – insbesondere seitens der Ärzteschaft – gegen die Gesundheitskarte[41] zurückzuführen, andererseits verläuft die Anpassung der rechtlichen Rahmenbedingungen nur langsam und mit erheblichen Konkurrenzkämpfen zwischen den zuständigen Ministerien ab. Insbesondere beim Widerstand der Ärzteschaft und der Klinikbetreiber gegen die Digitalisierung des Gesundheitswesens liegt in mindestens zweifacher Hinsicht ein pfadspezifisches deutsches Phänomen vor: erstens die im Vergleich zu den USA in Deutschland stärker verbreitete tech-

38 Gematik, Gesamtarchitektur Version 1.3.0, 215. www.gematik.de/(S(3ozkwo45visgue45lgt4z545))/Detailseite___Architektur___Gesamtarchitektur.Gematik (Zugriff vom 08.02.2009).

39 Vgl. Borchers 2007.

40 Pressemitteilung: Bundeskabinett beschließt gemeinsame eCard-Strategie. www.verwaltung-innovativ.de/nn_684508/DE/Presse/Artikel/ArtikelArchiv/2005/20050314__bundeskabinett__beschliesst__gemeinsame__ecard__Strategie__artikel.html (Zugriff vom 20.06.2008).

41 Vgl. Engemann 2012 b.

nikskeptische Tendenz, die in den einschlägigen Veröffentlichungen der Ärzteschaft deutlich wird, und zweitens die bis auf die Bismarck'sche Sozialgesetzgebung zurückführbare Einbettung der Medizin in ein staatlich organisiertes Transferleistungsregime, in welchem die neuen Medien anders als im amerikanischen Diskurs nicht als Mittel zur Intensivierung der Patientenbeziehung[42] gelesen werden, sondern als bürokratische Usurpationsversuche gegenüber der Medizin.

Trotz des bislang zu verzeichnenden Scheiterns ist festzuhalten, dass von staatlicher Seite nicht in Zweifel gezogen wurde, online und offline Identitätsmedien zu integrieren, und dass die staatlich zugestellte digitale Identität auch in privaten und privatwirtschaftlichen Kontexten genutzt werden solle und in einigen Fällen sogar müsse. Die deutsche Bevölkerung sollte mittels Chipkarten und digitaler Signaturen adressierbar gemacht werden, und diese Adressen sollten zugleich Biopolitik unter digitalen Bedingungen erlauben. Denn sie sollte sich sowohl mit der Fremd- als auch der Selbstadressierung der individuellen Körper verschalten und damit einen unter digitalen Bedingungen gesundheitspolitisch erreichbaren Körper konstituieren.[43]

Die USA: Digitale Identität jenseits des Staates

Während also in Europa, allen voran in Deutschland, der Sozialstaat zum Schauplatz des staatlichen Medienwandels wird, ist in den USA, wo es bis zur Einführung von Obamas Gesundheitsreform keinen nennenswerten vergleichbaren Sozialstaat gab, eine andere Entwicklung zu beobachten: Zwischen 2001 und 2009 formiert sich eine heterogene Gruppe von Open-Source-Aktivisten, Crypto-Nerds und netzpolitisch Engagierten, die als Identerati[44] bezeichnet werden können. Bereits 2001 gründen sich die Identity Commons[45] und die Liberty Alliance[46]. Letztere wurde vom damaligen Serverhersteller SUN unterstützt und suchte schwerpunktmäßig Identitätsmanagementanwendungen für Großunternehmen zu entwickeln, während die Identity Commons dieses Problem allgemeiner für das Internet anzugehen suchte. Gemeinsam war der Liberty Alliance und den Identity Commons, dass sie Protokolle und Verfahren für »eine dezentralisierte, konsumentenzentrierte Identitätsinfrastruktur und sich daraus ergebende Fragen des sozialen Vertrauens«[47] entwickeln wollten. Ähnlich wie von Gilmore und den Cypherpunks gefordert, sollen mittels kryptographischer Verfahren distribuierte Autorisierungs- und Identifikationsmechanismen entwickelt werden, die dem Nutzer die Wahl der Authentifikationsmittel und der verbreiteten Daten erlauben. Neben einer Reihe von Start-Ups engagieren sich Mitte der ersten Dekade auch Konzerne wie Sun Microsystems und

42 Vgl. Swan 2009; Topol 2012.

43 Zur Biomacht als zugleich individualisierende als auch »massebildende« »Verstaatlichung des Biologischen« vgl. Foucault 1999, S. 286 f.; Muhle 2008, S. 252 f.

44 Hamlin 2006.

45 Identity Common: www.identitycommons.net/ (Zugriff vom 12.05.2014).

46 Liberty Alliance: www.projectliberty.org/ (Zugriff vom 20.06.2014).

47 Identity Commons History: www.wiki.idcommons.net/History (Zugriff vom 12.05.2014); Übersetzung C.E.

Microsoft in diesen Debatten. Der »Architect of Identity« von Microsoft, Kim Cameron, wurde einer der prominentesten Stichwortgeber der Identerati und veröffentlichte 2005 seine vielbeachteten *Laws of identity*.[48] Darin forderte er ein »Identity Metasystem«, das unter der Kontrolle der Nutzer stehen solle, multiple Identitäten in verschiedenen Kontexten erlaube, den Datenschutz stärke, betriebssystemagnostisch sei und eine konsistente UI (*user interface*) über alle Anwendungsformate aufweise. Die Staatlichkeit taucht dabei als eine Instanz unter vielen auf, die digitale Identitäten vergeben kann, denn staatliche Authentifikationsansprüche seien nur in sehr begrenzten Kontexten legitim:

> »Heutzutage beabsichtigen einige Regierungen die Einrichtung von digitalen Identitätsdiensten. Die Nutzung offizieller Identitäten ist im Verkehr mit Behörden sinnvoll (und zweifellos auch gerechtfertigt). Aber es ist eine Frage der Kultur, ob die Bürger zum Beispiel zustimmen, dass es nötig und gerechtfertigt sei, dass diese regierungsamtlichen Identitäten beim Zugang zu einem Familienwiki – oder beim Konsum eines Hobbies oder eines Lasters – genutzt werden müssen.«[49]

Familien, Hobbies und Laster sind die suggestiven Beispiele, die Cameron anführt, um die Notwendigkeit selbstverwalteter digitaler Identitätsservices zu rechtfertigen. Im Hintergrund steht aber auch hier die Frage nach der Notwendigkeit für ökonomische Transaktionen und auch danach, Verträge jeweils mit staatlichen Identitätssystemen absichern zu müssen – oder ob das nicht private Unternehmen ebenfalls könnten. Microsoft betrieb zwischen 2003 und etwa 2007 aktiv und mit großem Werbeaufwand die Entwicklung eines Infocard genannten Produkts, das Pseudonym- und Klarnamenidentifikation im oben genannten Sinne erlaubt hätte. Infocard sollte kommende Betriebssystemversionen eingebaut bekommen, und die Protokolle sollten offengelegt werden. Während die Protokolle tatsächlich weitgehend veröffentlicht wurden und die Beta-Versionen des Systems in der Open-Source- und Krypto-Szene verhaltende Anerkennung fanden, blieb die tatsächliche Auslieferung in kommerziellen Produkten von Microsoft aus. Zugleich veränderte sich ab 2006 die Situation erheblich: Erstens kommen mit Facebook, Twitter und anderen soziale Medien auf, bei denen die Nutzer häufig mit ihren Klarnamen auftreten, zweitens lösen Smartphones den PC als primäre Schnittstelle zum Internet ab, und drittens steigen Apple, Amazon und Google zu Anbietern von *Cloudcomputing* auf. Insbesondere die bei Smartphones gegebene Vertragsbindung an einen Telekommunikationsanbieter und die mit Cloud-Services einhergehende Einschließung der Nutzer haben die von den Identerati debattierten Authentifikationsnotwendigkeiten und -systeme unterlaufen. Das Telefon stellte für die Privatwirtschaft eine hinreichend stabile und belastbare Adresse dar, die die Zuordnungsprobleme, die noch beim PC existierten, entschärfte.

48 Cameron 2006; Übersetzung C.E.

49 Ebd.

3. Nach 2010: eGovernment-Gesetz & NSTIC

Im Juni 2010 veröffentlichte Thomas de Maizière, Innenminister der 2009 gewählten schwarz-gelben Koalition, seine *14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft*. Dort heißt es: »Der freie Bürger zeigt sein Gesicht, nennt seinen Namen, hat eine Adresse. Gleichzeitig sind wir es gewohnt, im Alltag grundsätzlich unbeobachtet zu handeln. Beides muss auch im Internet normal bleiben. Eine schrankenlose Anonymität kann es jedoch im Internet nicht geben«.[50] Woher das Gesicht und die Namen, mithin die Adressen im Internet kommen sollen, ließ de Maizière offen. Allerdings ist zu konstatieren, dass auch im neuen Jahrzehnt die Linie der deutschen Politik unverändert blieb. Die in der vorangegangenen Dekade gescheiterten und verzögerten Projekte staatlich zugestellter digitaler Identitätsdokumente wurden und werden bis heute fortgeführt. Der politische Anspruch, im und mit dem Internet staatliche Hoheitlichkeit zu etablieren, ist ungebrochen. Im Oktober 2010 erfolgte die Einführung des neuen Personalausweises, dessen integrierter Chip eine digitale Signaturfunktion und einen elektronischen Identitätsnachweis enthält. Beide Funktionen bleiben für den Bürger fakultativ und bedürfen der Aktivierung bei der Meldestelle. Trotz der nach drei Jahren erfolgten Ausgabe von beinahe 21 Millionen Ausweisen[51] ist bislang keine signifikante Nutzung dieser Funktionen zu verzeichnen. Die ursprünglich für 2006 vorgesehene Ausgabe der elektronischen Gesundheitskarte mit digitaler Signaturfunktion erfolgt seit 2011 und wird Ende 2015 mit circa 80 Millionen Karten abgeschlossen sein. Der Zeitpunkt der Einführung der darauf aufbauenden individuellen elektronischen Gesundheitsakte bleibt unklar, die notwendige Infrastruktur wird jedoch implementiert.[52] Das 2013 erlassene eGovernment-Gesetz sieht vor, dass die Verwaltungsangebote aller Bundesbehörden ab 2015 mittels des elektronischen Identitätsnachweises zugänglich sein sollen.[53] Die interne Behördenkommunikation soll dabei konsequent auf die elektronische Form umgestellt werden und das Papier nach Möglichkeit gänzlich verschwinden. Im zehn Jahre vorher erlassenen Gesetz zur Modernisierung des Gesundheitswesens war noch vom »ersetzt werden« des Papiers die Rede. Der 2013 zirkulierende Referentenentwurf des eGovernment-Gesetzes ging mit dem Papier sehr viel härter ins Gericht und forderte unter § 7 »Übertragen und Vernichten des Papieroriginals« unzweideutig ein Ende des Papiers in der Behördenwelt:

(1) Die Behörden des Bundes sollen an Stelle papiergebundener Unterlagen deren elektronische Wiedergabe in der elektronischen Akte aufbewahren […].

50 Maizière 2010.

51 Vgl. Borchers 2013 a.

52 Vgl. Borchers 2013 b.

53 Vgl. Bundesregierung, Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG); Borchers 2013 a.

(2) Papiergebundene Original-Unterlagen sollen nach der Übertragung in die elektronische Akte mindestens drei Wochen in einer Zwischenablage aufbewahrt und *anschließend vernichtet* werden.[54]

In der schließlich amtlich gewordenen Fassung des eGovernment-Gesetzes sind diese Formulierungen aufgrund des absehbar weiter bestehenden Nebeneinanders von Papier und elektronischer Form einerseits und der insbesondere im Beweisrecht geforderten Vergleichbarkeit von Papierurkunden mit ihren Originalen andererseits etwas zurückgenommen:[55]

(1) Die Behörden des Bundes sollen, soweit sie Akten elektronisch führen, an Stelle von Papierdokumenten deren elektronische Wiedergabe in der elektronischen Akte aufbewahren.
(2) Papierdokumente nach Absatz 1 sollen nach der Übertragung in elektronische Dokumente vernichtet oder zurückgegeben werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.[56]

Im Kommentar zum eGovernment-Gesetz wird diesbezüglich erläutert: »Nach Einführung der elektronischen Akte soll diese grundsätzlich die einzige beziehungsweise die ›führende‹ Akte sein«.[57] Der Dokumentenstatus der in elektronischer Form erstellten und geführten Akten ergibt sich (mit wenigen Ausnahmen) aus digitalen Signaturen, welche mit dem elektronischen Personalausweis erstellt werden. Während in Deutschland somit die Nutzung der inzwischen etablierten *Public-Key*-Infrastruktur seitens der Bürger gering bleibt, werden die Schnittstellen in und zur Staatlichkeit weiterhin umgestellt. Sowohl die Beamten als auch die Bürger sollen vom Papier Abschied nehmen und ihre Akten und Prozesse digital abwickeln. In Deutschland spielen privatwirtschaftliche Akteure und der freie Markt in der Entwicklung digitaler Identitäten vordergründig kaum eine Rolle. Zugleich gibt es eine inzwischen fast 20 Jahre währende Kontinuität digitaler Identitätspolitik, die, ausgehend von der ersten Signaturgesetzgebung Mitte der 1990er Jahre, in drei Wellen verlief: Zunächst wurden die rechtlichen Grundlagen geschaffen, anschließend wurde versucht, im Rahmen sozialstaatlicher Reformen eine kritische Masse von digital adressierbaren Bürgern zu schaffen, um im dritten Schritt die internen und externen Kommunikationsprozesse auf digitale Dokumentenführung umzustellen. Alle drei Wellen sind jeweils deutlich hinter den hoch gesteckten Erwartungen zurückgeblieben und letztlich gescheitert. Dennoch werden noch vor Ablauf dieses Jahrzehnts die Bundesbürger digitale Adressen haben, die sie eventuell nicht nutzen,

54 Referentenentwurf des Gesetzes zur Förderung der elektronischen Verwaltung; Hervorhebung C.E. (in Verwahrung beim Autor).

55 Bundesministerium des Innern, Referat 02, Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, S. 25.

56 Bundesregierung, Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG).

57 Bundesministerium des Innern, Referat 02, Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften.

die aber als Funktion angelegt sind und mindestens mit der Gesundheitskarte systematisch in die Sozialstaatlichkeit eingebunden werden.

Hatte sich in den USA nach dem Ende der *Crypto-Wars* der Staat für beinahe 20 Jahre (zumindest öffentlich) nicht mehr für eine digitale Authentifikationsinfrastruktur engagiert, änderte sich dies 2011. Die von der Obama-Administration vorgestellte »Nationale Strategie für vertrauenswürdige Identitäten im Cyberspace« (National Strategy for Trusted Identities in Cyberspace – NSTIC) markiert dort den Beginn der dritten Phase und das Wiederauftreten des Staates als Akteur. In der NSTIC-Strategie wird Folgendes festgestellt:

> »Als Nation wollen wir viele der technischen und politischen Mängel angehen, die zu Unsicherheiten im Internet geführt haben. Zu diesen Mängeln gehört die Authentifizierung der Menschen und Geräte im Internet: Die Etablierung von vertrauenswürdigen Identitäten wurde im präsidialen Bericht zur Cyberspace-Politik als Eckpfeiler einer verbesserten Internetsicherheit festgestellt.«[58]

Die entscheidende Frage allerdings, was »vertrauenswürdige Identitäten« (*trusted identities*) sind und wie diese verfertigt werden, wird in der NSTIC-Strategie offengelassen. Anders als in Deutschland werden staatlich zugestellte digitale Signaturen nicht als unverzichtbare Formate digitaler Identitätsstiftung geführt. Stattdessen wird das Problem digitaler Authentifikation an die freie Wirtschaft delegiert: »Letztlich kann das ›Identitätsökosystem‹ nur von *privaten Unternehmen* entworfen und eingerichtet werden.«[59] Ganz den von den Identerati debattierten Konzepten entsprechend, soll das vom privaten Sektor zu entwickelnde »Identity Ecosystem« eine Vielzahl von Identitätssystemen fördern und deren Anwendung je nach Risikoklasse und -beurteilung zulassen:

> »Identitätsmedien sind in unterschiedlichen Formaten erhältlich, in mit Chips ausgestatteten Plastikkarten (*smartcards*), in den Sicherheitschips, die in Rechnern, Mobiltelefonen, Zertifikaten mit Informationsprogrammen oder USB-Geräten eingebaut sind. Die Auswahl der geeigneten Identitätsmedien und der Grad an Vertrauenswürdigkeit sind implementationsgebunden und hängen von der Risikotoleranz der Beteiligten ab.«[60]

Zugleich ist trotz des im Dokument mehrfach betonten Vertrauens in die Marktkräfte verschiedentlich von »wahren Identitäten« (*true identities*) die Rede. Dazu vermerken die Autoren in einer Fußnote: »Für eine Transaktion mit hoher Sicherheitsanforderung will man möglicherweise die wahre Identität wissen«. Was sich hinter dem empathischen Begriff der *true identity* verbirgt, bleibt im Unterschied zu anderen Aspekten im Glossar des NSTIC unbeantwortet. Offenkundig hat die in der NSTIC-Programmatik favorisierte marktliberale Pluralität der Identitätslösungen ihre Grenzen. Mit dem *New Deal* wurden vergleichsweise spät auch in den USA in den 1930er und 1940er Jahren die Geburtenregistratur des Personennamens und die auf eigenhändige Namensunterschrift rekurrierenden Formate der Identifikation

58 The White House, National Strategy for Trusted Identities in Cyberspace (NSTIC); Übersetzung C.E.

59 Ebd.; Hervorhebung C.E.

60 Ebd.

im Rechtsverkehr verpflichtend durchgesetzt. Das NSTIC-Dokument nimmt auf dieses Regime indirekt Bezug, indem es Folgendes erklärt:

> »Die Strategie befasst sich nicht explizit mit Identitäts- und Vertrauensfragen in der Welt außerhalb des Internets; dennoch sollen und können die Lösungen der Identitätsfrage in und außerhalb des Internets sich gegenseitig ergänzen. Identitätsbeweis (Verifizierung der Identität eines Individuums) und die Qualität der Identitätsquelldokumente haben eine tiefgehende Bedeutung für die Etablierung vertrauenswürdiger digitaler Identitäten. Die Strategie schreibt nicht vor, wie diese Prozesse und Dokumente sich weiterentwickeln müssen.«[61]

Wohl enthält sich die NSTIC-Strategie hier konkreter Vorschriften, aber »Identitätsquelldokumente« (*identity source documents*) der »offline-world« werden auch in den USA faktisch staatlicherseits bereitgestellt. Die in der NSTIC-Strategie vordergründige Rhetorik gegen ein staatlich basiertes digitales Identitätsregime ist mithin in dreifacher Hinsicht kritisch zu betrachten: Erstens tritt der Staat hier als Moderator und Finanzier der Entwicklung digitaler Identitätsdokumente auf, zweitens legt die Formulierung »need to evolve« nahe, dass sich genuin staatliche Identitätsdokumente mit dieser Entwicklung verändern werden. Drittens ist es unwahrscheinlich, dass sich die amerikanische Staatlichkeit von der Aufgabe der Bereitstellung der »identity source documents« zurückziehen wird.[62] Das »identity proofing« und die »high-quality«-Quellen-Dokumente der Offline-Welt basieren – wie in Europa – auf einer staatlich regulierten und rechtsbewehrten Kette wechselseitig aufeinander verweisender Signifikationen in Geburtsurkunden, Ausweisen und Registern. Der wesentliche Unterschied zu den in deutschen und europäischen Diskursen diskutierten Modellen besteht in einem größeren Laissez-Faire bezüglich der Klassifizierung von als besonders absicherungswürdig geltenden Transaktionen. Während insbesondere im deutschen Diskurs für quasi jeden Kontakt zwischen einem Individuum und einer Behörde ein rechtswirksamer Nachweis der Identität erforderlich ist, ist dieser in US-amerikanischen Kontexten nur in wenigen, als besonders sicherheitsrelevant eingestuften Anwendungsfällen vorgesehen.

4. Fazit

Wie in der Einleitung angemerkt, steht mindestens für den medienwissenschaftlichen Diskurs die Klärung der pfadspezifischen Hintergründe dieser eklatanten Differenzen zwischen der deutschen und den angelsächsischen Kulturen von Personaldokumenten aus. Gemeinsam ist den geschilderten deutschen und US-amerikanischen Projekten, dass sie ihre Bevölkerungen mit Adressen auszustatten suchen, die diese sowohl für staatliche Stellen adressierbar machen als auch den Individuen zur wechselseitigen Adressierung dienen können. Letzteres ist einer der wesentlichen Unterschiede zu den inzwischen bekannt gewordenen, im geheimen betriebenen Überwachungs- und Identifikationsprojekten. Wie die von Edward Snowden vorgelegten Dokumente zeigen, fanden insbesondere nach dem 11. September 2001 umfangreiche Bemühungen statt, eine Adressierung von Individuen

61 Ebd.

62 Vgl. Jens Schröters Argumentation zum medialen Monopol des Staates: Schröter 2014.

mittels Graphenanalysen[63] einerseits, auf Metadatenbasis generierter Verhaltenssignaturen[64] andererseits durchzuführen. Deren Gegenstand ist aber zunächst weniger die eigene Bevölkerung, sondern sind primär Menschen aus anderen Ländern. Auch bleiben die hier entwickelten Verfahren einem exklusiven Kreis innerhalb des staatlichen Institutionsgefüges vorbehalten und stehen nicht als Mittel der wechselseitigen Authentifizierung durch die Nutzer zur Verfügung. Inwieweit die Metadatensammlung eine mangels anderer Möglichkeiten notwendige Substitutionsfunktion zur Adressierung von Menschen und Dingen im Internet darstellt oder ob solche aus Metadaten gewonnenen Verhaltenssignaturen vielleicht irgendwann digitale Signaturen als an Papieranalogien ausgebildete Adressierungsformate ablösen, muss hier offenbleiben. Juristisch jedenfalls ist sowohl in den USA als auch in Deutschland – und im weiteren Sinne in ganz Europa – nur eine digitale Signatur rechtlich voll belastbar. Eine über Metadaten aggregierte Adresse, die ein Individuum ausweisen soll, fände dagegen vor einem öffentlichen Gericht keine Anerkennung. Dass das vor Geheimgerichten, die über Drohnenschläge befinden, anders ist, ist sowohl Teil des Phänomens der Gewaltförmigkeit der Staatenkonkurrenz als auch Teil der spätestens seit 9/11 zu beobachtenden und von Giorgio Agamben und anderen skandalisierten Verkehrungen des liberalen Rechts.[65] Die rechtliche Anerkennung von über Metadaten gestifteten Adressen würde aber gegenüber dem historisch entstandenen System eine signifikante Verschiebung bedeuten. Zum einem würden an die Stelle von Registern im Sinne von Dokumenten dann Lebensvollzüge registrierende Register treten, die »patterns of living« als Verhaltenssignaturen anschreiben und als Ausweise anbieten. Damit wäre zum anderen aus einem aktiven Sich-Ausweisen quasi ein passives Ausweis-Sein geworden. Das Problem der Authentifikation würde jedoch abermals darin liegen, die Gültigkeit der Beziehung zwischen diesen Registereinträgen und den sie adressierenden Individuen stabil und nachweisbar zu halten.

In der Kulturtechnik des Registers liegt damit eine seltsame, über den geschilderten Medienbruch hinwegreichende und historisch lange Kontinuität vor: »Herrschaft wird souverän dank ihrer Register«,[66] schrieb Cornelia Vismann über den Beginn frühmoderner Staatlichkeit, und ein solches Souveränitätsbegehren findet Ausdruck in den auf beiden Seiten des Atlantiks zu beobachtenden Versuchen, staatliche Register für digitale Identitätsregime zu schaffen. So groß die Unterschiede der Einsatzszenarien zwischen Deutschland und den USA auch sind, die Adressen der Menschen werden über die Stiftung von Relationen von Individuen zugeordneten Daten zu Registereinträgen gestellt. War es im papierbasierten System das Verhältnis zwischen Dokument und Registereintrag, das diese Relation ergab, so ist es unter digitalen Bedingungen eine kryptographische Beziehung zwischen Daten. Die souveränitätsrelevante Frage ist, wer diese Relation herstellen und speichern und ver-

63 Engemann 2014, S. 219 ff.

64 Vgl. Risen, Poitras 2014.

65 Vgl. Agamben 2005. Vgl. auch Opitz' Diskussion der Unperson: Opitz 2012, S. 139 ff.

66 Vismann 2000, S. 136.

arbeiten kann. Historisch ist dies die Staatlichkeit gewesen, die hier gebildet hat, was Jens Schröter ein »mediales Monopol« nennt: »[S]elbst die demokratischsten Staaten üben eine strenge Kontrolle über ebenso alltägliche, aber in der Regel viel weniger beachtete Massenmedien aus – nämlich über die Urkundenmedien von Banknoten, Identitäts- und anderen wichtigen Dokumenten«.[67] Mindestens für die letzten 20 Jahre zeigt sich, dass die Staatlichkeit auch unter digitalen Bedingungen dieses Privileg keineswegs aufzugeben gedenkt. Im Gegenteil ist es mindestens der US-amerikanischen Staatlichkeit inzwischen gelungen, sowohl die Privatwirtschaft als auch Teile der ehemals staatskritischen kryptographischen Hacker für ihr Projekt zu kooptieren. Dabei sind die Eskalation des Medienwissens und Medienhandels und das Herbeiführen von Konstellationen, in denen die Akteure nach der Relevanz dieses Wissens für die Organisation von Gesellschaft und Staat fragen können und sollen, offenkundig. Im Vergleich zu den 1990er Jahren und dem *Clipper-Chip* ist mit dem NSTIC-Prozess also eine Dezentralisierung und De-Institutionalisierung zu beobachten, die zugleich aber eine Zuarbeit zur Kontinuierung der Staatlichkeit unter digitalen Bedingungen zu stiften sucht. In Deutschland sind es der Chaos Computer Club und die re:publika-Konferenz, die diese Diskurse betreiben und an den Staat herantragen. Für die kurze Zeit ihrer politischen Relevanz galt das ebenso für die Piratenpartei, die mit ihren Slogan »Für dieses System ist ein Update verfügbar« Aushandlungsansprüche bezüglich der richtigen Medialität der Staatlichkeit anmeldete. Digitale Identitätslösungen sind ein zentraler Schauplatz einer solchen Gouvernemedialisierung[68] der Gouvernementalitität, indem die Medialität der Staatlichkeit problematisch wird, es aber zugleich auch zur Herbeiführung von deren Neuaushandlung und -implementierung kommt. Für Kittler stand noch 2010 fest, »dass der Staat erst mit der Schrift entstanden ist und mit ihr zugrunde geht: nämlich an der weltweiten Digitalisierung aller Daten, Akten, Bilder und Klänge«.[69] Hoffnungen auf das Absterben der Staatlichkeit haben sich bislang selten erfüllt, und Kittlers zuversichtlichem »Dem Staat schlägt seine Todesstunde also jetzt«[70] muss wohl entgegengehalten werden, dass es wieder einmal an der Zeit ist zu fragen, was »dem Staat das Überleben ermöglicht hat«.[71] Vielleicht war es kein Zufall, dass einer Medienwissenschaft just zu dem Zeitpunkt eine Institutionalisierung widerfuhr, als Medien zu einem Problem der Regierungskunst werden mussten.

67 Schröter 2014, S. 9.

68 Vgl. den Introtext in Engemann, Traue 2006; Engemann 2012 a; Traue 2010, S. 269 f.

69 Kittler 2012, S. 47.

70 Ebd.

71 Foucault 2004, S. 164.

Literatur

Agamben, Giorgio 2005. *State of exception*. Chicago, London: University of Chicago Press.

Borchers, Detlef 2007. *Elektronische Gesundheitskarte: Von der Wiege bis zur Bahre*. www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Von-der-Wiege-bis-zur-Bahre-168062.html (Zugriff vom 20.06.2014).

Borchers, Detlef 2013 a. *Der ePerso hat Geburtstag: Drei Jahre neuer Personalausweis*. www.heise.de/newsticker/meldung/Der-ePerso-hat-Geburtstag-Drei-Jahre-neuer-Personalausweis-2037387.html (Zugriff vom 12.05.2014).

Borchers, Detlef 2013 b. *Gesundheitskarte: Arvato baut telematische Infrastruktur für Gematik*. www.heise.de/newsticker/meldung/Gesundheitskarte-Arvato-baut-telematische-Infrastruktur-fuer-Gematik-2057396.html (Zugriff vom 02.12.2013).

Brin, David 1998. *The transparent society. Will technology force us to choose between privacy and freedom?* New York: Basic Books.

Cameron, Kim 2006. *Introduction to the laws of identity*. www.identityblog.com/?page_id=354 (Zugriff vom 20.06.2014).

Castells, Manuel 2001. *Das Informationszeitalter: Wirtschaft – Gesellschaft – Kultur*. Opladen: Leske + Budrich.

Castells, Manuel 2004. *The network society*. Cheltenham: Edward Elgar.

David, Paul 1985. »Clio and the economics of QWERTY«, in *American Economic Review* 75, 2, S. 332-337.

Derrida, Jacques 2005. *Paper maschine*. Stanford: Stanford University Press.

Engemann, Christoph 2011. »Im Namen des Staates: Der elektronische Personalausweis und die Medien der Regierungskunst«, in *Zeitschrift für Medien- und Kulturforschung* 2, S. 211-228.

Engemann, Christoph 2012 a. »Write me down make me real. Zur Gouvernemedialität der digitalen Identität«, in *Quoten, Kurven und Profile – Zur Vermessung der Gesellschaft*, hrsg. v. Passoth, Jan-Hendrik; Wehner, Josef, S. 205-230. Wiesbaden: VS Verlag für Sozialwissenschaften.

Engemann, Christoph 2012 b. »Elektronische Gesundheitsakte oder Fallakten – Medizinische Archivmacht und die elektronische Gesundheitskarte«, in *Qualität in der Medizin dynamisch denken: Versorgung – Forschung – Markt*, hrsg. v. Kray, Ralph; Koch, Christoph; Sawicki, Peter, T., S. 149-175. Berlin, Heidelberg: Springer.

Engemann, Christoph 2014. »Human terrain system: Soziale Netzwerke und die Medien militärischer Anthropologie«, in *Soziale Massen – Neue Medien*, hrsg. v. Baxmann, Inge; Beyes, Timon; Pias, Claus, S. 205-230. Berlin, Zürich: Diaphanes.

Engemann, Christoph; Traue, Boris 2006. *Governmediality of the life course*. www.governmediality.net (Zugriff vom 12.12.2010).

Foucault, Michel 1999. *In Verteidigung der Gesellschaft. Vorlesungen am Collège de France (1975-76)*. Frankfurt a. M.: Suhrkamp.

Foucault, Michel 2004. *Geschichte der Gouvernementalität I. Sicherheit, Territorium, Bevölkerung. Vorlesung vom 1. Februar 1978*. Frankfurt a. M.: Suhrkamp.

Hagen, Wolfgang 2005. *Das Radio. Zur Geschichte und Theorie des Hörfunks – Deutschland/USA*. München: Wilhelm Fink.

Hamlin, Kaliya 2006. *Identerati by Mark Dixon*. www.identitywoman.net/identerati-by-mark-dixon (Zugriff vom 12.05.2014).

Hornung, Gerrit 2005. *Die digitale Identität*. Baden-Baden: Nomos.

Hughes, Eric 1993. *A cypherpunk's manifesto*. www.activism.net/cypherpunk/manifesto.html (Zugriff vom 20.06.2014).

Kahn, David 1996. *Codebreakers. The story of secret writing*. New York: Scribner.

Kittler, Friedrich A. 2012. »And the gods made love. Zum Tode von Cornelia Vismann«, in *Das Schöne am Recht*, hrsg. v. Hamacher, Werner; Kittler, Friedrich A., S. 43-48. Berlin: Merve.

Levy, Steven 1994. »Battle of the clipper chip«, in *The New York Times* vom 12. Juni 1994. www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html (Zugriff vom 10.05.2014).

Levy, Steven 2001. *Crypto. How the code rebels beat the government, saving privacy in the digital age*. New York: Penguin.

Lovink, Geert 2014. *Hermes on the Hudson: notes on media theory after Snowden*. e-flux. www.e-flux.com/journal/hermes-on-the-hudson-notes-on-media-theory-after-snowden/ (Zugriff vom 04.04.2014).

Maizière, Thomas de 2010. *14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft*. https://netzpolitik.org/2010/14-thesen-zu-den-grundlagen-einer-gemeinsamen-netzpolitik-der-zukunft/ (Zugriff vom 23.06.2014).

May, Timothy C. 1994. *The cyphernomicon: cypherpunks FAQ and more*. www.swiss.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ (Zugriff vom 20.06.2014).

Muhle, Maria 2008. *Eine Genealogie der Biopolitik. Zum Begriff des Lebens bei Foucault und Canguilhem*. Bielefeld: Wilhelm Fink.

Müller, Lothar 2012. *Weiße Magie. Die Epoche des Papiers*. München: Carl Hanser.

Neymann, Harald 2001. *Verschlüsselung im Internet. Probleme der politischen Regulierung in den USA und der Bundesrepublik Deutschland*. Frankfurt a. M., New York: Campus.

North, Douglas C. 1990. *Institutions, institutional change, and economic performance*. Cambridge: Cambridge University Press.

Opitz, Sven 2012. *An der Grenze des Rechts. Inklusion/Exklusion im Zeichen der Sicherheit*. Weilerswist: Velbrück Wissenschaft.

Pierson, Paul 2005. *Politics in time: history, institutions, and social analysis*. Princeton: Princeton University Press.

Risen, James; Poitras, Laura 2014. »N.S.A. collecting millions of images, faces from web«, in *The New York Times* vom 31. Mai 2014. www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (Zugriff vom 01.06.2014).

Sassen, Saskia 2000. »Digital networks and the state. Some governance questions«, in *Theory, Culture & Society* 17, 4, S. 19-33.

Sassen, Saskia 2008. *Territory, authority, rights: from medieval to global assemblages*. Updated edition. Princeton: Princeton University Press.

Schmidgen, Henning 2013. »Eine originale Syntax. Psychoanalyse, Diskursanalyse und Wissenschaftsgeschichte«, in *Mediengeschichte nach Friedrich Kittler. Archiv für Mediengeschichte*, Sonderheft 13, hrsg. v. Balke, Friedrich; Siegert, Bernhard; Vogl, Joseph, S. 27-43. Paderborn: Wilhelm Fink.

Schneier, Bruce; Banisar, David 1997. *The electronic privacy papers. Documents on the battle for privacy in the age of surveillance*. New York: John Wiley & Sons.

Schröter, Jens 2014. *Das mediale Monopol des Staates und seine Verteidigungslinien*. Preprint vom 23. Juni 2014. http://uni-siegen.academia.edu/JensSchr%C3%B6ter (Zugriff vom 12.01.2015).

Schulte, Martin 2003. *Handbuch des Technikrechts*. Berlin, Heidelberg, New York: Springer.

Scott, James C. 1998. *Seeing like a state. How certain schemes to improve the human condition have failed*. New Haven: Yale University Press.

Sterling, Bruce 1992. *The hacker crackdown. Law and disorder on the electronic frontier*. London: Penguin.

Swan, Melanie 2009. »Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking«, in *International Journal of Environmental Research and Public Health* 6, S. 492-525.

Topol, Eric 2012. *The creative destruction of medicine. How the digital revolution will create better healthcare*. New York: Basic Books.

Torpey, John 1998. »Coming and going: on the state monopolization of the legitimate ›means of movement‹«, in *Sociological Theory* 16, 3, S. 239-259.

Traue, Boris 2010. *Das Subjekt der Beratung. Zur Soziologie einer Psycho-Technik*. Bielefeld: transcript.

Vismann, Cornelia 2000. *Akten – Medientechnik und Recht*. Frankfurt a. M.: Fischer.

Winthrop-Young, Geoffrey 2012. »Hunting a whale of a state: Kittler and his terrorists«, in *Cultural Politics* 8, 3, S. 399-412.

Zusammenfassung: Nationalstaaten haben ihre Populationen mit Personaldokumenten ausgestattet und die Bürger sowohl für sich als auch wechselseitig adressierbar gemacht. Mit der wachsenden Bedeutung des Internets werden diese auf Papier basierenden Systeme zunehmend dysfunktional, und Nationalstaaten versuchen, an ihrer Stelle digitale Authentifikationsmechanismen zu etablieren. Sowohl die USA als auch die Bundesrepublik Deutschland weisen eine inzwischen 20-jährige Geschichte weitgehend gescheiterter Versuche der Einführung offizieller digitaler Identitäten auf. Im Vergleich beider Länder zeigen sich unterschiedliche Ansätze, diesen Medienwandel der Staatlichkeit zu organisieren und zu regulieren. Während die Obama-Administration in den USA eine marktbasierte Lösung des Anonymitäts- und Identitätsproblems im Internet vorantreibt, wird dieses in Deutschland als genuin hoheitliches Problem behandelt.

Stichworte: Anonymität, Personaldokumente, digitaler Wandel, Medialität der Staatlichkeit, Vergleich USA-Deutschland, *Crypto-Wars*

Germany, the USA and digital identity systems

Summary: Nation states have addressed the populace via paper-based authentication media. With the advent of the Internet such personal documents are becoming dysfunctional. Since at least twenty years nation states have attempted to introduce official digital identity systems to address their citizen as well as for reciprocal communications. A comparison of Germany and USA illustrates the different approaches for managing and regulating this media change. While in the USA the Obama administration favors a market-based approach, the German government is pursuing a long-term state-based process and deems the solution of anonymity and identity on the Internet as a governmental problem.

Keywords: anonymity, identification documents, digital change, mediality of statehood, US-German comparison, crypto wars

Autor

Christoph Engemann
Wissenschaftlicher Mitarbeiter
DFG-Kollegforschergruppe
Medienkulturen der Computersimulation
Leuphana Universität Lüneburg
Wallstraße 3
21335 Lüneburg
http://mecs.leuphana.de/