Im Namen des Staates

Der elektronische Personalausweis und die Medien der Regierungskunst

Christoph Engemann

Am 1. November 2010 begann die in Berlin ansässige Bundesdruckerei mit der Auslieferung des elektronischen Personalausweises, den jährlich etwa acht Millionen Bürger in Deutschland erhalten werden. Neben den aufgedruckten persönlichen Identifikationsdaten enthält dieser Ausweis einen Chip, der die Identifikation im Internet erlauben soll. Ein Teil der zugehörigen Software, die *AusweisApp*,[1] wurde zwar prompt kompromittiert,[2] gleichwohl bedeutet der elektronische Personalausweis eine Zäsur in der Geschichte des Regierens, wird doch die Bevölkerung der Bundesrepublik digital und über das Internet adressierbar.

Die Ausgabe dieses Ausweises setzt die Individuen digital in Kontakt mit einer staatlichen Institution, die wie keine andere das tägliche Handeln begleitet. In Deutschland sind ihre Produkte überall dort zur Hand, wo Transaktionen in den Stand der Legalität erhoben werden: Banknoten beim Warentausch, Ausweispapiere bei Reisen, Bankgeschäfte, Anmeldungen, beim Bezug von Sozial- oder anderen Transferleistungen, Briefmarken beim Postversand, Zollmarken beim Kauf von Tabak und Alkoholika. Auf Initiative des Generalpostmeisters und späteren Initiators des Weltpostvereins Heinrich von Stephan 1879 als Reichsdruckerei in Berlin gegründet, war die Aufgabe dieser Institution der Druck solcher Medien, deren Form, Gestaltung und Ausgabe mit ihrer Gründung vom Deutschen Reich sukzessive monopolisiert wurden: Geldscheine, Reisepässe und Briefmarken. Hinzu kamen Patentschriften, bestimmte staatlich ausgestellte Urkunden, aber auch Adelsbriefe und Festschriften. Weiterhin fiel in ihren Zuständigkeitsbereich die Herstellung von Druckerzeugnissen, »deren Verbreitung wissenschaftliche oder kunstinteressen wesentlich zu fördern geeignet ist«.[3] Ebenfalls unter den

1 Bundesamt für Sicherheit in der Informationstechnik: Der neue Personalausweis – Startseite AusweisApp-Portal, unter: https://www.ausweisapp.bund.de (15. 12. 2010).

2 Vgl. heise online: Neuer Personalausweis: AusweisApp mit Lücken [2. Update], unter: http://www.heise.de/newsticker/meldung/Neuer-Personalausweis-AusweisApp-mit-Luecken-2-Update-1133376.html (30. 11. 2010).

3 Direktion der Reichsdruckerei: Die Reichsdruckerei in Berlin. Eine kurze Darstellung ihres Werdens und Wirkens, Berlin 1928, S. 9f.

Produkten der Reichsdruckerei befand sich ein Register, das den Gebrauch eines neuen Mediums ermöglichte: *Verzeichnis der bei der Fernsprecheinrichtung Beteiligten*. Das erste Berliner Telefonbuch erschien 1881 und damit zwei Jahre nach der Gründung der Reichsdruckerei.[4] Schließlich kam auch die Bismarcksche Sozialgesetzgebung nicht ohne Medien der Reichsdruckerei aus. Als *Klebegesetz* verballhornt beruhte das Herzstück der Arbeiterversicherung, das *Invaliditäts- und Altersversicherungsgesetz* von 1889, auf dem regelmäßigen Einkleben von Versicherungsmarken auf den zugehörigen Quittungskarten.[5]

Innerhalb des staatlichen Ensembles von Medien besetzt eine solche Druckerei offenbar eine besondere Position. Denn deren Produkte tragen die Zeichen des Staates und gewähren ihren Nutzern dadurch Zugang zu den Garantien und Schutzleistungen der Staatlichkeit. Evident wird diese Beziehung anhand der Signaturen, die auf allen Dokumenten der Reichsdruckerei wie auch ihrer Nachfolgeinstitution Bundesdruckerei zu finden sind.

In einem kurzen Text mit dem Titel *Signatura Rerum*[6] erinnerte Giorgio Agamben unlängst daran, dass eine Theorie derselben noch aussteht, modifizieren sie doch die Beziehungen zwischen Dingen und Akteuren und schreiben diese in ein Netzwerk der Autorität ein. Agamben erweitert dabei im Gegensatz zu Jacques Derrida[7] den Begriff der Signatur über die eigenhändige Namensunterschrift hinaus. Die Signatur bezeichnet nicht allein die *Quelle* einer schriftlichen Utterance und damit die paradoxe Figur des Ausweises eines Ereignisses und dessen Wiederholbarkeit. Vielmehr interessiert Agamben sich für die spezielle Beziehung der Signatur zur Macht. Jedes Ding kann eine Signatur tragen, und manche Medien versuchen selbst, eine Signatur zu sein. Beim Papiergeld stellt das Produkt durch seine Komposition im Zusammenwirken von Papier, Farben, Druckverfahren, dem Design, Wasserzeichen und den Seriennummern eine Signatur dar. Signaturen verweisen auf die ausstellende Autorität und evozieren eine Beziehung des signierten Mediums mit dieser Autorität, eine Beziehung, die so lange gleichsam virtuell bleibt, bis der Verdacht, dass das fragliche Medium – Geld, ein Pass, ein Patent, etc. – gefälscht ist, die Interaktionen kontaminiert. Solche Irritationen führen zur Realisierung der Beziehung zwischen den Signaturen und den Registern der ausstellenden Instanzen. Die Staatlichkeit, über die Signatur in das Material des in Frage stehenden Dokuments eingeschrieben, tritt dann mit einem Arsenal der Forensik auf, um in einer Prüfung Echtheit und Legitimität zu klären. Va-

4 Vgl. Gerd Gnewuch: 100 Jahre Bundesdruckerei, Berlin 1979, S. 143.

5 Vgl. ebd. S. 127.

6 Giorgio Agamben: Signatura Rerum. Über die Methode, Frankfurt/M. 2009.

7 Jacques Derrida: Signatur, Ereignis, Kontext, in: ders.: Randgänge der Philosophie, Wien 1988, S. 291–314, hier: S. 312. Siehe auch: ders.: Über das »Preislose« oder The price is right in der Transaktion, Berlin 1999, S. 25.

lentin Groebner hat in seiner Arbeit zur Geschichte der Personalpapiere gezeigt, dass Identität durch Vervielfältigung generiert wird.[8] Identität bezieht sich hier auf stabile und legale Identitäten von Menschen, von Bürgern und Nicht-Bürgern, deren Papiere jeweils dann den Status der Legalität haben, wenn sich eine Kopie in den Registern des Staates befindet. Dies gilt auch für andere Papiere, die von staatlichen Institutionen ausgegeben werden: Banknoten, Patente, Fahrzeugscheine oder Approbationen, die ebenfalls nur dann gültig sind, wenn ein Eintrag ihrer Existenz in staatlichen Registern vorliegt. Bei Banknoten verweisen Seriennummern sowie bestimmte Drucktechniken und Tinten auf das jeweilige Fertigungslos. Jede kommerzielle Transaktion, jede administrative Interaktion im Kontext derartiger staatlicher Medienproduktion ist durch das Potential gekennzeichnet, die Autoritäten zu evozieren, um die Validität ihrer Dokumente, nämlich ihre Signaturen, zu prüfen.

1. Regierungskunst elektronisch

Exakt im Jahr 2000 und auf dem Höhepunkt des *dot.com*-Booms legten Jörn von Lucke und Heinrich Reinermann, zwei deutsche Verwaltungswissenschaftler, ihre *Speyerer Definition von Electronic Government* vor. Auf acht knappen Seiten formulieren die Autoren Begriffe für das staatliche Verwalten unter digitalen Bedingungen, die bis heute in den Programmen, technischen Lastenheften und Standardisierungskatalogen der federführenden Ministerien und Behörden prominent sind: »Unter Electronic Government verstehen wir die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.«[9] Diese Definition des Electronic Government fasst selbiges keineswegs als lediglich verwaltungsinterne Technologiereform. Nach von Lucke und Reinermann greift das Electronic Government auf die gesamte Gesellschaft aus: »Bei Electronic Government geht es sowohl um Prozesse innerhalb des öffentlichen Sektors (G2G), als auch um jene zwischen diesem und der Bevölkerung (C2G und G2C) der Wirtschaft (B2G und G2B) und den Non-Profit und Non-Government Organisationen des Dritten Sektors (N2G und G2N).«[10]

Die Abkürzungen entsprechen der aus dem angelsächsischen Raum übernommenen Konvention, Government mit »G«, Business mit »B«, Citizen mit »C«,

8 Vgl. Valentin Groebner: Der Schein der Person – Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, München 2004.

9 Jörn von Lucke/Heinrich Reinermann: Speyerer Definition von Electronic Government, unter: http://foev.dhv-speyer.de/ruvii (11. 12. 2010).

10 Ebd.

schließlich NPO/NGO mit »N« zu bezeichnen und für das »to« eine 2 einzusetzen. In einer zugehörigen Grafik zeigen von Lucke und Reinermann, wie Electronic Government alle gesellschaftlichen Bereiche vermitteln soll:

E-Government	Bevölkerung Bürger	Staat Verwaltung	Zweiter Sektor Wirtschaft	Dritter Sektor NPO/NGO
Bevölkerung Bürger	C2C	C2G	C2B	C2N
Staat Verwaltung	G2C	G2G	G2B	G2N
Zweiter Sektor Wirtschaft	B2C	B2G	B2B	B2N
Dritter Sektor NPO/NGO	N2C	N2G	N2B	N2N

Speyerer Definition (2000): Electronic Government im gesellschaftlichen Beziehungsgeflecht[11]

Neben der Totalität des Electronic Government wird zudem das wesentliche Potential dieser Prozesse in ihrer Macht verortet, die Qualität und Intensität dieser Beziehungen tiefgreifend zu transformieren. Im schönsten Klartext werden Medien als Apriori dieser Entwicklung ausgemacht: »Electronic Government hebt sich in charakteristischer Weise von herkömmlichen EDV- Anwendungen dadurch ab, dass die medienbedingte ›Neue Erreichbarkeit‹ von Personen, Abläufen, Daten und Objekten als den wesentlichsten Bestimmungsgrößen des Verwaltungshandelns für grenzüberschreitende Lösungen genutzt wird.«[12] Unter digitalen Bedingungen wird Verwaltung also *grenzüberschreitend* und stellt eine sogleich als Substantiv angeführte *Neue Erreichbarkeit* her, denen Menschen wie Dinge unterliegen sollen:

»Nie zuvor war ein Kontakt mit Personen, etwa mittels E-Mail oder Videokonferenz, unabhängig von Aufenthaltsort, Uhrzeit oder Hierarchiestufe so wirksam herzustellen. Nie zuvor ließen sich Daten irgendwo auf der Welt so effizient abrufen oder fortschreiben. Nie zuvor konnten programmierte Abläufe irgendwelcher Institutionen so lückenlos zusammengefügt werden. Und nie zuvor ließen sich mit Computerchips ausgestattete Objekte grenzüberschreitend in Netze für Facility Management und Anlagensteuerung einbinden. […].«[13]

11 Ebd. S. 5.
12 Ebd. S. 2.
13 Ebd. S. 6.

Schließlich illustrieren von Lucke und Reinermann ihre »Neue Erreichbarkeit wichtiger Bestimmungsgrößen des Verwaltungshandelns«[14] mittels einer Tabelle als eine Totalität der möglichen Beziehungen zwischen Menschen, Abläufen, Daten und Objekten:

Erreichbarkeit	Menschen	Abläufe	Daten	Objekte
Menschen	M2M	M2A	M2D	M2O
Abläufe	A2M	A2A	A2D	A2O
Daten	D2M	D2A	D2D	D2O
Objekte	O2M	O2A	O2D	O2O

Speyerer Definition (2000): Neue Erreichbarkeit wichtiger Bestimmungsgrößen des Verwaltungshandelns[15]

In der Speyerer Definition von Electronic Government werden somit die Medien selbst als Problem der Regierung thematisch. Die lange Periode vom 16. bis zum 20. Jahrhundert, in der Staaten die Menschen und die Dinge mittels Papier speicherten, prozessierten und übertrugen, geht an der Schwelle zum 21. Jahrhundert endgültig zu Ende.[16] Wo der Papierkrieg staatlicher Verwaltung verschwindet und digitale Medien an dessen Stelle treten, kollabieren im Universalmedium Computer nicht allein Text, Film und Ton; in den Imaginationen der Speyerer Verwaltungswissenschaftler werden alle Dinge universell verwaltbar, weil sie digital und damit erreichbar sind. Der Medienwandel hin zur Digitalität ist damit zugleich die Möglichkeit und die Herausforderung einer neuen Regierungskunst,

14 Ebd.

15 Ebd. S. 5.

16 Frank Nullmeier hat gezeigt, dass in den 1990er Jahren nur wenige Verwaltungswissenschaftler an der Rolle der Informationstechnik für die öffentliche Verwaltung interessiert waren. Vgl. Frank Nullmeier: Zwischen Informatisierung und Neuem Steuerungsmodell, in: Politische Vierteljahreszeitschrift 41 (2000), S. 248–266, hier: S. 250f. Bis heute ist die Mediengeschichte der Verwaltung weitgehend ungeschrieben. Dabei werden im verwaltungswissenschaftlichen Diskurs Medienentwicklung und Verwaltungsreformen durchaus enggeführt. Vgl. Hans Brinckmann/Stefan Kuhlmann: Computerbürokratie – Ergebnisse von 30 Jahren öffentlicher Verwaltung mit Informationstechnik, Opladen 1990, S. 20f. Vgl. auch: Martin Hagen: E-Government und Change Management an Beispielen aus Bremen, unter: mediakomm.difu.de/content/kongress/nuernberg/referentenhagen/textbeitrag.pdf (20. 12. 2010); Cornelia Vismann: Akten. Medientechnik und Recht, Frankfurt/M. 2000, S. 303–305; Claus Pias: Der Auftrag. Kybernetik und Revolution in Chile, in: Daniel Gethmann/Markus Stauff (Hg.): Politiken der Medien, Zürich/Berlin 2005, S. 131–154.

insofern die *Neue Erreichbarkeit* das Potential hat, hergebrachte institutionelle Grenzen zu verschieben, zu überschreiten oder abzuschaffen. Das unter Bedingungen von papiergestützter Datenverarbeitung von Beamten und Sekretären betriebene Schreiben in Sachen des Staates soll sich von den Gemäuern der Institutionen lösen und *in actu* überall stattfinden können, wo die Menschen und die Dinge sind.

Es ist nicht nur eine kleine Anzahl von Verwaltungswissenschaftlern, die solche Visionen propagiert. Sowohl auf Seiten der Politik, die auf Bundesebene seit 1998 die Informatisierung der Verwaltung maßgeblich betrieb, wie auch von Seiten der Privatwirtschaft, die im Electronic Government einen neuen und lukrativen Markt sah, wurden hohe Erwartungen formuliert. Die berufsständische Vereinigung der deutschen Elektrotechniker, der Verband der Elektrotechnik, Elektronik und Informationstechnik VDE, publizierte wenige Monate nach der Speyerer Definition ihr Memorandum *Electronic Government als Schlüssel zur Modernisierung.*[17] Scheinbar neutral heißt es hier zunächst: »Unter Electronic Government wird im Folgenden verstanden, die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung und der Leistungserstellung in Politik, Staat und Verwaltung unter sehr intensiver Nutzung der Informationstechnik.«[18] Doch ebenso wie die Speyerer Definition ist Electronic Government nicht einfach das *Nutzen von Informationstechnik*, sondern wird als zugleich transformative und totale Entwicklung begriffen:

»[…] es geht jetzt um mehr als bloß um eine neue Anwendungsgeneration in der Entwicklung der Informationstechnik. Moderne Kommunikationsnetze wie Internet, Intranets und Extranets schaffen eine neue Realität […] Sie ergreift gleichsam das ganze Geschäft: die »Machinery of Government« stellt sich anders dar, wenn die Informations-(und Kommunikations-)Technik nicht nur einzelne Informationssammlungen oder Entscheidungsprozesse beeinflusst, sondern sich auf den Zusammenhang aller Aktivitäten über räumliche, zeitliche und organisatorische Grenzen hinweg auswirkt.«[19]

Diese Überschreitungsrhetorik ist charakteristisch für den Electronic Government-Diskurs und findet sich in den offiziellen Programmatiken ebenso wie in den Unmengen an grauer Literatur, die von Ministerien, Behörenden, Initiativen, Lobbyvereinigungen und der Industrie herausgeben werden. In der Speyerer Definition heißt es dazu:

17 VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V: Electronic Government als Schlüssel zur Modernisierung von Staat und Verwaltung, unter: http://www.vde.com/de/fg/ITG/Publikationen/Studien-Reports/Documents/electronic.pdf (27. 05. 2009).

18 Ebd. S. 3.

19 Ebd.

»Die ›Neue Erreichbarkeit von Personen, Abläufen, Daten und Objekten‹ bewirkt somit eine ›Neue Gestaltbarkeit gerade der grenzüberschreitenden Beziehungen‹ […] Sie lässt sich für Electronic Government nutzen, indem bei der Abbildung dieser Beziehungen auf den Informationsraum (den sogenannten Cyberspace) eine ›virtuelle Verwaltung‹ entwickelt wird, die vorgefundene institutionelle Abgrenzungen überwindet und damit Mehrwerte im Sinne heute mit Verwaltungshandeln verbundener Ziele bewirken kann.«[20]

Was hier als *Neue Erreichbarkeit* im Sinne einer Steigerung der räumlichen und zeitlichen Verfügbarkeit der Individuen und der Objekte und Abläufe vorausgesetzt wird, ist ihre Adressierbarkeit im digitalen Medium. Ist diese im Realraum zumindest für Menschen durchgesetzt, die Personenamen tragen müssen und zudem in Deutschland über ihre Meldeadresse erreichbar sind, so besteht sie im Internet nicht.

2. Drei Interaktionsformen des Electronic Government

In der Speyerer Definition findet sich außerdem eine Differenzierung in drei Interaktionsformen steigender Komplexität, die in den offiziellen Diskurs sowohl deutscher als auch schweizerischer und österreichischer Electronic-Government-Programmatiken Aufnahme gefunden hat.[21] Bei den Akteuren sowie in der wissenschaftlichen Debatte besteht Einigkeit darüber, dass die Implementierung von Electronic Government in einer dreistufigen Abfolge von Übertragungsformen erfolgen müsse: Information, Kommunikation und Transaktion.[22] Unter *Information* wird die Veröffentlichung von Verwaltungseinrichtungen im Internet verstanden, im ersten Schritt die Einrichtung einer Homepage der jeweiligen Behörde. Der Informationsfluss bleibt einseitig von der Verwaltungseinrichtung zum Bürger, der als Rezipient in Erscheinung tritt, aber keine Möglichkeit hat, Daten an die Verwaltung zurück zu übermitteln.

Auf der Ebene der *Kommunikation* wird das Informationsangebot »mit Dialog- und Partizipationsmöglichkeiten« ergänzt: »Sie reichen von einfachen Lösungen wie Internet Relay Chat (IRC), E-Mail, webbasierte Diskussionsforen und Chatrooms bis hin zu komplexen Anwendungen auf Audio- und Videobasis, etwa Interactive-Voice-Response-Systeme oder Videokonferenzsysteme für Teleprä-

20 von Lucke/Reinermann: Speyerer (wie Anm. 9), S. 6.

21 Vgl. ebd. S. 3. Vgl. Heide Brücher/Michael Gisler: E-Government – Von den Grundlagen zur Anwendung, in: Praxis der Wirtschaftsinformatik 226 (2002), S. 12.

22 Vgl. von Lucke/Reinermann: Speyerer (wie Anm. 9), S. 3.

senz und Telekooperation«.[23] Schon die Einrichtung von E-Mail-Adressen wirft dabei Fragen über den Rechtsstatus dieser Dokumente auf. Mangels gerichtlicher Anerkennungsfähigkeit digitaler Kommunikation ist jenseits weniger Ausnahmen und unverbindlicher Formen des Austauschs wie Auskünften und Terminvereinbarungen keine Kommunikation von öffentlichen Stellen mit dem Bürger zulässig. Dieser muss bislang digital zur Verfügung gestellte Unterlagen ausdrucken und unterschreiben, um ihnen Rechtsgültigkeit zu verleihen. Der eigentliche Verwaltungsakt findet somit häufig immer noch in Papierform statt, und in vielen Fällen ist das persönliche Erscheinen und das Ausweisen in der Behörde vorgeschrieben.

Transaktion schließlich wird von von Lucke und Reinermann als die vollständige, medienbruchfreie Abwicklung von Verwaltungsleistungen im Internet verstanden. Während in den Stufen *Information* und *Kommunikation* die eigentliche Verwaltungsdienstleistung noch immer ein Papierakt war, mithin die entscheidenden Registeroperationen nur unter Vorlage der Papiere der betreffenden Personen bzw. unter Zuhilfenahme ihrer Unterschrift zur Authentifikation und Autorisierung rechtlich gültig waren, werden hier die staatlichen Register und die Personen authentifizierenden Medien digital. Mit der Implementierung von Transaktionsfähigeit soll also die Verabschiedung des Papiers in der öffentlichen Verwaltung vollzogen werden und der Staat das Internet an dessen Stelle nutzen. Von Luckes und Reinemanns im Jahre 2000 geprägte Nomenklatur wird in den vom Bundesministerium des Inneren seit 2002 herausgegebenen und ständig aktualisierten *Standards und Architekturen für E-Government-Anwendungen* (SAGA) übernommen:

»Transaktion hat das höchste Interaktionsniveau. Dieser Bereich umfasst die eigentliche Erbringung von Dienstleistungen in der öffentlichen Verwaltung. Dazu gehören z. B. die elektronische Annahme und Bearbeitung von Anträgen oder Aufträgen sowie die Bereitstellung von Formularen, die direkt am Computer ausgefüllt und sofort an den zuständigen Empfänger versandt werden. Auch elektronische Zahlungs- oder Ausschreibungssysteme sind hier zuzuordnen.«[24]

Die SAGA-Standards haben keine Rechtsverbindlichkeit, gelten aber als Maßgaben für die Implementierung von Electronic-Government-Projekten auf allen Verwaltungsebenen in Deutschland. Als solche werden sie jeweils den rechtlichen wie technischen Entwicklungen angepasst. In der acht Jahre nach der Speyerer

23 Ebd.

24 Bundesministerium des Innern: Standards und Architekturen für E-Government ›SAGA‹, http://www.cio.bund.de/DE/Standards/SAGA/saga_node.html (15. 12. 2010).

Definition veröffentlichten *SAGA Version 4.0* kommt zur Sprache, dass »Transaktionsdienstleistungen im Vergleich zu den anderen Interaktionsstufen in geringerem Maße realisiert worden« sind.[25] Denn: »[…] um die Authentizität und Vertraulichkeit der zwischen den einzelnen Instanzen übermittelten Daten sicherzustellen, sind Public Key Infrastructures (PKIs) eine wichtige Voraussetzung.«[26]

Von Personen ist hier nicht die Rede, und der gewählte Begriff Instanzen steht nicht allein für Verwaltungsabteilungen ein, sondern verweist darauf, dass nicht nur Menschen, sondern, ganz von Luckes und Reinermanns Vision der *Neuen Erreichbarkeit* entsprechend, auch Abläufe, Daten und Objekte unter Bedingungen von Authentizität und Vertraulichkeit von den digitalen Verwaltungen ansprechbar werden sollen. Der Diskurs des Electronic Government thematisiert somit mit dem Begriff der Transaktion seine eigenen Vorraussetzungen. Die Medien der *alten Erreichbarkeit*: Unterschriften, Pässe und Papiere, aber auch Parameter wie Zeit und Raum, die die Adressierbarkeit von Personen, Orten und Abläufen unter Bedingungen von Authentizität und Vertraulichkeit ermöglichen und sie so als Transaktionen ausweisbar machen, haben keine Äquivalente im Internet. Sind im Realraum die Bedingungen für Transaktionalität allgemein durchgesetzt und verfügbar, hat sich historisch ein mediales Regime ausgebildet, das es erlaubt, bestimmte Übertragungen mit Zeichen auszustatten, die sie für den Staat *ex ante* oder zumindest *ex post* lesbar und damit verlässlich, nachvollziehbar und wo nötig vertraulich machen, so ist das für den virtuellen Raum nicht der Fall. Entsprechend ist Transaktionsfähigkeit, die staatlichen Ansprüchen genügt, im digitalen Raum erst noch herzustellen und eine zentrale Herausforderung der gegenwärtigen Regierungskunst. In den SAGA-Standards wird zugleich die Kulturtechnik benannt, die Transaktionen im Internet ermöglichen soll: *Public-Key-Infrastrukturen*.

3. Public-Key-Infrastrukturen und Digitale Signaturen

Unter dem unscheinbaren Titel *New Directions in Cryptography*[27] veröffentlichen die Mathematiker Whitfield Diffie und Martin E. Hellmann 1976 ein zehnseitiges Papier, das in der langen Geschichte der Kryptographie eine Zäsur darstellt.[28] Für

25 Ebd.

26 Ebd.

27 Whitfield Diffie/Martin E. Hellmann: New Directions in Cryptography, in: IEEE Transactions on Information Theory 22 (1976), S. 644–654.

28 Vgl. David Kahn: The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, New York 1996, S. 982 f.; Simon Singh: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 1999, S. 323 f.

alle bis dahin bekannten kryptograpischen Verfahren stellte sich das fundamentale Problem des Schlüsseltausches. Bevor verschlüsselte Nachrichten übermittelt werden konnten, mussten zwischen Sender und Empfänger die Schlüssel zum Ver- und Entschlüsseln der Nachrichten ausgetauscht werden. Dazu ist ein sicherer Kanal notwendig, der es unmöglich macht, dass der Schlüssel publik wird oder in die Hände unberechtigter Dritter fällt. In militärischen Kontexten wurden Schlüssel häufig von Boten persönlich übermittelt.

Im vollen Bewusstsein der Bedeutung ihrer Entdeckung lautet der erste Satz in Diffies und Hellmanns Artikel: »We stand today on the brink of a revolution in cryptography.«[29] Das von ihnen vorgestellte Modell stellte in der Tat einen Paradigmenwechsel der Kryptographie dar, denn in Diffies und Hellmanns System wird die unbedingte Notwendigkeit einer geheimen und sicheren Übertragung der Schlüssel verworfen. Stattdessen schlagen sie eine öffentliche Kryptographie vor, die sie *public key cryptosystem*[30] taufen. An Stelle der so genannten symmetrischen Schlüssel in bis dahin gängigen Kryptosystemen benutzen Sender und Empfänger in Diffies und Hellmanns System für die Prozesse des Verschlüsselns und Entschlüsselns nun jeweils unterschiedliche Schlüssel. Sowohl Sender als auch Empfänger verfügen über ein solches Schlüsselpaar, das aus einem geheim gehaltenen privaten Schlüssel und einem öffentlichen Schlüssel besteht. Letzterer dient ausschließlich dem Verschlüsseln, kann allgemein bekannt gemacht werden und trägt entsprechend die Bezeichnung *Public Key*. Um eine Nachricht zu übermitteln, benutzt der Sender den *Public Key* des prospektiven Empfängers, verschlüsselt mit diesem die Nachricht und sendet sie ihm zu. Der Empfänger kann die Nachricht dann mit Hilfe seines *Private Keys* entschlüsseln. Ein solches System hat zwei Vorraussetzungen: Erstens müssen die *Public Keys* tatsächlich allgemein zugänglich sein: »Each user […] can […] place his enciphering key in a public directory […]. A private conversation can be held between any two individual regardless of whether they have ever communicated before.« Zweitens muss sichergestellt werden, dass die *Private Keys* geheim und ausschließlich in der Verfügung des jeweiligen Schlüsseleigners bleiben. Auch darf der private Schlüssel nicht aus dem öffentlichen Schlüssel ableitbar sein, da das System sonst kompromittiert werden würde. Diffie und Hellman bewiesen, dass es mathematisch möglich ist, eben solche Schlüsselpaare zu produzieren, für die es kein mathematisch bekanntes Verfahren gibt, um in sinnvollen Zeiträumen aus dem öffentlichen Schlüssel den jeweiligen geheimen Schlüssel zu berechnen. Das kryptographische Problem der Übermittlung geheimer Nachrichten, das nicht zuletzt im Zweiten Weltkrieg Anlass zur

29 Diffie/Hellmann: New Directions (wie Anm. 26), S. 644.
30 Ebd.

Entwicklung des Computers gegeben hatte,[31] wird in Diffies und Hellmanns Text jedoch eher beiläufig abgehandelt. Ihr Interesse gilt vielmehr dem Problem der Authentifizierung im Sinne der Überprüfung der Identität eines Kommunikationspartners durch den Austausch von geheimen Informationen. Die einfachste Variante besteht darin, jedem Kommunikationspartner einen bestimmten Schlüssel zuzuordnen, sodass, wenn Nachrichten empfangen werden, anhand des Schlüssels ablesbar ist, von welchem Sender diese stammen. Alternativ kann die verschlüsselte Nachricht eine Information enthalten, die zwischen den Kommunikationspartnern zum Zweck der Identifizierung vereinbart wurde. Beide Systeme haben dieselben Nachteile wie alle symmetrischen Kryptographiesysteme: Der Austausch der identifizierenden Information muss über sichere Kanäle im Vorfeld der eigentlichen kryptographierten Kommunikation erfolgen.

Zum Zeitpunkt der Veröffentlichung von *New Directions in Cryptography* im Jahre 1976 existierte das Internet noch nicht, und das ARPANET war ein kaum sieben Jahre altes, ausschließlich akademisch und militärisch genutztes Forschungsnetzwerk mit gerade 100 Netzwerkknoten.[32] Gleichwohl leiten Diffie und Hellman gleich zu Beginn ihres Artikels aus dem Aufkommen von digitalen Netzwerken prospektive Nutzungsmöglichkeiten wie Geldautomaten und »remote computer terminals« ab, die ein »equivalent of a written signature« erfordern würden:

»In current business, the validity of contracts guaranteed by signatures. A signed contract serves as legal evidence of an agreement which the holder can present in court if necessary. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for this paper instrument, each user must be able to produce message whose authenticity can be checked by anyone, but which could not have been produced by anyone else, even the recipient.«[33]

Materialistischer ist kaum zu argumentieren: Wirtschaftliches Handeln erfordert »paper instruments«, d.h. Verträge, deren vollständige digitale Ersetzung durch die Public-Key-Kryptographie geleistet werden soll. Die Argumentation Diffies und Hellmanns bleibt dabei strikt auf der Ebene der Medialität des Vorgangs. Weder die Inhalte von Verträgen, noch ihre strukturelle Form als Anerkennungsverhältnis des jeweils anderen Eigentums und deren wechselseitige Aufgabe als verbriefter und damit einklagbarer Tauschakt werden thematisch. Sehr viel

31 Vgl. Friedrich A. Kittler: Grammophon, Film, Typewriter, Berlin 1986, S. 367 ff.

32 Vgl. Katie Hafner/Matthew Lyon: Arpa Kadabra oder die Geschichte des Internet, Heidelberg 2000, S. 250 ff.

33 Diffie/Hellmann: New Directions (wie Anm. 26), S. 644.

schlichter werden Verträge als ein informationstechnisches Problem, nämlich als eine bestimmte Klasse von Nachrichten gefasst, die durch die Signaturen ihre Gültigkeit erhalten. Signaturen werden wiederum selbst als Nachrichten definiert, deren Eigenschaft in der für jeden zu überprüfenden Nachweisbarkeit liegt, von einem bestimmten Sender produziert worden zu sein. Niemand anderes, auch der Empfänger nicht, darf in der Lage sein, eine solche Nachricht herzustellen. Ein Fälscher oder ein »Meddler«[34] – jemand, der sich in fremde Angelegenheiten einmischt – muss daran gehindert werden, eine »authentic looking message« einzuspeisen, was insbesondere Folgendes einschließt: »[…] he must be prevented from creating apparently authentic messages by combining, or merely repeating, old messages which he has copied in the past.«[35] Zugleich ist es notwendig, nachweisen zu können, dass der Sender ein bestimmtes Dokument – z. B. einen Vertrag – verschlüsselt hat und dieses verschlüsselte Dokument während der Übertragung nicht verändert worden ist. Dazu wird aus den Daten der zuzustellenden Nachricht mittels eines für alle Nutzer transparenten, also allgemein bekannten Algorithmus ein *Hashwert*[36] – eine Art Quersumme die als mathematischer Fingerabdruck der Nachricht fungiert – gebildet. Der Sender verschlüsselt den Hashwert mit seinem *Private Key* und übermittelt das Resultat zusammen mit den Daten der Nachricht. Die Botschaft an den Empfänger enthält also zwei Elemente: die Daten der Nachricht – zum Beispiel einen Vertragstext – und den mit dem Private Key des Absenders verschlüsselten Hashwert dieser Nachricht. Der Empfänger geht in drei Schritten vor: Erstens bildet er mittels desselben Hashalgorithmus, der vom Absender benutzt wurde, aus den empfangenen Daten der Nachricht den Hashwert. Zweitens entschlüsselt er mit Hilfe des *Public Key* des Senders den ihm vom Absender zugesandten Hashwert. Schließlich vergleicht er beide Hashwerte. Stimmen diese überein, liegt der Nachweis vor, dass das Dokument während der Übertragung nicht verändert wurde. Darüber hinaus ist nachgewiesen, dass derjenige, der über den geheimen Schlüssel verfügt, mit dem der Hashwert verschlüsselt wurde, der Absender ist. Der mit dem *Private Key* verschlüsselte Hashwert fungiert hier also als digitales Äquivalent einer »written signature«.[37] Er stellt im Sinne Diffies und Hellmans diejenige Nachricht dar, mit der jedermann überprüfen kann, dass sie von einem bestimmten privaten Schlüssel in Verbindung mit bestimmten Daten ausgegangen ist: »a true, digital, message dependent signature«.[38]

34 Ebd. S. 646.

35 Ebd.

36 Hash = gehacktes: Die Daten werden mathematisch nach einem vorgegebenen Verfahren zerhackt.

37 Diffie/Hellmann: New Directions (wie Anm. 26), S. 644.

38 Ebd. S. 645.

Worauf sich eine solche digitale Signatur bezieht, bleibt offen. Sie kann für eine Person, oder wie in der Vision von von Lucke und Reinermann für Objekte, Prozesse oder Daten selbst stehen. Signaturen waren einst ein Privileg von Schriftkundigen. Mit der Alphabetisierung und der Herausbildung des modernen Rechts wurden sie zu einem besonderen Schreibereignis, weil sie als die vom Staat garantierte Präsenz des Körpers bei einem Schreibakt gelten. Im Bürgerlichen Gesetzbuch heißt es zur Schriftform explizit, diese habe »eigenhändig durch Namensunterschrift«[39] zu erfolgen. Signaturen sind somit der Punkt, an dem durch die gesetzlich vorgeschriebene Eigenhändigkeit Körper, Name und Staat im Schreiben einander berühren. Mit dem elektronischen Personalausweis erhalten die Bürger in Deutschland ein Substitut solcher Eigenhändigkeit zugestellt. Auf dem Chip des elektronischem Personalausweises ist ein dem jeweiligem Bürger zugeordneter *Private Key* gespeichert, mit dem sich digitale Signaturen für den rechtsgültigen Geschäftsverkehr im Internet erstellen lassen.

Ein solches System von mittels durch Public-Key-Kryptographie bereitgestellten digitalen Signaturen hat jedoch eine weitere wesentliche Vorraussetzung: den Nachweis der Zugehörigkeit einer digitalen Signatur und eines bestimmten öffentlichen Schlüssels zu einem bestimmten Individuum. Diffie und Hellmann erwähnen beiläufig und in einem Halbsatz, dass sie von einem initialen Erscheinen der Nutzer zur Registrierung ihrer Schlüssel ausgehen: »We now suggest a new public key distribution system […] its use can be tied to a public file of user information which serves to authenticate user A to user B vice versa. By making the public file essentially a read memory, one personal appearance allows a user to authenticate his identity many times to many users.«[40]

One personal appearance – vor dem Schreiben der eigenen Signatur steht das Aufgeschriebenwerden: aufgeschrieben im *public file*, indem der »enciphering key […] along with the user's name and address«[41] registriert werden sollen. Unklar bleibt, wohin die Nutzer ihre Körper zum Eintrag in dieses öffentliche Verzeichnis tragen sollen. Offenbar liegt das *public file* nicht in der Verfügung des jeweiligen Nutzers, sondern wird durch eine dritte Instanz geführt. Zwischen den Nutzern, die mittels Public-Key-Kryptographie sich authentifizieren wollen oder müssen, steht also ein Register, dem sie begegnen müssen, bevor sie miteinander kommunizieren können. Bei dieser Begegnung, bei dem der Nutzer erscheint, d. h. sich körperlich präsentiert[42] und seinen Namen angibt, findet ein Schreibakt statt, der

39 BGB §126 Schriftform, Bürgerliches Gesetzbuch, unter: http://dejure.org/gesetze/BGB/126.html (15. 12. 2010).

40 Diffie/Hellmann: New Directions (wie Anm. 26), S. 644.

41 Ebd. S. 648.

42 Derrida ist diese Notwendigkeit der Deckung digitaler Signaturen durch die eigenhändige Signatur nicht entgangen. Vgl. Derrida: Über das »Preislose« (wie Anm. 7), S. 26.

für die Legitimität und Beweiskraft der Signatur essentiell ist. Beim elektronischen Personalausweis kann der Eintrag in das *public file* beim Meldeamt stattfinden, wenn der Bürger die freiwillig nutzbare Signaturfunktion freischalten lässt. Das unscheinbar *public file* genannte Register nimmt somit innerhalb einer für Authentifizierungszwecke genutzten Public-Key-Kryptographie einen zentralen Stellenwert ein. Eine digitale Signatur, die die Geltung der für sie genutzten Schlüssel nicht aus einem stabilen und überprüfbaren Register ableiten kann, ist für die Authentifizierung wertlos. Erst das Register verknüpft die Elemente des einem Körper zugeschriebenen Nutzernamens, der Adressen und digitale Schlüsselcodes zu einem funktionalen Äquivalent des »paper instrument« realweltlicher Transaktionen und somit des von eigener Hand unterschriebenen Vertrags.

4. Der Name des Staates: Die Bundesnetzagentur

Das Register – der stetige Grund des Staates[43] – für digitale Signaturen, die von den Bürgern mit dem elektronischen Personalausweis verfertigt werden können, wird in Deutschland nicht von den Meldeämtern, sondern von der Bundesnetzagentur verwaltet.[44] Sämtliche so genannten akkreditierten Digitalen Signaturen, die in Deutschland höchsten Rechtsschutz genießen und der eigenhändigen Namensunterschrift nach § 126 BGB rechtlich vollständig gleichgestellt sind, stehen in Deutschland in einer nationalen Schlüsselhierarchie, deren Spitze die Bundesnetzagentur bildet. Sie ist die so genannte Wurzelinstanz, die *Root Certification Authority*, der Public-Key-Infrastrukturen in Deutschland und hält somit das Register der Register vor. Dieses Register ist selbst aus einer digitalen Signatur gebildet, aus der mathematisch alle akkreditierten digitalen Signaturen in Deutschland abgeleitet sind. Staatlichkeit selbst ist eine Signatur, ein Name, eine Chiffre, aus dem sämtliche digitalen Signaturen, mithin sämtliche Äquivalente der Eigennamen und der Eigenhändigkeit der Bürger geschöpft werden. Der öffentliche Schlüssel dieser digitalen Signatur wird von der Bundesnetzagentur im Internet zugänglich gemacht.[45] Der derzeit gültige Schlüssel trägt die Bezeichnung klein *a*, und das Zertifikat, bei dem man an den »großen Anderen« i. S. v. Jacques Lacan denken kann und auf das sich alle legitimen digitalen Signaturen in Deutschland beziehen sollen, liest sich in seiner ganzen alphanumerischen Buchstäblichkeit folgendermaßen:

43 Vgl. Vismann: Akten (wie Anm. 16), S. 144.

44 Bundesnetzagentur: Bundesnetzagentur Startseite, unter: http://www.bundesnetzagentur.de/cln_1912/DE/Home/home_node.html (13.12.2010).

45 Bundesnetzagentur: Bundesnetzagentur | Öffentliche Schlüssel, unter: http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Oeffentliche_Schluessel_st.html (13. 12. 2010).

Angaben zu neuen öffentlichen Schlüsseln (Signaturprüfschlüsseln) der zuständigen Behörde:

a) Root-CA-Schlüsselinformation 12:
Signaturalgorithmus: RSA, 2048 Bit

Seriennummer [dezimal]:
313

Issuer Distinguished Name und Subject Distinguished Name:
CN=12R-CA 1:PN
O= Bundesnetzagentur
C=DE

Modul n [hexadezimal]:
0098 3aa6 3152 aafa 65d9 48b9 56b3 d6b6 844e 695d f36b 4208 58d4 9c89 471a 9693 6c11 90f5 d756 e297 6474 d98a e1d1 c37a c027 1850 7ab6 0673 1536 22be 34d8 272c efdc dba7 32d8 7c02 3c02 8af4 34bb 6441 96e9 d8da 383a 74d4 9e4f 01a5 98e9 46ef 4f47 8163 c7be f01b a2a2 c3a1 5f35 9273 1b35 b1b8 3fb1 5fff e96c 4e76 cdfe 04f4 5f97 c753 3e54 3b77 a8c3 2976 903e 8605 9c1b fa7a 11ff ce94 d15d fdc9 7b24 643f cd34 15ca 3b32 a8f5 55f1 d3d4 b552 ad36 ec27 3e54 86ba d835 9479 41a2 5038 c25d 7268 6801 76c1 0703 fdca eb00 9954 cde3 9566 44b3 4495 e98e 91bc 9198 4a81 280e a607 e7a6 30d7 0175 9b90 9bb2 0cbd 9fa9 72cf c40c 81ab 74e1 8141 d94f df6c 4127 77

Öffentlicher Exponent e [hexadezimal]:
4000 0081

Gültig von: 25.05.2007, 13:01:44 (UTC) d.h. 15:01:44 (MESZ)
Gültig bis: 25.05.2012, 12:56:07 (UTC) d.h.14:56:07 (MESZ)

Anhand dieses Zertifikats, das die Gültigkeitsdauer sekundengenau angibt, zudem Seriennummer und ausstellende Behörde des Schlüssels benennt, kann jeder Nutzer die Gültigkeit seiner akkreditierten digitalen Signatur bzw. die Gültigkeit der ihm zugegangenen signierten Nachrichten überprüfen. Dieser Abgleich ist während eines Signaturvorgangs nicht zwingend, kann aber mit einem so genannten *Online Certificate Service Protocol* automatisiert erfolgen. So ist es möglich, dass während des Signierens überprüft wird, ob der vom Absender genutzte Schlüssel zum Zeitpunkt der Signatur gültig ist oder in der Zertifikatssperrliste des Zertifikatsanbieters steht.[46] Es handelt sich somit bei einer akkreditierten Signatur nicht

46 Diese sind bei der Bundesnetzagentur zu erreichen: Bundesnetzagentur | Telekommu-

nur um eine rechtliche Beziehung, sondern um eine im Signaturverfahren implementierte mediale Beziehung des auf dem elektronischen Personalausweis gespeicherten individuellen *Private Keys* zu einem staatlichen Register. War die Beziehung der Signaturen analoger Medien des Staates, des Geldes, der Papiere und der Urkunden gleichsam virtuell, so heißt digital zu signieren im Moment der Signatur eine reale Verschränkung mit dem Register zu vollziehen, sich seine Identität als aus dem Register geschöpfte bestätigen zu lassen. Man schreibt seinen Namen im Namen des Staates.

5. Sans signature

Mit dem elektronischen Personalausweis bekommen Menschen in Deutschland die Möglichkeit des Vollzugs der Verschränkung mit dem Register, das ihnen einen Namen, eine Adresse im digitalen Raum gibt. Dinge dagegen sind noch *sans signature*. Ihnen Signaturen zuzustellen und sie transaktionsfähig zu machen ist Gegenstand der gegenwärtigen Forschungsinitiativen der Bundesdruckerei. Zusammen mit fünf Instituten der Frauenhofer Gesellschaft und den Berliner Universitäten hat die Bundesdruckerei 2008 den *Innovationscluster Sichere Identität Berlin-Brandenburg* gegründet. In diesem Forschungsprogramm, das sich wie eine Implementierung der Vision von Luckes und Reinermanns liest, steht Identität nicht für personale Identität, sondern gilt für alle Dinge. Auf der Website des Innovationsclusters heißt es:

»Every relationship or transaction is based on connection between (at least) two uniquely identifiable actors or entities […]. Unique identity thus applies equally to relationships between people – sellers and customers, public authorities and citizens – to relationships between people and objects – drivers and cars, young people and cigarette machines, researchers and databases – and to relationships between object and object – spare parts and machines, software updates and computers, cars to cars etc.«[47]

Die Verfertigung solcher universeller Identitäten wird vom Frauenhofer Innovationscluster unter dem Motto »ID basierte Kommunikation der Zukunft« in aktiver Mitarbeit der deutschen Industrie untersucht. Hatten klassische Signaturen noch ein Moment der Äußerlichkeit und wurden durch einen Schreibakt oder in

nikationsanschlüsse der BNetzA zum Abrufen von Zertifikaten, unter: http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Kommunikationsverbindung_sv.html (13. 12. 2010).

47 Innovationscluster Sichere Identität: What exactly does ›Secure Identity‹ mean, unter: http://www.sichere-identitaet.de/faq#wasGenauBedeutet (20. 12. 2010).

Druck- und Prägeverfahren aufgebracht, sollen sie hier Bestandteil von Objekten werden. »Inherent-ID«[48] bezeichnet der Innovationscluster sein Forschungsprojekt, Materialien selbst als Signaturen fungieren lassen zu können. Was Valentin Groebner im Hinblick auf Identitätspapiere für Personen als Lücke zwischen Papier und Körper beschrieben hat, sollen diese Projekte für Objekte schließen: »Optische 2D- und 3D-Merkmale sowie Geruchsmerkmale, die aufgrund qualitativ hochwertiger Herstellungstechnologie inhärent mit dem echten Produkt verbunden sind, werden dabei zum Nachweis der Produktidentität miteinander kombiniert. Diese bilden die Basis für elektronische Echtheitszertifikate […]«.[49] Während im Inherent-ID-Projekt die Identität durch das sensorische Auslesen und Registrieren von schon vorhandenen Produkteigenschaften generiert wird, wird im *SeMaTec Forschungsprojekt*[50] untersucht, inwieweit sich die spezifischen spektralen Eigenschaften bestimmter isometrischer organischer Moleküle im Terahertzband eignen, um als Eingangssignal für die Erstellung digitaler Echtheitszertifikate genutzt werden zu können. Solche so genannten Markermoleküle können auch in lose Güter wie Trockenchemikalien oder Flüssigkeiten eingebracht werden. Ziel ist es, den Rohmaterialien vor der Weiterverarbeitung Identifikationsmerkmale beizugeben, die es erlauben, ihre Herkunft, Produktionsstätten und Verschiffungswege und so den gesamten Lebenslauf des Produktes nachvollziehen zu können. Vor allem aber soll so der Schutz des Markenrechts und des geistigen Eigentums von Industrieprodukten ermöglicht werden.

6. Gouvernemedialität der Transaktion

Im Diskurs des Electronic Government wird die Herstellung von Transaktionsfähigkeit als zentrale Aufgabe von Staatlichkeit unter digitalen Bedingungen formuliert. Transaktionen selbst erweisen sich hier als voraussetzungsreiche Form der Übertragung, die wie keine andere an besondere Autorisierungs- und Beglaubigungspraxen gebunden sind. Für Menschen und in Zukunft vielleicht auch für Dinge wird Transaktionsfähigkeit im digitalen Raum über digitale Signaturen in

48 Innovationscluster Sichere Identität: Innovationscluster Sichere Identität – Inherent-ID, unter: http://www.sichere-identitaet.de/images/sichere_identitaet/szenariokarten/si_flyer02_inherentid_100327–3_web_de.pdf (20. 12. 2010).

49 Innovationscluster Sichere Identität: Innovationscluster Sichere Identität – Inherent-ID, unter: www.sichere-identitaet.de/.../sichere_identitaet/.../si_flyer02_inherentid_100327–3_web_de.pdf (20. 12. 2010).

50 Innovationscluster Sichere Identität: Innovationscluster Sichere Identität – SecMaTec, unter: http://www.sichere-identitaet.de/images/sichere_identitaet/szenariokarten/si_flyer10_secmatec_100327_web_de.pdf (20. 12. 2010).

Public-Key-Infrastrukturen hergestellt. Der elektronische Personalausweis als Teil einer staatlich betriebenen Public-Key-Infrastruktur dient dazu, Menschen im digitalen Raum adressierbar und sie zugleich zu Transaktionsinstanzen zu machen. Zeitgenössisches Regieren bedeutet, den Medienwandel zur Digitalität zu betreiben und somit die Medialität des Regierens selbst zum Interventionsfeld zu machen. Nicht allein staatliche Akteure betreiben diese Prozesse, Hacker sind darin genauso engagiert[51] wie die IT-Industrie, die Bürger und die Netziens. Sie alle versuchen, Konstellationen herbeizuführen, in denen die Medialitäten der Führungen und Selbstführungen thematisch werden, deren Potentiale befragt und technisch implementiert wie politisch ausgehandelt werden können. Die Cryptowars[52] der 90er Jahre, die in einer Liberalisierung der einst streng regulierten kryptologischen Technologien und der Freisetzung der asymmetrischen Verschlüsselung aus der Kontrolle von Geheimdiensten endeten, bieten hier eine beispielhafte Vorgeschichte. Die Auseinandersetzungen um das, was man mit einem von Boris Traue und mir vorgeschlagenen Begriff Gouverne*medialität* der Gegenwart nennen könnte,[53] sind im vollen Gange. Dabei ist festzuhalten, dass die digitale Gouvernemedialität, wie sie sich derzeit in Deutschland entwickelt, nicht mehr die Unterschrift eines Souveräns benötigt,[54] sondern in ein System eingebettet ist, bei dem der Souverän selbst zu einem Zeichen wird, zu einer Signatur, aus der alles im Akt der Transaktion seine Legitimation beziehen soll.

51 Vgl. Christoph Engemann: Electronic Government und die Free Software Bewegung: Der Hacker als Avantgarde Citoyen, in: Gethmann/Stauff (Hg.): Politiken der Medien (wie Anm. 16), S. 155–172.

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

53 Vgl. Christoph Engemann/Boris Traue: Governmediality of the Life Course, unter: governmediality.net (12. 12. 2010).

54 Jochen Hörisch: Kopf oder Zahl. Die Poesie des Geldes, Frankfurt/M. 1998, S. 11 f.