Die Regulierung von Privatheit: technische Innovation als Herausforderung von Datenschutzregimes

Busch, Andreas

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Verlag Barbara Budrich

Empfohlene Zitierung / Suggested Citation:
Busch, A. (2011). Die Regulierung von Privatheit: technische Innovation als Herausforderung von Datenschutzregimes. *der moderne staat - dms: Zeitschrift für Public Policy, Recht und Management*, *4*(2), 403-422. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-61006-0

Andreas Busch

Die Regulierung von Privatheit: Technische Innovation als Herausforderung von Datenschutzregimes

Zusammenfassung
Veränderungen im Bereich von Telekommunikation und Computernutzung (hin zu einem *ubiquitous computing*) haben das Thema der Regulierung von Privatheit auf die politische Agenda gesetzt. Der vorliegende Aufsatz fragt, wie etablierte Datenschutz-Systeme auf diese Entwicklung reagiert haben und untersucht das für die Länder Deutschland, Großbritannien, USA und Schweden. Anhand der Beispiele ausgewählter Technologien werden regulative Reaktionen untersucht und konkurrierende Hypothesen über zu erwartende Gemeinsamkeiten getestet. Die Ergebnisse werden vor dem Hintergrund von Theorien über Staatstätigkeit diskutiert.

Schlagworte: Regulierung, Datenschutz, Vergleich, Staatstätigkeit

Abstract
The Regulation of Privacy: Technical Innovation as a Challenge for Data Protection Regimes
Changes in the use of telecommunications and computers towards a situation of 'ubiquitous computing' have put the topic of regulation of privacy squarely onto the political agenda. This article asks how established systems of data protection have reacted to these developments and looks at the cases of Germany, the United Kingdom, the United States and Sweden. The examples of selected technologies are subjected to an analysis of regulatory reactions, and competing hypotheses about expected commonalities are being tested. The results are being discussed against established theories of determinants of public policy.

Key words: Regulation, Privacy, Data Protection, Comparative Public Policy

1. Einleitung

Debatten über das Thema Datenschutz und den Gebrauch von Technologien, die in Verbindung mit personenbezogenen Daten stehen, haben in der letzten Zeit stark zugenommen.[1] Dazu beigetragen haben – zumindest in der Bundesrepublik Deutschland – eine Reihe von publizitätsträchtigen Datenskandalen, die sich in den vergangenen Jahren in mehreren deutschen Unternehmen ereignet haben, sowie öffentliche Diskussionen über geplante Datensammlungen sowohl im öffentlichen wie im privaten Sektor:

– So wurde im Jahr 2008 bekannt, dass die Deutsche Telekom Verkehrsdaten von Mitarbeitern, Aufsichtsratsmitgliedern, Journalisten und Gewerkschaftern missbraucht hatte, um eigene Untersuchungen über die Weitergabe vertraulicher Konzerninformationen anzustellen. Personenbezogene Daten waren zu diesem Zweck an Detekteien weitergegeben worden (*Der Bundesbeauftragte für den Datenschutz und die Informa-*

tionsfreiheit, 2009, S. 33f.). Der Vorfall führte zu einer Umstrukturierung des Unternehmensvorstandes.

– Die Deutsche Bahn unternahm im Jahr 2009 den Versuch, Korruption im eigenen Unternehmen durch die geheime Überprüfung von 173.000 Mitarbeitern vermittels automatischem Datenabgleich und unter Umgehung der Arbeitnehmervertretungen zu bekämpfen – ein Vorgehen, das nicht nur einen großen Vertrauensverlust für das Unternehmen bedeutete, sondern auch den Vorsitzenden des Vorstands der Deutschen Bahn, Hartmut Mehdorn, schließlich zum Rücktritt zwang.[2]
– Über den Discounter Lidl wurde in den selben Jahren bekannt, Mitarbeiter seien in den Filialen heimlich per Video überwacht worden und die Firma habe über Toilettengänge und Krankheitstage umfassend Protokoll geführt. Die Verstöße gegen Datenschutzregeln führten schließlich zur Entlassung des Deutschland-Chefs der Firma.[3]

Doch nicht nur bei großen Unternehmen fanden sich Probleme im Umgang mit personenbezogenen Daten; auch im öffentlichen Sektor gab es eine Reihe von Debatten, die dem Thema Datenschutz erhöhte Aufmerksamkeit sicherten:

– So sorgte beispielsweise das bereits vor vielen Jahren beschlossene Verfahren zum „elektronischen Entgeltnachweis“ (ELENA) – das zu Vereinfachung und Effizienzsteigerung in der Verwaltung von Einkommensdaten beitragen sollte – zu Beginn des Jahres 2010 für Unruhe. Unter dem neuen System sind Unternehmen seit Januar 2010 verpflichtet, die Einkommensdaten ihrer Mitarbeiter an eine zentrale elektronische Datei zu übermitteln. In Zukunft sollen Arbeitsagenturen und Elterngeldstellen, später dann auch Kranken- und Pflegekassen sowie die Sozialversicherungen mithilfe dieser Daten Ansprüche auf Zahlungen effizienter und kostengünstiger bearbeiten können. Sorgen hinsichtlich der zentralen Speicherung sowie über die Zugriffsrechte auf die Daten führten im März 2010 dann zu einer Massenklage von etwa 10.000 Bürgern vor dem Bundesverfassungsgericht.[4]
– Ebenfalls im Frühjahr 2010 thematisierte Verbraucherschutzministerin Ilse Aigner (CSU) Datenschutzprobleme beim Unternehmen *Facebook* und eröffnete somit eine politische Debatte zu diesem Thema. Die Ministerin kritisierte, das amerikanische Unternehmen gehe mit den Privatheitsinteressen seiner weltweit 400 Millionen Mitglieder im firmeneigenen sozialen Netzwerk nachlässig um. Auslöser war das Vorhaben der Firma, personenbezogene Daten an ausgewählte Kooperationspartner weiterzugeben, ohne die Nutzer vorher zu konsultieren. Selbst wenn die Ministerin mit ihrer Drohung, ihre Mitgliedschaft bei Facebook zu beenden, falls das Unternehmen sein Verhalten nicht ändere, auch Spott erntete – es gelang ihr doch, erhebliche öffentliche Aufmerksamkeit für ihren Vorstoß zu erreichen.

Als dann im Sommer 2010, unter Ausnutzung einer Sicherheitslücke im System von Facebook, die Namen sowie die Zugangsadressen der Facebook-Seiten von über 100 Millionen Facebook-Benutzern zusammengestellt und im Internet veröffentlicht wurden, gewann das Thema weitere Popularität. Titelgeschichten in Zeitschriften wie *Stern* und *Focus* spitzten die Problematik zu: *Focus* porträtierte Facebook als „Großen Bruder“ und konstatierte: „Facebook weiß mehr als jede Stasi der Weltgeschichte.“ Auch der *Stern* bemühte die Analogie mit George Orwells berühmtem Roman und schrieb auf seinem Titelblatt: „Big Brother Google is watching you“.

Sowohl in der öffentlichen wie auch in der akademischen Diskussion verbreitete sich in Folge das Bewusstsein darüber, dass einmal ins Internet gestellte Daten dort vermutlich

auch immer verfügbar bleiben würden, da sie nicht mehr sicher gelöscht werden können; denn schließlich können andere Benutzer sofort Kopien der Daten anlegen, über die der Urheber nicht verfügen kann. Diese Problematik ist auch ein Beispiel für die Vielfältigkeit diskutierter Lösungen: sie reichen in diesem Fall von dem Vorschlag, automatisierte Löschfristen für ins Internet eingestellte personenbezogene Daten einzuführen (*Mayer-Schönberger* 2009) bis zu der von Google-CEO Eric Schmidt geäußerten Idee, ein Recht auf Namensänderung bei Erreichen der Volljährigkeit einzuführen, um sich so mit einem Schlag der eigenen (und im Internet dokumentierten) Jugendsünden zu entledigen.[5]

Auch aus dem politischen Raum wurden vermehrt Forderungen nach verbesserter Regulierung von Privatheit laut, die insbesondere von Bundesministerin Aigner vorgetragen wurden. Nachdem ihr Konflikt mit der Firma *Facebook* über mangelnde Datenschutzbestimmungen zu ihrem Austritt aus diesem sozialen Netzwerk geführt hatte,[6] griff die Ministerin Sorgen über den Dienst *Google Streetview* auf, der ab Ende des Jahres 2010 auch in Deutschland angeboten werden sollte. Das systematische Fotografieren von Straßen und Häusern wurde von ihr als datenschutzrechtliches Problem bewertet, gegen das besserer Schutz gewährleistet werden müsse.[7] Eine Widerspruchsregelung, auf die sich die Politik mit der Firma Google schließlich einigte, beendete die Diskussionen dann im Herbst 2010 zunächst.

Die Regulierung von personenbezogenen Daten und Privatheit im weiteren Sinne ist also ein Thema, das auf der politischen Agenda in den letzten Jahren beständig weiter nach oben gestiegen ist.[8] Ein weiteres Indiz hierfür – und auch für die Wichtigkeit, die politische Parteien diesem Themenbereich neuerdings zuschreiben – ist die Einrichtung der Enquête-Kommission „Internet und digitale Gesellschaft" durch den Deutschen Bundestag im Frühjahr 2010. Und die Bundesrepublik steht mit dieser wachsenden Thematisierung von Privatheit, Überwachung und „Netzpolitik" nicht allein, wie etwa die Untersuchungskommissionen zum Thema Überwachung in Großbritannien (sowohl durch das britische Unterhaus wie durch das House of Lords) zeigen.[9]

Aus analytischer Perspektive handelt es sich bei den geschilderten Entwicklungen um Reaktionen auf die Herausforderungen, denen sich die etablierten Datenschutz-Systeme im letzten Jahrzehnt durch die Entstehung einer Situation „allgegenwärtiger Datenverarbeitung" (engl.: *ubiquitous computing*) ausgesetzt gesehen haben.[10] Vor allem drei Faktoren sind hier zu nennen, die die ursprünglich ja aus den 1970er und 1980er Jahren stammenden Regimes des Datenschutzes einem Änderungsdruck aussetzen:

– Die technologische Entwicklung hat zu einer „Kommunikationsrevolution" geführt, in der die Zahl der Nutzer ebenso wie die der Daten explodiert ist. So ist die Zahl der Internetnutzer zwischen 1997 und 2007 um den Faktor sechs (entwickelte Länder) beziehungsweise mehr als den Faktor 10 (entwickelnde Länder) gestiegen; ihre Zahl wurde im Januar 2009 auf weltweit 1,5 Milliarden geschätzt.[11] Die Zahl der Mobiltelefone liegt noch deutlich höher: mit über 4 Milliarden im Jahr 2008 ergibt sich eine globale Abdeckungsrate von 61% (!) der Weltbevölkerung (*International Telecommunication Union*, 2009, S. 3). Gemeinsam ist diesen Kommunikationstechnologien, dass für ihr ordnungsgemäßes Funktionieren große Mengen an personenbezogenen Daten notwendig sind, die Überwachung in einem völlig neuen Umfang möglich machen, etwa in Bezug auf geographische Bewegung (durch Einbuchung in Mobilfunkmasten), Interessen (über Suchmaschinen) und Kommunikationspartner (durch Telefon- und Email-Kontakte).

- Der beschriebene Zuwachs an Datenverkehr hat nicht nur *in*, sondern durch steigende Internationalisierung auch sehr stark *zwischen* Ländern zugenommen. Neben den ökonomischen Vorteilen von zunehmendem Handel bringt dies allerdings auch Schwierigkeiten durch Konflikte zwischen zum Teil stark voneinander abweichenden nationalen Regulierungsmodellen mit sich – einschließlich der Frage, auf welche Weise solche Konflikte angesichts der Abwesenheit internationaler Institutionen oder Regimes in diesem Feld gelöst werden sollen.
- Eine dritte Herausforderung für die etablierten Regulierungen im Bereich des Datenschutzes ist seit September 2001 der Kampf gegen den internationalen Terrorismus. Die diesbezügliche Gesetzgebung hat praktisch in allen Ländern Einschränkungen von Bürger- und Datenschutzrechten und eine massive Ausweitung der Rolle von Informationstechnologie bei Polizei und Geheimdiensten mit sich gebracht. Die leitende Idee dabei ist, dass die Strafverfolgungsbehörden durch die systematische Erlangung, Speicherung und Auswertung aller Arten von Informationen terroristische Gewaltakte noch vor deren Ausführung verhindern können, zumal internationale Kooperation dabei den gegenseitigen Zugriff auf Datenbestände erlaubt. Gleichzeitig wirft dieses Vorgehen aber auch die Frage auf, ob hier nicht der Schritt weg vom Rechtsstaat und hin zu einem „Präventionsstaat" gemacht wird (*Denninger* 2002).

Der vorliegende Artikel konzentriert sich auf die erste dieser drei Herausforderungen und fragt, auf welche Weise etablierte Datenschutz-Systeme auf die vor allem durch technologische Weiterentwicklung ausgelösten Veränderungen und die massive Ausweitung der anfallenden Daten reagiert haben. Denn die zur Zeit der Entstehung der Datenschutzregimes (also zu Beginn der 1970er Jahre) typische Situation, in der wenige Großcomputer unverbunden nebeneinander standen, ist heute einer Wirklichkeit gewichen, in der zahlreiche und miteinander vernetzte Geräte vom Großcomputer bis zum mobilen Kleingerät, von Mobiltelefonen über mit dem Internet verbundenen PCs bis zu Bankautomaten und intelligenten Kundenkarten beständig personenbezogene Daten von sich geben. Hinzu kommt, dass die Regulierung personenbezogener Daten in wachsendem Maße politisch umstritten geworden ist (*Bennett* 2008), wie auch aus einigen der weiter oben genannten Episoden deutlich wurde.

Die Diskussion des Themas beginnt mit theoretischen Überlegungen zu den Themen Regulierung von Privatheit und Staatstätigkeit, bevor das der hier vorgelegten Untersuchung zu Grunde liegende Forschungsdesign dargelegt wird. Im Hauptteil werden dessen Ergebnisse dargestellt, und ein abschließender Teil diskutiert diese und ordnet sie in die gegenwärtige Debatte um Regulierung und Privatheit ein.

2. Die Regulierung von Privatheit als *public policy*: Theoretische Überlegungen

Als Gegenstand der politikwissenschaftlichen Analyse von regulativer Politik oder von Staatstätigkeit ist der Themenbereich Privatheit beziehungsweise Datenschutz bisher kaum hervorgetreten. Es gibt nur wenige Studien, die in den letzten Jahrzehnten Ausnahmen von dieser Regel gebildet haben (etwa *Bennett* 1992; *Regan* 1995; *Bennett*/*Raab* 2006).

Die Studie von *Bennett*, die die Entstehung von Datenschutz-Regimes in vier Ländern (Vereinigte Staaten, Großbritannien, Bundesrepublik Deutschland und Schweden)

nachzeichnete und analysierte, extrapolierte die Erfahrungen der Vergangenheit in die Erwartung, dass die Gemeinsamkeit der sachpolitischen Herausforderungen, gepaart mit wachsender Diffusion erfolgreicher Lösungen, zu einer immer stärkeren Angleichung der Politikergebnisse in diesem Bereich führen werde. *Bennetts* Thesen waren zu Beginn der 1990er Jahre ein Auslöser für die Debatte über *policy learning* und *policy transfer* (vgl. *Bennett* 1991a, b; *Bennett*/*Howlett* 1992; *Dolowitz/Marsh* 1996). Die Begründung für diese Erwartungen lag unter anderem in der zunehmenden internationalen Integration sowie der wichtigen Rolle, die ein Netzwerk transnationaler Politikexperten und Datenschutzbeauftragter wahrnehmen würde. Auch in den Vereinigten Staaten wurde erwartet, dass sich das dort im internationalen Vergleich eher gering ausgeprägte Niveau gesetzlicher Datenschutzbestimmungen durch internationalen Wettbewerb – sowohl im Hinblick auf politische Wirkungsfaktoren wie die EU-Datenschutzrichtlinie als auch durch wirtschaftliche Mechanismen wie das Streben nach Marktvergrößerung – im Sinne einer Konvergenzbewegung „nach oben" anpassen werde (*Regan* 1993; *Shaffer* 2000). Einige Autoren erwarteten sogar, dass die EU-Datenschutzrichtlinie einen „globalen Standard" setzen werde (*Heisenberg*/*Fandel* 2004).

Tatsächlich aber zeigt ein Blick in die Empirie 20 Jahre nach der Konvergenz-Prognose eine anhaltende Diversität von Datenschutz-Regimen, selbst in so relativ ähnlichen Ländern wie den Mitgliedsstaaten der OECD (*Busch* 2010). Sowohl im Hinblick auf Institutionalisierung, Ausstattung und Mandat wie auch hinsichtlich der inhaltlichen Ausrichtung unterscheiden sich die Regelungen im internationalen Vergleich. So gibt es beispielsweise in den Vereinigten Staaten von Amerika als einzigem OECD-Land keine Institutionalisierung in Form einer für den Datenschutz zuständigen Behörde; in der Bundesrepublik Deutschland hingegen gibt es ein Nebeneinander von Datenschutzbeauftragten sowohl auf der Landes- wie auf der Bundesebene. Und auch im Hinblick auf die Ausrichtung der Gesetzgebung in diesem Bereich kann man Unterschiede feststellen zwischen umfassend angelegten Regulierungssystemen und solchen, die nur spezifische Teile von Privatheit einem gesetzlichen Schutz unterstellen (*Newman* 2008).

Die weiter oben gestellte Frage, wie die etablierten Datenschutz-Systeme auf die Herausforderungen durch technologische Innovationen reagiert haben, lässt sich in theoretischer Hinsicht gut kombinieren mit der Frage, inwieweit die in der vergleichenden Staatstätigkeitsforschung etablierten Theorieangebote[12] auch in diesem – außerhalb des sozioökonomischen Schwerpunkts jener Literatur liegenden – Themenfeld eine Erklärungskraft besitzen. Insbesondere vier theoretische Ansätze sind hierbei von Interesse:

- *Theorien über Pfadabhängigkeit* und institutionelle Trägheit, die die Stabilität nationaler Politikprofile betonen und diese auf etablierte Routinen und positive Feedback-Effekte zwischen nationalen Institutionen zurückführen (*Pierson* 2000, 2004). Aus dieser Perspektive bestimmen zeitlich früher vorgenommene Entscheidungen oft in einem erheblichen Maße den später zur Verfügung stehenden Handlungsspielraum, so dass größere Abweichungen von in der Vergangenheit getroffenen Entscheidungen unwahrscheinlich sind, da sie mit hohen politischen und administrativen Kosten verbunden sind.
- Die *Parteiendifferenzhypothese* stellt hingegen die programmatischen Unterschiede zwischen verschiedenen miteinander konkurrierenden politischen Parteien in den Mittelpunkt ihrer Analyse und postuliert, dass die Ergebnisse von Staatstätigkeit vor allem durch die parteipolitische Zusammensetzung der Regierung bestimmt werden

(*Schmidt* 1996; *Schmidt* u.a. 2007, Kap. 4). Aus dieser Perspektive ist also davon auszugehen, dass politische Entscheidungen dergestalt getroffen werden, dass sie den Interessen der Anhänger der die Regierung bildenden Parteien entsprechen. Dabei wird davon ausgegangen, dass diese Interessen eindeutig zu bestimmen sind und die Anhänger verschiedener Parteien unterschiedliche Interessen haben.

– *Institutionalistisch orientierte Theorien* betonen die Wichtigkeit der Regeln und Normen, mit denen – formell oder informell und im staatlichen Sektor oder außerhalb desselben – kollektiv verbindliche Entscheidungen getroffen werden. Diese Entscheidungsregeln bilden Anreize für die verschiedenen an einer Entscheidung beteiligten Akteure, etwa, indem sie ihnen die Möglichkeit zu einem Veto einräumen (*Tsebelis* 2002).
– *Theorien über nationale Politikstile* verweisen auf länderspezifische Konglomerate von Faktoren, die Politikergebnisse durch zentrale strukturelle und kulturelle Eigenschaften beeinflussen, die den nationalen Institutionensystemen innewohnen. Diese Politikstile bilden eine über Politikfelder hinweg wirkende stabile Einflussmacht, die in der Literatur vor allem auf die Herangehensweise der Regierung bei der Lösung von politischen Problemen sowie auf das Verhältnis der Regierung zu anderen an Entscheidungen beteiligten Akteuren zurückgeführt wird (*Richardson* u.a. 1982).

Um diese theoretischen Ansätze im Hinblick auf die hier im Mittelpunkt stehende Frage nach der Veränderung von Datenschutz-Regimes überprüfbar zu machen, bedarf es zunächst einer konkreten Operationalisierung sowie eines geeigneten Forschungsdesigns. Beides steht im Mittelpunkt des nächsten Abschnitts.

3. Untersuchte Sektoren und Länder

Der Ausgangspunkt für die Untersuchung der Entwicklung von Datenschutz-Regimes ist die These, dass es in diesem Bereich unterschiedliche Interessen gibt und dass die jeweilige Konstellation der Interessen die Entwicklung der Regulierungsregimes erklären kann. Zu erwarten ist demnach, dass sich die Regulierung von Privatheit nicht einheitlich verändert, sondern dass unterschiedliche Aspekte der Regulierung von Privatheit unterschiedlichen Entwicklungen unterlegen haben. Bezugnehmend auf die Literatur kann man demnach von der Existenz unterschiedlicher „advocacy coalitions“ (*Sabatier*/*Jenkins-Smith* 1993), „policy ideas” (*Braun*/*Busch* 1999) und „discourses” (*Schmidt* 2002) im Themenbereich Privatheit/Datenschutz ausgehen. Genauer untersucht werden muss, welcher dieser Diskurse in einer Gesellschaft dominant wird und sich in Bezug auf die übernommenen Regelungen durchsetzen kann. So wird im Folgenden in Bezug auf personenbezogene Daten zwischen wirtschaftlichen Interessen, Sicherheitsinteressen und Bürgerrechtsinteressen unterschieden. Aus jedem dieser drei Interessengebiete wird dann ein entsprechendes Thema ausgewählt, dessen Regulierung vergleichend in unterschiedlichen Ländern untersucht wird, um so der oben angesprochenen erwarteten Unterschiedlichkeit der Entwicklungen durch ein angemessenes Untersuchungsdesign zu entsprechen.

– Aus der Perspektive *wirtschaftlicher Interessen* sind personenbezogene Daten ein wirtschaftliches Gut, das in verschiedener Hinsicht profitabel genutzt werden kann – etwa für Marketingzwecke (durch direkte, zielgruppenspezifische und oft sehr per-

sönliche Werbung), zur Durchsetzung von differenzierten Preisen für dasselbe Gut (durch Nutzung unterschiedlicher Zahlungsbereitschaft durch verschiedene Konsumentengruppen), oder zur Kosteneinsparung (durch massive Rationalisierung der Kosten von Inventarisierung und Verfolgung von Gütern). Aus Sicht dieser Interessen sind Informationen ein Gut, das für die Wissensökonomie eine ähnliche Bedeutung hat wie sie Kohle für das Industriezeitalter hatte. Zudem sind Aufbau und Unterhaltung der Infrastruktur für die Sammlung solcher Informationen und ihrer Verarbeitung natürlich selbst mit erheblichen wirtschaftlichen Möglichkeiten verbunden.

Als Fallstudie für die wirtschaftlichen Interessen werden so genannte RFID-Chips (*radio frequency identification*) hinsichtlich ihrer Einführung und Regulierung untersucht.[13] Dabei handelt es sich um kleine Chips, die bei Bestrahlung mit Radiowellen durch ein Lesegerät digitale Daten aussenden und dadurch die automatisierte Identifikation unterschiedlichster Gegenstände (vom Schokoriegel bis zum Container) erlauben. Neben der vereinfachten und verbilligten Inventarisierung können dadurch sowohl Fehlleitungen wie auch Diebstähle verhindert beziehungsweise erschwert werden; vor allem aber (und hier setzen die Sorgen von Konsumentenorganisationen an) können diese Güterdaten digital mit den Kennungen von Kunden sowie Zeit- und Ortsdaten verknüpft und daraus wertvolle neue Informationsbestände aufgebaut werden.

– Betrachtet man hingegen personenbezogene Daten unter dem Gesichtspunkt von *Sicherheitsinteressen*, so stehen Gesichtspunkte wie die zuverlässige Identifikation von Individuen mit dem Zweck der Erhöhung von Sicherheit, der Verhinderung von Kriminalität oder der Rationalisierung von Verwaltungsaufgaben im Vordergrund. Hierbei spielen natürlich auch wirtschaftliche Interessen eine Rolle (etwa durch Einsparungen bei der Verwaltung), doch sind diese nicht zentral. Zentral sind vielmehr die Verhinderung bzw. Aufklärung von Straftaten und Terrorismus, wozu Informationen z.B. über individuelle Telefon- und Internetverbindungen, von Kameras im öffentlichen Raum oder aus DNS-Datenbanken genutzt werden sollen. Generell gilt für diese Perspektive, dass der erhoffte Schutz- bzw. Aufklärungseffekt umso größer erwartet wird, je mehr Informationen über Individuen verfügbar und zugänglich sind.

  Die Regulierung von Sicherheitsinteressen bei personenbezogenen Daten wird anhand von Kameras im öffentlichen Raum (sogenannte CCTV-Kameras) untersucht.[14] Solche Kameras haben in den letzten zwei Jahrzehnten erhebliche Verbreitung erfahren, die jedoch zwischen Ländern variiert. Dabei sind z.T. erhebliche Kosten entstanden, angesichts derer die Effektivität dieses Instruments zur Verbrechensbekämpfung kontrovers diskutiert wird (*Ditton/Short* 1999). Der Fokus der Fallstudien liegt deshalb auf der Spannung zwischen den Sicherheits- und den Privatheitsinteressen der Bürger sowie der Frage, für welche Balance zwischen den beiden sich das politische System entscheidet.

– *Bürgerrechtsinteressen* spielen in Bezug auf personenbezogene Daten in mehrfacher Hinsicht eine Rolle: Zum einen gibt es Länder, deren Verfassungen Regeln über den Schutz von Privatheit beinhalten – sowohl der Europarat wie auch die Europäische Union betrachten Privatheit beispielsweise als ein zu schützendes Menschenrecht, und in der Bundesrepublik Deutschland ist ein solcher Schutz ebenfalls verfassungsrechtlich verankert (*Busch*/*Jakobi* 2011). Zum anderen haben eine Reihe von Menschenrechtsgruppen (sowohl traditionelle wie auch neu entstandene) sich des Themas Privatheitsschutz im Bereich der Informations- und Telekommunikationstechnologie angenommen und fordern eine Berücksichtigung ihrer Interessen bei Entscheidungen der regulativen Politik.

Die ersten beiden Untersuchungsthemen fokussieren auf Bereiche, die eher spezielle Interessen als die Gesamtbevölkerung betreffen. Aus der Literatur ist aber bekannt, dass die Anreize für politisches Engagement mit der Größe von Gruppen variieren (*Olson* 1965). Das dritte Untersuchungsthema behandelt deshalb einen Bereich, der alle Bürger eines Landes betrifft, nämlich die Einführung von Pässen und Personalausweisen mit biometrischen Merkmalen. Erfahrungen wie etwa der Fall der Volkszählung von 1983 in der Bundesrepublik Deutschland haben gezeigt, dass die Massenmobilisierung von Protest zum Schutz von Privatheitsinteressen möglich ist (*Pfetsch* 1986); ob es auch im Fall der neuen Technologien zu Protestbewegungen kommen wird, ist deshalb von besonderem Interesse.

Die Auswahl der Untersuchungsländer (Bundesrepublik Deutschland, Großbritannien, Schweden und die Vereinigten Staaten) ist geleitet von dem Bestreben, innerhalb einer Gruppe relativ ähnlicher Fälle die Variation zu maximieren. Innerhalb des Grundansatzes eines „most similar systems"-Designs (*Przeworski/Teune* 1970) unterscheiden sich diese Länder hinsichtlich einer ganzen Reihe potentiell erklärungskräftiger politischer Variablen wie etwa in Bezug auf die staatliche Organisation (föderal versus unitarisch), die dominante Regierungspartei über die letzten Jahrzehnte, die Unabhängigkeit parlamentarischer Ausschüsse von der Regierung, den Typ des Rechtssystems sowie die Länge der Mitgliedschaft in der Europäischen Union. Die Vereinigten Staaten von Amerika sind als einziges OECD-Land ohne eine Behörde zum Datenschutz ein Ausnahmefall (*Bennett*/*Raab* 2006, S. 137), und sie unterscheiden sich im Hinblick auf die rechtliche Konzeption eines Schutzes von Privatheit deutlich von den Ländern der Europäischen Union (*Busch* 2006). Die Bundesrepublik Deutschland und Großbritannien sind zwei Mitgliedsländer der Europäischen Union, die in der Vergangenheit bei innereuropäischen Verhandlungen oft die Pole besonders hohen beziehungsweise besonders niedrigen Schutzes für Privatheit vertreten haben – etwa im Fall der Europäischen Datenschutzrichtlinie zu Beginn der 1990er Jahre (*Heisenberg* 2005, S. 64f.). Schweden schließlich ist mit einer langen Tradition von Transparenz-Gesetzgebung ein besonders interessanter Fall, da diese in einem potentiellen Spannungsverhältnis mit den Zielen von Daten- und Privatheitsschutz steht.

Insgesamt ergibt ein solches Forschungsdesign eine Matrix aus 3 Themen mal 4 Ländern, mithin 12 detaillierte Fallstudien. Das Design hat den Vorteil, dass die Fälle in zwei Dimensionen – also sowohl hinsichtlich der Themen wie auch hinsichtlich der Länder – auf Ähnlichkeiten und Unterschiede untersucht werden können, was es erlaubt, die Zahl der untersuchten Fälle zu steigern, ohne den Vorteil einer fall-orientierten Analyse (nämlich die Detailkenntnis) zu verlieren (*Levi-Faur* 2006). Damit wird es auch möglich, zwei in der Literatur konkurrierende Hypothesen zu testen, nämlich die Frage, ob in diesem Bereich eher spezifisch nationale, institutionelle und historische Charakteristika eines Landes (*policy styles*, vgl. *Richardson* u.a. 1982) bestimmenden Einfluss auf die Politikergebnisse haben, oder ob die *policy networks*, die sich auf supra- und internationaler Ebene entlang bestimmter Politiksektoren und -themen bilden, durch Diffusions- und Lerneffekte entscheidend wirken und so den Einfluss nationaler Netzwerke und Bestimmungsfaktoren übertreffen (*Freeman* 1986).

4. Die Herausforderung etablierter Datenschutzregimes durch technische Entwicklungen

Wie haben die Datenschutzregimes in den vier untersuchten Ländern auf durch technologische Entwicklungen ermöglichte Ausweitung personenbezogener Daten in den hier betrachteten drei Bereichen reagiert? Im folgenden Abschnitt werden diese Reaktionen zunächst überblicksartig nach den drei Themenbereichen geschildert, bevor eine zusammenfassende Analyse folgt.

4.1 CCTV: Kameras im öffentlichen Raum

Die Verbreitung von Kameras im öffentlichen Raum variiert zwischen den vier untersuchten Ländern erheblich. Genaue statistische Kennzahlen sind von öffentlicher Seite zwar für keines der Länder erhältlich, aber Angaben in der Literatur von kompetenter Seite deuten darauf hin, dass beispielsweise die Zahl der in der Bundesrepublik Deutschland installierten CCTV-Kameras lediglich ein Zehntel der in Großbritannien vorhandenen beträgt: 400.000 versus über 4 Millionen (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* 2004, S. 80).

Die vergleichsweise geringe Zahl von CCTV-Kameras in Deutschland erweist sich bei genauer Untersuchung als das Produkt vor allem zweier Faktoren: zum einen besteht durch das Bundesdatenschutzgesetz ein umfassender regulativer Rahmen, der (nicht zuletzt durch eine Initiative der Konferenz deutscher Datenschutzbeauftragter im Jahr 2000[15]) Videoüberwachung im öffentlichen Raum auf so genannte „Kriminalitätsbrennpunkte" beschränkt – und dabei auch das verfassungsrechtlich abgesicherte Recht auf „informationelle Selbstbestimmung" berücksichtigt;[16] zum anderen liegt die Polizeikompetenz in der Hoheit der Bundesländer, was eine zentral gesteuerte Initiative zur landesweiten Einführung einer solchen Technologie unmöglich machte.

Der deutlichste Kontrastfall dazu ist der Großbritanniens. Hier wurde zu Beginn der 1990er Jahre von der damaligen konservativen Regierung die Einführung von CCTV-Kameras als zentrale Strategie gegen andauernd ansteigende Kriminalität ausgewählt und unter Einsatz großer Investitionsmittel umgesetzt. Die Zentralregierung stellte insgesamt 500 Mio. £ (etwa 80 Prozent des Budgets zur Kriminalitätsbekämpfung des Home Office) zur Verfügung (*House of Lords Select Committee on the Constitution* 2009) und verteilte dieses Geld unter den regionalen Polizeidirektionen vermittels eines Wettbewerbs. Erleichtert wurde diese massive Verbreitung von Kameras im öffentlichen Raum durch den Umstand, dass es lange Zeit keine Regulierung für diese Technologie gab, da der Data Protection Act von 1984 diese nicht erfasste. Der flächendeckenden Einführung standen also wenig Hindernisse entgegen; angesichts des starken politischen Drucks hatte man sich allerdings auch keine Gedanken über die Effektivität von CCTV-Kameras gemacht, und nachträgliche Evaluationen des Innenministeriums kamen zu weitgehend negativen Einschätzungen (*Gill*/*Spriggs* 2005). Erst im Jahr 2007 wurde zudem eine *National CCTV Strategy* beschlossen, die – unter anderem durch die Einführung verbindlicher technischer Standards sowie der Betonung von Interoperabilität – die Effizienz der Technologie verbessern sollte (*Gerrard* u.a. 2007).

Auch in Schweden sind CCTV-Kameras relativ weit verbreitet, doch der (ähnlich wie in Großbritannien) zentralisierte Staat hat bei deren Einführung eine vergleichsweise ge-

ringe Rolle gespielt. Bereits 1977 gab es eine gesetzliche Regulierung für diese Technologie, die zudem auch durch das schwedische Datenschutzgesetz erfasst wird (*Svenonius* 2004). Im Gegensatz zum britischen Fall liegt die Kompetenz zur Lizenzierung der Kameras jedoch auf der Ebene der Kommunen und Landkreise, und dieses „Wachstum von unten" sicherte sowohl die öffentliche Akzeptanz der Technologie wie auch die Effizienz ihres Einsatzes (vgl. *Gras* 2004).

Auch in den Vereinigten Staaten ist das Thema „Kameras im öffentlichen Raum" politisch nicht sehr umstritten, was an der vergleichsweise geringen Verbreitung der Technologie liegt. Versuche von Bürgerrechtsorganisationen wie der *American Civil Liberties Union* (ACLU), das Thema zu politisieren, haben bisher nicht zu staatlicher Regulierung geführt – und da es in den USA keinen gesetzlichen Datenschutz auf Bundesebene gibt, greift in Bezug auf CCTV-Kameras bisher keine gesetzliche Regulierung. Es gibt daher nur regional unterschiedliche Regulierungen auf kommunaler Ebene, unterschiedliche Gerichtsentscheidungen (*Lin* 2006, S. 137-139) und Selbstregulierung etwa durch die Standards der *American Bar Association*. Obwohl einer weiten Verbreitung der Technologie mithin wenig Hindernisse entgegenstehen, ist es bis jetzt dazu nicht gekommen, da auch die Faktoren fehlen, die eine solche Initiative auf der Ebene des Gesamtstaates vorantreiben könnten. In Großstädten wie New York, Washington D.C. oder Chicago hat jedoch in den letzten Jahren ein Anstieg der Zahl von CCTV-Kameras stattgefunden.

Zusammenfassend lässt sich sagen, dass sich im Falle von CCTV-Kameras die Variablen „Staatsstruktur" und „Existenz von Regulierung" als wichtige Erklärungsfaktoren für die Variation in der Verbreitung erweisen: In zentralisierten Staaten kann – entsprechender politischer Wille vorausgesetzt – die Einführung einfach umgesetzt werden, vor allem, wenn dem wenig regulative Hindernisse entgegenstehen; in föderalen Staaten hingegen, in denen die Polizeikompetenz zumeist auf der unteren Ebene angesiedelt ist, ist dies ohne gute Effizienz-Argumente kaum möglich, und bereits existierende Regulierungen können einem Ausbau zusätzlich entgegenstehen.

4.2 RFID: Automatisierte Identifikation von Gütern

Im Gegensatz zu CCTV-Kameras, die als Hilfsmittel zur Kriminalitätsbekämpfung vor allem von staatlicher Seite eingeführt wurden, ist die Verbreitung von RFID-Chips hauptsächlich das Resultat von Interessen im privatwirtschaftlichen Sektor. Auf die politische Agenda ist das Thema daher vor allem insoweit gekommen, als Reaktionen auf Regulierungswünsche – etwa durch Bürgerrechtsbewegungen – notwendig wurden. Dabei unterscheidet sich das Niveau der Politisierung des Themas im internationalen Vergleich deutlich.

In der Bundesrepublik Deutschland ist diese Politisierung als vergleichsweise gering einzuschätzen. Als politisches Problem taucht es erstmals im Jahr 2003 im Bericht des Datenschutzbeauftragten an den Deutschen Bundestag auf und zwei Jahre später konkretisiert durch die Verwendung von RFID-Chips im neuen elektronischen Reisepass und den Eintrittskarten zur Fußballweltmeisterschaft (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* 2007, S. 71f.). Die Bundesregierung war jedoch zögerlich, hier regulierend einzugreifen, und sowohl die Konferenz der Datenschutzbeauftragten wie auch die damaligen Oppositionsparteien Grüne und FDP forderten eine gesetzliche Regelung nur für den Fall, dass eine Selbstregulierung durch die Wirtschafts-

verbände scheitere. Nachdem der Bundesdatenschutzbeauftragte die Bundesregierung aufgefordert hatte, ihre Pläne in diesem Bereich offen zu legen, legte diese im Januar 2008 dem Bundestag einen Bericht vor, in dem sie den Sinn einer nationalen Regulierung in Zweifel zog und auf die Verhandlungen auf der Ebene der Europäischen Union verwies.[17]

Auch in den Vereinigten Staaten gibt es bis jetzt keine staatliche Regulierung im Bereich RFID-Chips, da die Federal Trade Commission (FTC) sich im März 2005 explizit für eine Selbstregulierung dieses Bereichs durch die Wirtschaft entschieden hat (*Hildner* 2006) und diese Haltung aufrecht erhält. Doch verglichen mit der Bundesrepublik ist es in den USA zumindest zeitweise zu einer erheblich höheren Politisierung und Standardisierung gekommen: hierzu haben vor allem Aktivisten wie die Konsumentenorganisation CASPIAN beigetragen, die die Technologie als „Spionage-Chips" brandmarkten und zum Boykott von diese nutzenden Unternehmen wie Benetton oder Gillette aufriefen.[18] Breite Unterstützung durch 35 Bürgerrechtsgruppen, die ein Moratorium für die Einführung der Technologie forderten, erhöhte den politischen Druck beträchtlich: Es kam zu Anhörungen im Kongress und zu Gesetzgebungsinitiativen sowohl auf staatlicher wie auf der Bundesebene, doch mit geringem Erfolg.[19] Ein wichtiger Grund hierfür ist die große Vielfalt von Einsatzgebieten für die Technologie und die daraus folgenden sehr unterschiedlichen Schwerpunkte der Gesetzesinitiativen, welche von Konsumentenschutz bis zur Regelung von RFID-Implantaten reichte. Wirtschaftsverbände argumentierten dagegen erfolgreich, eine voreilige Regulierung verhindere die Entfaltung des der Technologie innewohnenden Wachstumspotentials.

US-Aktivisten versuchten, ihren Protest gegen die RFID-Technologie nach Großbritannien zu exportieren, wo (wie in den USA Wal-Mart) vor allem große Handelsketten wie Tesco den Einsatz stark forcierten. Doch fand der Protest wenig Resonanz. Vielmehr rief der britische *National Consumer Council* lediglich dazu auf, die Datenschutz-Gesetzgebung an die neue Technologie anzupassen, und das Londoner Parlament beriet sehr abgewogen die Gefahren für die Privatheit, aber auch die neuen Geschäftsmöglichkeiten, die sich im Groß- und Einzelhandel durch RFID-Chips boten (*House of Commons* 2004, Spalte 284-292). Die Regierung, die die Technologie aktiv als zukunftsweisend förderte und bewarb, verweigerte sich einer restriktiven Regulierungen und sprach sich für eine Selbstregulierung auf der Ebene der Wirtschaft aus.

Förderten sowohl in Großbritannien wie in den USA große Wirtschaftsunternehmen die Einführung von RFID-Chips aktiv, so bildet die Entwicklung in Schweden in dieser Hinsicht einen markanten Kontrast: Die geringe Verbreitung der Technologie in diesem Land ist vor allem auf das Zögern von Handelsketten wie *Svensk Handel* oder *ICA* zurückzuführen, RFID-Chips im Konsumentenmarkt einzusetzen. Der Grund dafür waren Befürchtungen, es könne zu Protesten kommen, da Meinungsumfragen Sorgen in der Bevölkerung über den Eingriff der Technologie in die Privatsphäre festgestellt hatten (*Integritetsskyddskommittén* 2007,S. 78). Auch von staatlicher Seite erfuhr RFID-Technologie wenig aktive Unterstützung, so dass in Schweden die Abwesenheit von Promotoren die vergleichsweise geringe Verbreitung der Technologie erklären kann. Auch der Versuch der Liberalen Partei, das Thema auf die politische Tagesordnung zu bringen, führte nicht sehr weit – zumal auch die Partei von einer klaren Forderung nach gesetzlicher Regulierung angesichts der Kosten für Unternehmen absah (vgl. *Folkpartiet liberalerna* 2008).

Zusammenfassend lässt sich also feststellen, dass RFID-Technologie in den vier untersuchten Ländern (mit der qualifizierten Ausnahme Schwedens, wo sie nur in der Logis-

tik und nicht im Konsumentensektor eingesetzt wird) relativ ungehindert eingeführt werden konnte. Hierfür sind vor allem wirtschaftliche Interessen, die noch dazu zumeist von den Regierungen aus strategischen Gründen unterstützt wurden, verantwortlich. Versuche zur Skandalisierung und zur Mobilisierung von verbreitetem Protest gab es lediglich in den USA, und auch dort waren diese nur für einen geringen Zeitraum erfolgreich.

4.3 Biometrische Pässe und Ausweise

Die Einführung biometrischer Merkmale in Personalausweise und Reisepässe ist in vielen Ländern mit dem terroristischen Anschlägen vom 11. September 2001 auf die politische Agenda gekommen, da sie als probates Mittel gegen die Fälschung solcher Ausweispapiere und für die sichere Identifikation der sie benutzenden Individuen gilt. Doch auch andere Motive haben bei ihrer Einführung eine Rolle gespielt – im Falle Deutschlands gegen Ende der 1990er Jahre beispielsweise Initiativen zur Verwaltungsmodernisierung und zur Förderung von e-Commerce. Es gibt von diesem Thema also Verbindungen zu mehreren „policy streams“ (*Kingdon* 1995; *Rüb* 2009).

In der Bundesrepublik Deutschland gibt es seit jeher eine Pflicht zum Besitz von Personalausweisen, die seit den 1980er Jahren auch maschinenlesbar sind (*Hornung* 2005). Die Einführung biometrischer Ausweise und Pässe stellte daher im internationalen Vergleich nur eine relativ geringe Veränderung dar. Die Datenschutzbeauftragten des Bundes und der Länder problematisierten die geplante Einführung, doch erwiesen sich in der politischen Diskussion vor allem die Fragen der Informationszentralisierung und der Kosten als wichtig, da es hinsichtlich der biometrischen Merkmale eine Verpflichtung von EU-Seite gab. Nachdem in beiden Fragen für die Kritiker weitgehend zufrieden stellende Lösungen gefunden worden waren, erwies sich die Einführung der neuen Pässe als unproblematisch. Bei den geplanten neuen Personalausweisen wurde entschieden, die Aufnahme von Fingerabdrücken lediglich optional zu machen.

Die Vereinigten Staaten bilden mit einem hohen Maß an Politisierung bei diesem Thema einen deutlichen Kontrast zum Fall Deutschland. Da nur etwa ein Viertel der US-Bürger einen Reisepass besitzt und es historisch keine Ausweispflicht gibt, entzündete sich der Streit am Plan zur Einführung eines Personalausweises. Der REAL ID Act 2005, der angesichts drohender Opposition nur mit Verfahrenstricks verabschiedet werden konnte (*Ni/Ho* 2008; *Milberg* 2007), löste eine heftige Kontroverse aus und mobilisierte eine Koalition aus Gegnern, die von Bürgerrechtsgruppen bis zur konservativen Libertären reichte. Neben den entstehenden Kosten spielen hier vor allem Bedenken hinsichtlich der Kompetenzanmaßung der Bundesregierung eine Rolle. Durch massive Opposition auf der Ebene der Staaten wurde die Durchsetzung der Pläne für einen Personalausweis gestoppt, so dass es auch zehn Jahre nach den die Initiative auslösenden Terroranschlägen in den USA noch immer kein sicheres und verfälschungsfestes Identifikationsmittel gibt.

Auch in Großbritannien gibt es seit Mitte der 1950er Jahre keinen verpflichtenden Personalausweis mehr, und ähnlich wie in den USA hat der Versuch einer Wiedereinführung massive politische Kontroversen ausgelöst. Auch hier erwies sich die Einführung eines biometrischen Passes als unproblematisch, während die Pläne für einen Personalausweis (ID Card) bislang gescheitert sind. Hierfür sind zum einen politisch-taktische Gründe ausschlaggebend (die Konservative Partei wechselte ihre frühere Position und opponierte gegen die Einführung), vor allem aber der Plan eines umfassenden, zentralisierten

und computergestützten Identitäts-Registers, das mit der ID Karte eingeführt werden sollte. Experten befürchteten hierfür hohe Kosten und bezweifelten Sicherheit und technische Durchführbarkeit (*Davies*/*Hosein* 2005), was angesichts vergangener schlechter Erfahrungen mit von der britischen Regierung betriebenen zentralen IT-Großprojekten (vgl. *Dunleavy* u.a. 2008) in der Öffentlichkeit erhebliche Resonanz fand. Nach der Abwahl der Labour-Regierung wurde das Projekt durch die Regierung Cameron/Clegg gestoppt.

In Schweden gab es, ebenso wie in Großbritannien und den USA, vor 2001 keine Personalausweis-Pflicht. Identitätsdokumente wurden jedoch beispielsweise von Unternehmen für ihre Angestellten ausgegeben, vom *Swedish Standards Institute* zertifiziert und allgemein anerkannt. Obwohl der Staat sich mit der Übernahme dieser Aufgabe eine neue Kompetenz sicherte, kam es nicht zu einer Politisierung des Themas oder gar zu politischen Protesten. Vielmehr werden seit 2005 sowohl Pässe wie auch Personalausweise ausgegeben, die den EU-Vorschriften für biometrische Dokumente entsprechen. Der Verweis auf die auf der europäischen Ebene eingegangenen Verpflichtungen, den die Regierung als Rechtfertigung vorbrachte, reichte offenbar zur Legitimation dieses Schrittes.

Bei der Einführung biometrischer Merkmale in Pässe und Ausweispapiere ist es in den untersuchten Ländern in keinem Fall zu Protesten mit Massenmobilisierung gekommen. Die Legitimation dieser Neuerung stand im Gefolge der terroristischen Anschläge vom September 2001 wohl nicht grundsätzlich infrage. Politisch kontrovers diskutiert wurden vor allem die Themen Kosten und Datenzentralisierung. Wo es gelang, diese zu entschärfen, stieß die Einführung auf keine größeren Probleme – wie in der Bundesrepublik und Schweden. In Großbritannien führte ein Festhalten an den Plänen der Datenzentralisierung in Verbindung mit hoher Politisierung und einem Regierungswechsel zur Beendigung des Projekts der Einführung einer *ID card*. In den USA hingegen führten weniger das Kostenproblem als vielmehr verbreitete prinzipielle Opposition gegen die Schaffung eines nationalen Identitätdokuments zur andauernden Verschleppung der Pläne und zum Scheitern einer zeitnahen Umsetzung.

4.4 Die Reaktionen der untersuchten Länder

Soweit die Analyse nach Themengebieten. Wie aber sieht es aus mit den themenübergreifenden Charakteristika der vier untersuchten Länder hinsichtlich ihrer Reaktionen auf die Herausforderungen im Bereich des Schutzes von Privatheit? In wie weit können wir hier ländertypische Muster erkennen?

In der Bundesrepublik Deutschland zeigen die Fallstudien, dass das Thema Datenschutz als wichtiges Prinzip institutionell im politischen Prozess verankert ist und über das gesamte politische Spektrum der politischen Kräfte weitgehend akzeptiert wird. Diese Haltung mag ein Reflex auf die Tatsache sein, dass die deutsche Bevölkerung das Thema für wichtig hält, wie in Meinungsumfragen immer wieder bestätigt wird – auch im internationalen Vergleich. Obwohl die Politisierung der hier untersuchten Themen im Durchschnitt nur gemäßigt war, existiert ein erhebliches Potenzial in dieser Richtung, wie vor allem in den Debatten über die biometrischen Ausweise deutlich wurde. Was den Modus der Regulierung betrifft, so ist für den Fall Deutschland eine Präferenz für gesetzliche Regelungen zu konstatieren, die vorzugsweise auf der Ebene des Zentralstaates stattfindet.

In den Vereinigten Staaten hingegen spielt die Bundesebene keine Rolle in zwei der hier untersuchten drei Themenbereiche. Dies ist in erheblichem Maße die Folge der Mitte

der 1970er Jahre gescheiterten Institutionalisierung im Bereich Datenschutz, die zu mangelnder Kontinuität und Einseitigkeiten in den öffentlichen Diskursen über dieses Thema geführt hat. Eine in der amerikanischen politischen Kultur tief verwurzelte Skepsis gegenüber der Rolle zumal des Zentralstaates und dessen Kompetenzen hat sich damals ebenso durchgesetzt wie sie in den letzten Jahren den Versuch zur Einführung eines nationalen Personalausweises hintertrieben hat. Dabei sind in der Debatte bisweilen hysterische Züge zu konstatieren, und die Zersplitterung der Zuständigkeiten sowie die Vielfalt der involvierten Akteure macht eine kohärente Politik in diesem Bereich praktisch unmöglich.

Doch auch die gegenteilige Situation – ein hoch zentralisiertes politisches System praktisch ohne relevante Gegenakteure – führt nicht unbedingt zu regulativem Erfolg, wie das Beispiel Großbritannien zeigt. Die technokratischen Lösungsträume in den Bereichen CCTV-Kameras und nationales Identitätregister fügen sich gut in die Analysen des britischen regulativen Staates als gekennzeichnet durch „high modernism" und „hyperinnovation" ein (*Moran* 2003), und auch ihr allenfalls mäßiger Erfolg erweist sich als durchaus nicht untypisch für das Land. Angesichts dieser starken Rolle des Staates mag die sektorübergreifende Präferenz für den Modus der Selbstregulierung zunächst erstaunen, ist aber durch tiefe Verwurzelung im britischen politischen Denken zu erklären.

In Schweden fällt im Kontrast dazu das dem Staat entgegengebrachte Vertrauen der Bürger bei der Regulierung des Schutzes von Privatheit auf, das sich in einer ausgesprochen niedrigen Politisierung dieses Themenbereiches niederschlägt. Dass dies nicht auf Ignoranz oder Sorglosigkeit zurückgeführt werden kann, zeigt sich in den oft bereits zu einem sehr frühen Zeitpunkt vorgenommenen Regulierungen, die von staatlicher Seite oft bereits eingeführt zu werden scheinen, bevor sich eine allgemeine Problemperzeption bildet. Der schwedische Staat kann also als „vorausschauend" oder „fürsorglich" charakterisiert werden, und dem entspricht eine Präferenz für Gesetze als Regulierungsmodus.

5. Schluss

Die vorangegangenen Abschnitte des Aufsatzes haben deutlich gemacht, dass die zwölf hier kurz in ihren Ergebnissen zusammengefassten Fallstudien erhebliche Unterschiede sowohl hinsichtlich der politischen Dynamiken wie auch in Bezug auf die Regulierungsergebnisse aufweisen – trotz des gemeinsamen Bezuges auf die Thematik Regulierung von personenbezogenen Daten und Privatheit. Im Hinblick auf die weiter oben erwähnten konkurrierenden Theorien, die Ähnlichkeiten entweder vor allem entlang nationaler oder aber entlang sektoraler Linien erwarten ließen, scheint daher keine Entscheidung möglich: Weder in die eine noch in die andere Richtung der Fallstudien-Matrix lassen sich offenkundige systematische Ähnlichkeiten erkennen.

Tabelle 1: Regulierungsmodi der 12 Fallstudien

	CCTV	RFID	Biometrische Ausweise
Deutschland	gesetzlich	keine / Delegation an EU	gesetzlich
Großbritannien	gesetzlich + Selbstregulierung	Selbstregulierung	gesetzlich
Schweden	gesetzlich	keine / Delegation an EU	gesetzlich
Vereinigte Staaten	Selbstregulierung	(gesetzlich) [Ebene der Einzelstaaten]	gesetzlich

Betrachtet man die Fallstudien im Hinblick auf die Modi der Regulierung (vgl. Tabelle 1), so zeigt sich sowohl nach Ländern wie nach Themenbereichen eine Mischung von gesetzlicher Regulierung, Selbstregulierung und Abwesenheit von Regulierung bzw. Delegation derselben an die europäische Ebene. Die einzige Ausnahme bildet der Bereich biometrische Ausweise, für deren Einführung bzw. Änderung durchgängig eine gesetzliche Grundlage erforderlich ist, da der Bereich einen Kern staatlicher Hoheitlichkeit betrifft. Doch auch hier sind jenseits dieser eher formalen Ähnlichkeit erhebliche Unterschiede im Detail aufgetreten, wie weiter oben ausgeführt wurde.

Einen Hauptunterschied stellt hierbei das Ausmaß an Politisierung dar, und deren deutliche Variation lässt sich auch für die Matrix der Fallstudien als ganze zeigen (vgl. Tabelle 2). In fast allen untersuchten Ländern (mit der Ausnahme Schwedens) gab es zum Teil erheblichen politischen Streit um die Einführung bzw. Regulierung von personenbezogene Daten produzierenden Technologien. Dass die Umstrittenheit ausgerechnet im Bereich der biometrischen Ausweisdokumente im Schnitt am höchsten liegt, deutet darauf hin, dass ein Grund für die Einbeziehung dieses Themenfeldes, nämlich die auf *Olson* (1965) zurückgehende Erkenntnis unterschiedlicher politischer Mobilisierungsanreize für Themen, die nur kleine Gruppen betreffen und solchen, die die gesamte Bevölkerung betreffen, sich als valide herausgestellt hat.

Tabelle 2: Ausmaß der Politisierung der 12 Fallstudien

	CCTV	RFID	Biometrische Ausweise
Deutschland	Mittel	mittel	erheblich
Großbritannien	Gering	gering	erheblich
Schweden	Gering	keine	keine
Vereinigte Staaten	Gering	erheblich	erheblich

Dennoch bleibt auch eine solche Erkenntnis unbefriedigend, wenn gleichzeitig eingeräumt werden muss, dass für die deutlichen Unterschiede in der Politisierung der verschiedenen Fallstudien keine systematische Erklärung angeboten werden kann. Der Grund dafür liegt allerdings hauptsächlich darin, dass die Literatur zur Entstehung politischen Protests sehr unterschiedliche Erklärungsmodelle anbietet (vgl. etwa *McAdam*/*McCarthy*/*Zald* 1996), es aber keine systematisch erhobenen Daten zu privatheitsbezogenen Protesten gibt, die einen empirischen Test zwischen den miteinander im Wettstreit liegenden Ansätzen erlauben würden.

So kann das unterschiedliche Ausmaß an Politisierung wohl am ehesten mit Bezug auf das Ausmaß an Vertrauen bzw. Misstrauen erklärt werden, mit dem die Bürger dem Staat begegnen. Hier gibt es, wie die Fallstudien insbesondere im Bereich der biometrischen Ausweispapiere zeigen (freilich ein Gebiet, in dem der Staat besonders stark involviert ist), deutliche Unterschiede. Das Vertrauen in den Staat scheint am höchsten in Schweden zu sein, wo es trotz einer erheblich gestiegenen Rolle des Staates noch nicht einmal Ansätze zu Kritik gab; in Deutschland wurden die Reformvorschläge der Regierung kritisch geprüft, die in der Debatte erreichten Kompromisse hinsichtlich der zentralisierten Speicherung biometrischer Daten und geringer Kosten dann jedoch nicht mehr in Frage gestellt. In Großbritannien basierten Einwände gegen die Pläne der Regierung hauptsächlich auf rationaler Kritik, die jedoch ignoriert wurden (was auch möglich war, da die Regierung nicht auf die Zustimmung anderer Akteure angewiesen war). In den Vereinigten Staaten entsprachen die Behauptungen über die Motive der Regierung bei

den Plänen für REAL ID und RFID im allgemeinen hingegen sicher nicht immer dem Standard rationaler Kritik (vgl. *Albrecht*/*McIntyre* 2006); doch ist dies im amerikanischen politischen Diskurs keine Ausnahme, gibt es in dieser Hinsicht doch eine ehrwürdige Tradition im Lande (*Hofstadter* 1996).[20]

Anhand dieses Beispiels wird noch einmal deutlich, was die kurze Darstellung der zwölf Fallstudien insgesamt vor Augen führt: Sowohl Politikentwicklung wie Politikergebnisse im Bereich der Regulierung von Privatheit scheinen stark kontextabhängig zu sein. Im Gegensatz zu den eingangs des Artikels erwähnten Erwartungen haben sich systematische Ähnlichkeiten weder entlang von Ländercharakteristika noch in Bezug auf die untersuchten Technologien ergeben. Man muss deshalb die Frage stellen, ob so etwas wie „privacy policy" als Politikfeld vielleicht nur in der Vorstellung des politikwissenschaftlichen Analytikers existiert, wenn man in der Wirklichkeit keine Hinweise auf entsprechende Gemeinsamkeiten findet? Offenbar führen ja die in Bezug auf die Kategorie „Privatheit" bestehenden theoretischen Gemeinsamkeiten der hier untersuchten Politikepisoden nicht zu Gemeinsamkeiten im politischen Handeln – was auch die Frage aufwirft, ob man überhaupt von der Existenz von Regimes in diesem Bereich ausgehen kann. Es scheint, als ob man eher von *issue networks* sprechen kann, da die Zusammensetzung der Akteure und ihre Involviertheit zwischen den einzelnen hier untersuchten Themen doch erheblich variiert.

Weniger pessimistisch fällt die abschließende Bewertung mit Hinblick auf die Theorieansätze der Staatstätigkeitsforschung aus. Zwar sind auch hier keine alle untersuchten Fälle abdeckenden Gemeinsamkeiten zu konstatieren, doch ist dies als Nachweis für die Relevanz der Theorieansätze auch im nicht-sozioökonomischen Bereich ja auch nicht notwendig. Zumindest können eine Reihe von relevanten Aussagen gemacht werden:

- So wird etwa mit Bezug auf den *Parteienwettbewerb* deutlich, dass dieser in den hier untersuchten Fällen wenig Einfluss auf die Positionen von Regierung und Opposition gehabt hat. Eine Ausnahme von dieser Regel stellt der Fall der geplanten ID Cards in Großbritannien dar: dieses Projekt wurde von der *Conservative Party* seit 2007 politisiert und nach der Regierungsübernahme durch Premierminister David Cameron im Frühjahr 2010 gestoppt. Doch im Allgemeinen gilt, dass die Details der Regulierung in diesem Bereich komplex und durch eine Vielzahl technischer Argumente beeinflusst sind und sich daher schlecht für eine (Partei-)Politisierung eignen – eine generelle Erkenntnis im Bereich der regulativen Politik, die auch damit zusammenhängt, dass die politischen *issues* in diesem Bereich keine distributiven Konsequenzen haben.
- *Institutionelle Variablen* beeinflussen die Politikentwicklung in den hier betrachteten Fällen offenbar erheblich und können somit einen Erklärungsbeitrag bei der Analyse leisten. So haben beispielsweise die Existenz von Föderalismus und das Ausmaß an Zentralisierung von staatlicher Entscheidungsmacht in den Fällen CCTV und RFID eine wichtige Rolle gespielt; CCTV-Kameras haben bisher weite Verbreitung nur in unitarischen Staaten wie Großbritannien und Schweden gefunden, während in föderalen Systemen wie der Bundesrepublik Deutschland oder den Vereinigten Staaten die „push"-Faktoren auf der zentralstaatlichen Ebene aufgrund der Kompetenzverteilung zwischen den staatlichen Ebenen fehlten.
- *Pfadabhängigkeit* (also der Einfluss von in der Vergangenheit getroffenen Entscheidungen) ist in einer Reihe von Fallstudien zu diagnostizieren, am stärksten mit Bezug

auf die Institutionalisierung von Datenschutzbeauftragten. Sofern diese stattfand (in den hier untersuchten Ländern im Lauf der 1970er Jahre), führte sie zu einer Beeinflussung des öffentlichen Diskurses und oft zu einer stärkeren Berücksichtigung von datenschutz-affinen Positionen; scheiterte die Errichtung einer Datenschutzbehörde (wie in der Untersuchungsgruppe nur in den Vereinigten Staaten der Fall), dann fehlte zum einen ein Standpunkt in der öffentlichen Debatte (mit entsprechend zu den eben geschilderten entgegengesetzten Ergebnissen); daneben fehlte aber auch ein konsistenter Ansprechpartner für die internationalen Verhandlungen im Bereich Datenschutz, die seit Ende der 1990er Jahre von zunehmender Wichtigkeit gewesen sind (vgl. *Busch* 2010).

Auch außerhalb ihres *home turf* im Bereich der Analyse sozio-ökonomischer Zusammenhänge besitzen diese Theorieansätze der vergleichenden Staatstätigkeitsforschung mithin eine Erklärungskraft. Ihre Reichweite genauer auszuloten wird eine Aufgabe zukünftiger Forschung sein.

Anmerkungen

1 Dieser Artikel entstand im Zusammenhang von Forschung, die durch den britischen Economic and Social Research Council im Rahmen des Drittmittelprojekts „Coping with innovation: The political regulation of personal information in comparative perspective“ (RES-062-23-0536) gefördert wurde. Die empirischen Informationen befinden sich auf dem Stand vom Frühjahr 2010. Mein Dank für Hilfen bei der Erforschung der schwedischen und britischen Fallstudien gilt Dr. Michael Koß und insbesondere Dr. Tobias Jakobi.

2 Vgl. etwa http://www.spiegel.de/wirtschaft/0,1518,605225,00.html (30.8.2010).

3 Vgl. http://www.spiegel.de/wirtschaft/0,1518,543431,00.html, http://www.spiegel.de/wirtschaft/0,1518,617723,00.html (Stand: 30.8.2010).

4 Vgl. beispielsweise http://www.wdr.de/themen/politik/nrw03/datenschutz/100317.jhtml (Stand: 30.8.2010).

5 Vgl. das Interview im *Wall Street Journal* vom 14. August 2010, online erhältlich unter: http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html?KEYWORDS=schmidt (Stand: 01.09.2010).

6 Siehe dazu das Interview der Ministerin auf der website ihres Ministeriums unter http://www.bmelv.de/cln_172/SharedDocs/Interviews/2010/2010-06-05-AI-Facebook-TheEuropean.html (Stand: 30.08.2010): „Mit dem Austritt ist das Thema für mich nicht erledigt“.

7 Interview *Süddeutsche Zeitung*, 1. März 2010.

8 Vgl. auch die diesbezügliche Einschätzung des Bundesbeauftragten für den Datenschutz: „In den vergangenen beiden Jahren hat der Datenschutz die öffentliche Diskussion in einem Maße geprägt, wie man es seit der Volkszählungsdebatte Anfang der achtziger Jahre des vorigen Jahrhunderts nicht mehr erlebt hat.“ (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* 2009, S. 16)

9 Siehe dazu den Bericht des House of Lords Select Committee zum Thema „Surveillance: Citizens and the State“ (*House of Lords Select Committee on the Constitution* 2009).

10 Siehe zur Problematik einführend etwa *Rossnagel* 2006.

11 Vgl. http://en.wikipedia.org/wiki/Internet#Growth (Stand: 24.08.2009).

12 Einen guten Überblick zu diesen Theorieangeboten bieten Kap. 2 bis 7 von *Schmidt* u.a. 2007.

13 Siehe als einführenden Überblick zu RFID-Chips etwa *Royal Academy of Engineering* 2007; *Glasser* u.a. 2007.

14 Vgl. als einführenden Überblick *Gill* 2003; *Kammerer* 2008.

15 Vgl. den Bericht des Bundesbeauftragten für Datenschutz für die Jahre 1999-2000, abgedruckt in *Bundestags-Drucksachen*, 14/5555 vom 13. März 2001, S. 223-224.

16 Zur Entstehung dieses Rechts vgl. *Busch*/*Jakobi* 2011.

17 Vgl. Bundestag Drucks. 16/7891 vom 23.1.2008, zugänglich unter http://dip21.bundestag.de/dip21/btd/16/078/1607891.pdf (Stand: 06.09.2009).

18 Die Argumentation der Aktivisten wird ausführlich dargestellt in *Albrecht*/*McIntyre* 2005, den beiden Gründerinnen von CASPIAN. Es ist wohl eine US-amerikanische Besonderheit, dass es von dem Buch auch eine gesonderte Ausgabe gibt, die sich eigens an Christen wendet und RFID-Chips in Verbindung bringt mit apokalyptischen Bibel-Prophezeiungen aus Kapitel 13 der Offenbarung des Johannes. Dort ist nämlich die Rede von „Malzeichen" eines Ungeheuers, ohne das „niemand kaufen oder verkaufen kann", und das sind nach Ansicht der Autorinnen RFID-Chips (*Albrecht*/*McIntyre* 2006).

19 Allerdings gab es Regulierungsversuche auf der Ebene der Staaten. Ausweislich der website der *National Conference of State Legislatures* (http://www.ncsl.org/default. aspx?tabid=13451, Stand 28.6.2011), bei der man Details über die Gesetzgebung der Staaten einsehen kann, haben im Jahr 2005 mindestens 12 Staaten Gesetze zum Schutz von Privatheit im Bereich von RFID-Chips erlassen; 2006 waren es 17, 2007 13 und 2008 20 Staaten.

20 *Hofstadter* (1996 S. 3) spricht in seinem ursprünglich aus dem Jahr 1963 stammenden Essay von „heated exaggeration, suspiciousness, and conspiratorial fantasy".

Literatur

Albrecht, Katherine/*McIntyre, Liz*, 2005: Spychips. How major corporations and government plan to track your every move with RFID, Nashville, TN: Nelson Current.

Albrecht, Katherine/*McIntyre, Liz*, 2006: The spychips threat. Why Christians should resist RFID and electronic surveillance, Nashville, TN: Nelson Current.

Bennett, Colin J., 1991a: How States Utilize Foreign Evidence, in: Journal of Public Policy, 11, S. 31-54.

Bennett, Colin J., 1991b: Review Article: What is Policy Convergence and What Causes It?, in: British Journal of Political Science, 21, S. 215-233.

Bennett, Colin J., 1992: Regulating privacy: Data protection and public policy in Europe and the United States, Ithaca: Cornell University Press.

Bennett, Colin J., 2008: The privacy advocates: Resisting the spread of surveillance, Cambridge, Mass.: MIT Press.

Bennett, Colin J./*Howlett, Michael*, 1992: The lessons of learning: Reconciling theories of policy learning and policy change, in: Policy Sciences, 25 (3), S. 275-294.

Bennett, Colin J./*Raab, Charles D.*, 2006: The governance of privacy: Policy instruments in global perspective, Cambridge, MA, London: MIT Press.

Braun, Dietmar/*Busch, Andreas*, 2000: A Reassessment of Public Policy and Political Ideas, in: *Braun, Dietmar*/*Busch, Andreas* (Hrsg.), Public policy and political ideas, Cheltenham: Elgar, S. 189-199.

Busch, Andreas, 2006: Verfassungspolitik in der Bundesrepublik, in: *Schmidt, Manfred G./Zohlnhöfer, Reimut* (Hrsg.), Regieren in der Bundesrepublik Deutschland, Wiesbaden: VS Verlag für Sozialwissenschaften. S. 33-56.

Busch, Andreas, 2009: Regulatory regimes under stress: Protecting privacy in Germany and the United States. Paper presented to the panel "Networks of regulation and the management of transnational risk" at the 5th ECPR General Conference, Potsdam, Sept. 10-12, 2009.

Busch, Andreas, 2010: The Regulation of Privacy, Jerusalem Papers in Regulation & Governance, No. 26. Online verfügbar unter: http://regulation.huji.ac.il, Stand: 28.06.2011.

Busch, Andreas/*Jakobi, Tobias*, 2011: Die Erfindung eines neuen Grundrechts: Zu Konzept und Auswirkungen der „informationellen Selbstbestimmung", in: *Hönnige, Christoph/Kneip, Sascha/Lorenz, Astrid* (Hrsg.), Verfassungswandel im Mehrebenensystem, Wiesbaden: VS Verlag für Sozialwissenschaften, S. 297-320.

Davies, Simon/*Hosein, Gus*, 2005: The Identity Project. An assessment of the UK Identity Cards Bill and its implications, Department of Information Systems, London School of Economics and Political Science, London (Hrsg.).Online verfügbar unter: http://is.lse.ac.uk/idcard/identityreport.pdf, Stand: 09.03.2010.

Denninger, Erhard, 2002: Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz, in: Aus Politik und Zeitgeschichte, 10-11, S. 22-30.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2007: Tätigkeitsbericht 2005-2006. 21. Tätigkeitsbericht, Bonn.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2009: Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008, 22. Tätigkeitsbericht, Bonn.

Ditton, Jason/*Short, Emma*, 1999: Yes, it works – no, it doesn't: Comparing the effects of open-street CCTV in two adjacent town centres, in: Crime Prevention Studies 10, S. 201-223.

Dolowitz, David/*Marsh, David*, 1996: Who Learns What from Whom: A Review of the Policy Transfer Literature, in: Political Studies, 44, S. 343-357.

Dunleavy, Patrick/*Margetts, Helen*/*Bastow, Simon*/*Tinkler, Jane*, 2008: Digital era governance. IT corporations, the state, and e-government. Oxford: Oxford University Press.

Folkpartiet liberalerna, 2008: Integritet i en ny tid: Integritetspolitikt program för folkpartiet liberalerna, Stockholm.

Freeman, Gary P., 1986: National Styles and Policy Sectors: Explaining Structured Variation, in: Journal of Public Policy, 5 (4), S. 467-496.

Gerrard, Graeme/Parkins, Garry/Cunningham, Ian/Jones, Wayne/Hill, Samantha/Douglas, Sarah, 2007: National CCTV Strategy, London: Home Office and Association of Chief Police Officers.

Gill, Martin (Hrsg.), 2003: CCTV, Leicester: Perpetuity Press.

Gill, Martin/*Spriggs, Angela*, 2005: Assessing the impact of CCTV, Home Office research study, London: Home Office Research Development and Statistics Directorate.

Glasser, Dara J./*Goodman, Kenneth W.*/*Einspruch, Norman G.*, 2007: Chips, tags and scanners: Ethical challenges for radio frequency identification, in: Ethics and Information Technology, 9, S. 101-109.

Gras, Marianne L., 2004: The Legal Regulation of CCTV in Europe, in: Surveillance and Society, 2 (2/3).

Heisenberg, Dorothee, 2005: Taking a second look at Germany's motivation to establish economic and monetary union: A critique of "economic interests" claims, in: German Politics, 14 (1), S. 95-109.

Heisenberg, Dorothee/*Fandel, Marie-Hélène*, 2004: Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard, in: *Braman, Sandra* (Hrsg.), The emergent global information policy regime, International political economy series, Basingstoke: Palgrave Macmillan, S. 109-129.

Hildner, Laura, 2006: Defusing the Threat of RFID: Protecting Consumer Privacy through Technology-Specific Legislation at the State Level, in: Harvard Civil Rights-Civil Liberties Law Review, 41 (1), S. 133-176.

Hofstadter, Richard, 1996: The paranoid style in American politics, and other essays. Cambridge/Mass: Harvard University Press.

Hornung, Gerrit, 2005: Die digitale Identität. Der elektronische Rechtsverkehr, Bd. 10, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden: Nomos.

House of Commons, 2004: House of Commons Debates, Her Majesty's Stationery Office, January 27.

House of Lords Select Committee on the Constitution, 2009: Surveillance: Citizens and the State. Volume I: Report, The Stationery Office Limited, HL Paper, 18-1.

Integritetsskyddskommittén, 2007: Skyddet för den personliga integriteten: kartläggning och analys. Delbetänkande, del 1, SOU 2007, 22, Stockholm: Fritze.

International Telecommunication Union, 2009: Measuring the information society: The ICT Development Index, Geneva: International Telecommunication Union.

Kammerer, Dietmar, 2008: Bilder der Überwachung, Frankfurt a.M.: Suhrkamp.

Kingdon, John W., 1995: Agendas, alternatives, and public policies, 2. Aufl., New York: Longman.

Levi-Faur, David, 2006: Varieties of Regulatory Capitalism: Getting the Most Out of the Comparative Method, in: Governance, 19(3), S. 367-382.

Lin, Chen-Yu, 2006: Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland: Ein Drei-Länder-Vergleich, Dissertation, Georg-August-Universität Göttingen. Online verfügbar unter: http://webdoc.sub.gwdg.de/diss/2006/lin/lin.pdf, Stand: 28.06.2011.

Mayer-Schönberger, Viktor, 2009: Delete: The virtue of forgetting in the digital age, Princeton, NJ: Princeton University Press.

McAdam, Doug/*McCarthy, John D.*/*Zald, Mayer N.* (Hrsg.), 1996: Comparative perspectives on social movements. Political opportunities, mobilizing structures, and cultural framings, Cambridge: Cambridge University Press.

Milberg, Debra, 2007: The National Identification Debate. Real ID and Voter Identification, in: I/S: A Journal of Law and Policy for the Information Society, 3 (3), S. 443-472.
Moran, Michael, 2003: The British regulatory state: high modernism and hyper-innovation, Oxford: Oxford University Press.
Newman, Abraham L., 2008: Protectors of privacy: Regulating personal data in the global economy, Ithaca u. a.: Cornell University Press.
Ni, Anna Ya/*Ho, Alfred Tat-Kei*, 2008: A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform, in: Public Administration Review, 68 (5), S. 1063-1078.
Olson, Mancur, 1965: The logic of collective action. Public goods and the theory of group, Cambridge, Mass.: Harvard University Press (Harvard economic studies).
Pfetsch, Barbara, 1986: Volkszählung '83: Ein Beispiel für die Thematisierung eines politischen Issues in den Massenmedien, in: *Klingemann, Hans-Dieter*/*Kaase, Max* (Hrsg.), Wahlen und politischer Prozeß: Analysen aus Anlaß der Bundestagswahl 1983, Opladen: Westdeutscher Verlag, S. 201-231.
Pierson, Paul, 2000: Increasing Returns, Path Dependence, and the Study of Politics, in: American Political Science Review, 94 (2), S. 251-267.
Pierson, Paul, 2004: Politics in Time: History, Institutions, and Social Analysis, Princeton, NJ, Oxford: Princeton University Press.
Przeworski, Adam/*Teune, Henry*, 1970: The Logic of Comparative Social Inquiry, New York/London/Toronto/Sidney: Wiley-Interscience.
Regan, Priscilla M., 1993: The Globalization of privacy: Implications of recent changes in Europe, in: American Journal of Economics and Sociology, 52, S. 257-274.
Regan, Priscilla M., 1995: Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill, London: University of North Carolina Press.
Richardson, Jeremy J./*Gustafsson, Gunnel*/*Jordan, Grant*, 1982: The Concept of Policy Style, in: Policy Styles in Western Europe, S. 1-16.
Royal Academy of Engineering, 2007: Dilemmas of Privacy and Surveillance: Challenges of Technological Change, London.
Rüb, Friedbert W., 2009: Multiple-Streams-Ansatz. Grundlagen, Probleme und Kritik, in: *Schubert, Klaus/ Bandelow, Nils C.* (Hrsg.), Lehrbuch der Politikfeldanalyse 2.0., vollständig überarb. und erw. Aufl., München: Oldenbourg (Lehr- und Handbücher der Politikwissenschaft), S. 348-376.
Sabatier, Paul A./*Jenkins-Smith, Henk* (Hrsg.), 1993: Policy change and learning. An advocacy coalition approach, Boulder, CO: Westview Press.
Schmidt, Manfred G., 1996: When parties matter: A review of the possibilities and limits of partisan influence on public policy, in: European Journal of Political Research, 30, S. 155-183.
Schmidt, Manfred G./*Ostheim, Tobias*/*Siegel, Nico A.*/*Zohlnhöfer, Reimut* (Hrsg.), 2007: Der Wohlfahrtsstaat: Eine Einführung in den historischen und internationalen Vergleich, Wiesbaden: VS Verlag für Sozialwissenschaften.
Schmidt, Vivien A., 2002: The Futures of European Capitalism, Oxford: Oxford University Press.
Shaffer, Gregory, 2000: Globalization and social protection: the impact of EU and international rules in the ratcheting up of U. S. privacy standards, in: Yale Journal of International Law, 25 (1), S. 1-88.
Svenonius, Ola, 2004: Surveillance Intensification - Privacy Simulation: Swedish Surveillance and its Basic Conditions, Master Thesis, Stockholm: Södertörns Högskola.
Tsebelis, George, 2002: Veto players: How political institutions work, New York/Princeton/NJ: Princeton University Press.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2004: Tätigkeitsbericht 2004, Kiel: Landeszentrum für Datenschutz.

Anschrift des Autors:
Prof. Dr. Andreas Busch, Universität Göttingen, Institut für Politikwissenschaft, Platz der Göttinger Sieben 3, 37073 Göttingen
E-Mail: andreas.busch@sowi.uni-goettingen.de