Martin Rost

Gegen große Feuer helfen große Gegenfeuer

Datenschutz als Wächter funktionaler Differenzierung

Worum geht es? Vordergründig um das gesteigerte Datenschutzrisiko, das durch die Nutzung von Bürgerportalen, Einheitlichen Ansprechpartnern und E-Government-Gateways sowie durch die Aktivitäten von Google Analytics besteht. Bringt man diese in einen Zusammenhang, dann zeigt sich nämlich, in welchem Ausmaß die Funktionstrennungen, die eine wesentliche Eigenschaft eines modernen Rechtsstaates kennzeichnen, durch Zugriff auf Personen(daten) aufgehoben werden. Was die eindeutige Personenkennziffer als zentrales Verkettungssymbol für Beziehungen von Personen und Organisationen nur verspricht, lösen diese aktuell betriebenen Projekte tatsächlich ein: An einigen wenigen Konzentratoren befinden sich sämtliche Daten und Kommunikationsbeziehungen der Menschen im komfortabel automatisierten Zugriff.

Warum ist das ein Problem? Die moderne Gesellschaft kennt, so lautet der erkenntniskritische Befund aktueller sozialwissenschaftlicher Theorien, keinen logisch zentralen Attraktor (mehr). Moderne Gesellschaft erschließt sich nicht hinreichend, wenn alles von DER Wirtschaft und DEM Kapital oder DER Politik oder DER Wissenschaft oder DEM Recht oder gar DER Religion aus analysiert wird. Sie zeichnet sich durch eine ganze Reihe von steuerungsunfähigen Intransparenzen aus, die sich nicht untereinander hierarchisch anordnen lassen. Man denke an die Unwägbarkeiten der Gewaltenteilung und die „checks and balances“, ebenso natürlich an die des Marktes, an die politisch konkurrierenden Programme und öffentlichen Meinungen sowie wechselnden politischen Führungen in den Verwaltungsspitzen oder an die verunsichernden wissenschaftlichen Diskurse oder künstlerischen Provokationen. Diese moderne Gesellschaft bietet einem Großteil der Menschen, überwiegend und in historischer Sicht, gute Lebens-, Gestaltungs- und Partizipationsbedingungen.

Eine Person kann und muss dabei verschiedene Rollen einnehmen, die in ihrer Vielgestaltigkeit zur Ausbildung der schützenswerten Individualität beitragen. Freiheit zeigt sich u.a. darin, dass gleiche Rollen in unterschiedlicher Form und, wichtiger noch, in unterschiedlichen Kontexten unabhängig voneinander, gestaltet werden können oder müssen. Es gibt derzeit keine zentrale gesellschaftliche Instanz, die das gesamte Tun ei-

nes einzelnen Menschen überblickt, dieses Tun zu einem schlüssigen Ganzen orchestriert und davon abweichendes Tun zur Rechenschaft zieht.[1] Gegenwärtig entstehen jedoch einige wenige Beobachtungsplätze, an denen sich die gesellschaftlich funktionalen und persönlich wünschenswerten Intransparenzen, durch automatisierbaren Zugriff auf die Daten der einzelnen Person, aufheben lassen. Für Gesellschaft kann diese Entwicklung eine zumindest teilweise Aufhebung funktionaler Differenzierung und somit einen Rückfall in eine stratifizierte Sozialstruktur bedeuten, für den Einzelnen das Entstehen eines freiheitsbedrohlichen latenten Rechtfertigungsdrucks.

Die angelaufene Industrialisierung der Verwaltung

Die europäischen Behörden sichten derzeit unter Hochdruck ihre Strukturen und Prozesse, um sie im Hinblick auf Kostenreduktion, Steuerbarkeit sowie technische Umsetzbarkeit zu optimieren. Die Beachtung der Rechtskonformität, welche die Grundlage einer jeden Verwaltungstätigkeit ist, gilt dabei zunehmend als lästige, abzuschüttelnde Pflicht, der man durch ruppige Reformen, etwa die Föderalismusreform II, beizukommen trachtet. Gesetze, Verordnungen und Zuständigkeiten werden umstandslos zusammengekloppt oder die im Weg stehend vorhandenen geschliffen und dann, wie die organisatorischen und technischen Prozesse auch, mit dem Ziel standardisiert, die Verwaltungstätigkeiten kostensenkend zu industrialisieren.[2]

Der Druck zur Technisierung von Verwaltungstätigkeiten besteht auch von außen, durch Wirtschaft, Bürger sowie durch technische Entwicklungen. So verlangt die EU-Dienstleistungsrichtlinie, dass bis Ende 2009 Gewerbetreibende ihre Gewerbeanträge mit in ganz Europa per Internet zugänglichen „Einheitlichen Ansprechpartnern“ (EAP) zentral abwickeln können sollen[3]. Wenn eine Behörde im Beantragungsprozess nicht innerhalb enger Fristen mit einer Entscheidung reagiert, soll eine Genehmigung als automatisch erteilt gelten.

Druck üben ferner die vom Bundesministerium des Inneren jüngst konzipierten Bürgerportale aus.[4] Bürgerportale (BP) sollen Bürgern, Verwaltungen sowie Unternehmen eine sichere Infrastruktur insbesondere zur E-Mail-Kommunikation über das Internet bieten, die den technischen Aufwand für den unumgänglichen Einsatz von Sicherheitsprogrammen insbesondere beim Bürger gering halten.

Und nicht zuletzt sind die Versprechen der Computerindustrie verführerisch, dass sich mit ihren Produkten die gesamte interne und externe Kommunikation der Verwaltungen, trotz immens steigender Anforderungen, transparenter, dadurch endlich überhaupt steuerbar und kostengünstiger über zentrale E-Government-Gateways (GG) abwickeln lassen. Das Herzstück der Government-Gateways ist ein „Nachrichtenbroker“ oder „Enterprise-Services-Bus“, über den sämtliche Kommunikationen, an der die Verwaltung eines Landes teilhat, zentral gesteuert und in die verschiedenen Formate unterschiedlicher Verfahren und Programme gewandelt und den Empfängern dann, typischerweise über WebServices, zugeleitet werden.

EAP, BP und GG fungieren somit als Konzentratoren von Datenbeständen und Datenflüssen für juristische und natürliche Personen sowie für Maschinen, die die Daten-

ströme untereinander steuern. Damit ist das Setup kommunikativ erreichbarer Entitäten vollständig abgedeckt, nämlich: Organisationen agieren über Einheitliche Ansprechpartner, Bürger über Bürgerportale, Maschinen über Government-Gateways. Da läuft eine technische Entwicklung in aller Breite an, die aus Sicht des Datenschutzes hoch brisant ist.

Datenschutz als Wächter funktionaler Differenzierung

Worin besteht die gesellschaftliche Funktion des Datenschutzes? Datenschutz wirkt darauf hin, dass die Kommunikationen zwischen Organisationen (öffentliche Verwaltungen, private Unternehmen, wissenschaftlich orientierte Praxen und Institute, private Interessensvereine) und ihrem Klientel (Bürger, Kunden, Patienten, Menschen) formbar sind. Formbar soll heißen, dass diese Kommunikationen unter Bedingungen stehen bzw. gestellt werden können. Datenschutzrechtlich muss deshalb jede Kommunikation auf einer Rechtsgrundlage (Gesetz, Vertrag, Einwilligung), die den Zweck und die gegenseitigen Zusicherungen ausweist, sowie datenschutztechnisch gesichert und datensparsam erfolgen.[5] Als Regulativ zwecks Herstellung materiellrechtlicher Bewertbarkeit derartiger Kommunikationen dienen der explizierte Zweck der Kommunikation, der wiederum die Zugänglichkeit der erhobenen und ausgetauschten Daten und der dabei zum Einsatz kommenden Prozesse voraussetzt („Transparenzgebot“), um deren Erforderlichkeit nachzuweisen. Die juristische Bewertung der Datenverarbeitung richtet sich nach der Rechtmäßigkeit der Kommunikation, die politisch letztlich auf eine faire Beziehung bzw. grundrechtlich auf eine Achtung der immer bedrohten Autonomie des Bürgers, des Kunden, des Patienten und des Menschen (als Subjekt und einzigartigem Individuum) durch die latent ihre Klientel imperialistisch vereinnahmenden Organisationen hinausläuft. Die Durchsetzung dieser Achtung auf Seiten der Organisation erfordert es, dass auch auf deren interne Speicherung und Nutzung von Informationen zur Formung von Kommunikation staatlicherseits Einfluss genommen wird. Diese normativen Anforderungen und technischen Umsetzungen bzw. Zusicherungen müssen deshalb so ausgestaltet sein, dass sie von einer unbeteiligt-neutralen, externen Instanz – d.h. konkret in Deutschland: den Datenschutzbeauftragten der Länder bzw. des Bundes sowie den Aufsichtsbehörden für den Privatbereich – geprüft und bei Verstößen sanktioniert werden können. Datenschutz soll verhindern, dass Kunden zu Marionetten privater Unternehmen, Bürger zu Befehlsempfängern öffentlicher Verwaltungen und Menschen zur Verfügungsmasse von Praxen bzw. wissenschaftlichen Institutionen werden, ohne dass deshalb Organisationen auf den Einsatz effizienter Informations- und Kommunikationsmaschinen verzichten müssen.

Die im vorigen Absatz hervorgehobene gesellschaftliche Funktion des Datenschutzes – nämlich dass dieser die Formbarkeit der Kommunikationen zwischen Organisationen und deren Klientel in den Blick nimmt – setzt voraus, dass Kommunikationen bzw. deren Inhalte und Formen, überhaupt konstruktiv zugänglich und nicht bedingungslos, etwa durch kulturelle und psychologisch verankerte Traditionen oder technische Vorkehrungen, unverrückbar festgezurrt sind. Kommunikationen lassen sich nur

unter rechtliche und operative Bedingungen stellen, wenn auf Datenflüsse tatsächlich operativ und regulativ Einfluss genommen werden kann, also wenn unterschiedliche Datenbestände vorhanden sind und entsprechend Datenströme aus unterschiedlichen Quellen über bestehende Grenzen der eigensinnigen Konstitution und des Prozessierens von Informationen hinweg erfolgen. Das setzt wiederum voraus, dass es stabile kommunikative Grenzen gibt.

Und von derartigen kommunikativen Grenzen gibt es bislang eine ganze Reihe. Zum einen lässt sich auf die kommunikative Grenze zwischen der rechtsorientierten öffentlichen Verwaltung und der kapitalverzinsungsorientierten privaten Wirtschaft verweisen, zum zweiten auf die durch Gewaltenteilung in Jurisdiktion, Legislative und Exekutive, ein Teil der Publizistik sei noch dazugegeben, konstituierten Grenzen des politischen Raumes. In den derzeitigen Verhandlungen über den Zuschnitt der neuen IT sehr praxiswirksam sind auch die Grenzen zwischen verschiedenen Organen der Kommunen, Länder und des Bundes, aber auch die zur EU und zu den Vereinten Nationen. In diesen Auseinandersetzungen geht es darum, dass zwischen den Institutionen auf Augenhöhe im gegenseitigen Zugriff und Auferlegen von Beschränkungen und Inanspruchnahmen kooperiert und nicht einseitig subordiniert werden kann.

Die Existenz weiterer sozialer Grenzen, die Kommunikationen und damit soziale Systeme generieren[6], behaupten die Sozialwissenschaften. So unterscheidet die moderne Soziologie zwischen a) Gemeinschaften der Interaktion und b) Organisationen, deren Mitglieder an der Reproduktion von Entscheidungen aus Entscheidungen beteiligt sind sowie c) Funktionssystemen der Gesellschaft, die funktional differenziert bestimmte eigensinnige Formen kommunikativer Erreichbarkeit bereitstellen.[7] Als die strukturell führenden gesellschaftlichen Funktionssysteme sind Ökonomie, Recht, Politik und Wissenschaft zu nennen. Diese gesellschaftlichen Funktionssysteme zeichnen sich dadurch aus, dass sie funktional separiert voneinander operieren, wonach bspw. politische Macht nicht umstandslos und verlustfrei auf Recht oder Zahlungen oder Wahrheitsdiskurse durchgreifen kann. Steuern sind wirtschaftlich nur Kosten, politisch dagegen Rohstoff für Gestaltungschancen. Es gibt kein übergeordnetes Funktionssystem, dem die anderen Systeme sich zu fügen haben. Diese gleich„berechtigten“ Sozialsysteme stören einander gegenseitig, sie müssen aus den Störungen ihrer Umwelten ihre eigenen Formen an Informationen konstruieren. Indem sie das tun, reproduzieren sie ihre Grenzen als spezifische Systeme.

Die Separation der Funktionssysteme in der Moderne hat zu einer ungeheuren Vielfalt und Komplexität sozialer Kommunikationen geführt, die durch Medienausbildungen unwahrscheinliche kommunikative Anschlüsse in wahrscheinliche Kopplungen transformieren. Diese Systeme haben, und das ist für den hier angesprochenen Aspekt wichtig, die kommunikativen Erwartungsschemata *des Bürgers, des Kunden und Subjekts* erst ausgebildet, die gesellschaftlich angeliefert als verallgemeinerte kommunikative Rollenschemata den Bezug zwischen Organisationen und ihrem Klientel regulieren, an denen sich dann die konkreten Rollenausgestaltungen mit konkreten Personen und deren psychischen Erwartungen orientieren. Der Bürger gilt als souverän, der sich trotzdem dem staatlichen Gewaltmonopol bzw. den Gesetzen zu unterwerfen hat; der Kunde gilt als Nutzen/Kosten-Optimierer, dessen entsprechend rationalen Präferenzen durch

verführerische Werbung und Verhandlungstricks beeinflusst werden dürfen; und der Mensch gilt als vernunftbegabt aber triebgeleitetes Individuum, das deshalb vielfach gegen die eigenen Interessen handelt. Und bei Mitarbeitern will man es nicht allzu genau wissen, wie es um deren Souveränität als Bürger und Mensch tatsächlich steht.[8] Es sind diese Widersprüche, die die Kommunikation zwischen Organisationen und deren Klientel überhaupt unter Formungsbedingungen stellen. Die Funktion des Datenschutzes besteht insofern auch darin darauf hinzuwirken, dass diese Widersprüche nicht einseitig aufgelöst sondern als solche reproduziert werden. Das ist einer der Gründe, warum Datenschutz politisch nicht einseitig vereinnahmbar ist.

Traditionell beargwöhnt der Datenschutz moderne Informations- und Kommunikationstechniken. Diese Techniken können von Organisationen zu leicht dafür eingesetzt werden, um Informationen auch über die funktionalen Trennungsgrenzen hinweg zur Informationsgewinnung für ihre speziellen Interessen zweckzuentfremden, was sich als eine konkrete Gefahr für den einzelnen Menschen auswirken kann. Etwa in der Mitte der 90er Jahre machte der staatlich institutionalisierte Datenschutz allerdings einen paradigmatischen Schwenk durch. Die ersten Erfahrungen mit dem Internet zeigten einerseits, dass sich bestimmte Bereiche der sozialen Realität dem Zugriff durch das Recht zu entziehen drohten, und andererseits, dass sich verbesserte Chancen abzeichneten, grundrechtliche Zusicherungen tatsächlich durchzusetzen. Progressive Datenschützer ließen sich deshalb zunehmend auf ein Spiel mit dem Teufel oder zumindest mit dem Feuer ein: Sie suchten nach technischen Lösungen, um Datenschutz in Technik zu gießen und ihn, in technischer Infrastruktur geronnen, durchzusetzen („Privacy Enhancing Technologies“, PET). Die Aufgabe der datenschutzgerechten Gestaltung von Technik besteht darin, dass die Datenverarbeitung, ihrerseits technisch gestützt!, geplant, kontrolliert, transparent und sicher geschieht und sich dadurch auf der inhaltlichen Ebene Kommunikationen unter Bedingungen stellen lassen. Daher stellt sich die Frage, ob oder wie die in den letzten zehn Jahren entwickelten PETs helfen können, die oben genannten Probleme zu lösen. Wir kommen gleich auf diese Frage zurück.

Konzentratoren für die Verwaltung, unique users für die Wirtschaft

Die durch die Verwaltungsmodernisierung derzeit anstehende Bündelung von Kommunikationsströmen und Datenbeständen für natürliche und juristische Personen durch Bürgerportale und Einheitliche Ansprechpartner sowie durch die Nachrichtenbroker der E-Government-Gateways in den Rechenzentren der Verwaltungen sind aus Datenschutzsicht hochproblematisch, weil diese die oben angesprochenen konstitutiven Funktionstrennungen des modernen Rechtsstaates operativ, in der Zuspitzung auf Personen, unterlaufen. Sie machen das wahr, was die von den Datenschützern seit je her bekämpfte Personenkennziffer, die zu bekämpfen in rein technischer Hinsicht allerdings sinnlos[9] ist und die spätestens mit der SteuerID als real eingeführt gelten darf, als Katastrophe nur in Aussicht stellte: Die Portale und zentralen Nachrichtenbroker machen die Daten der verschiedenen Kommunikationsbeziehungen des einzelnen Bürgers, Kunden, Patienten und Menschen ganz real, an nur wenigen Zugriffspunkten konzentriert, technisch

leicht zugänglich.[10] Sie agieren als zentrale Verkettungsinstanzen direkt an den einzelnen Personen.[11] Bürgerportale müssen beispielsweise die E-Mails der Bürger auf ihren Servern bereits ver- und entschlüsseln oder signieren, um das Komfortversprechen einzulösen, dass sich niemand mit den als kompliziert geltenden, aber unerlässlichen Sicherheitssverfahren beschäftigen muss. Damit sind diese Daten dem Zugriff und etwaigen Manipulationen oder Fehlfunktionen der Portalbetreiber sowie externen Angriffen ausgesetzt.

Neben diesen aktuellen Projekten und Entwicklungen aus dem Bereich des E-Governments muss man noch einen weiteren Akteur aus der Wirtschaft betrachen, der insbesondere die Aktivitäten der Internetnutzer im Netz beobachtet: Google Analytics. Mit Hilfe von Google Analytics lassen sich in vielen Fällen bereits Server und Organisationen übergreifend sogenannte „unique users" generieren. Unique users sind Profile von Netznutzern, von denen der Beobachter, sprich ein Betreiber der Google-Analytics-Technologie, vieles genau weiß, mit Ausnahme vielleicht nur noch des Namens und der Straße, in der dieser User wohnt. Der Betreiber von Google Analytics kennt den charakteristischen Klickstream des unique users und weiß, welche Links und Server, also: Themen, dieser derart beobachtete User typischerweise anklickt. Zusätzlich kann er einen User über den typischen Zeitpunkt der Netznutzung und den verwendeten IP-Adresspool der Internet-Provider recht eng geolokalisieren. Und falls ein Zugriff auf die weltweit einzigartigen MAC-Adressen oder Timing-Eigenschaften eines PCs besteht, so kann der PC des Users sogar eineindeutig identifiziert werden.[12] Je mehr Daten von einem Web-Nutzer derartig organisiert gesammelt werden können, desto konturierter wird das Profil eines unique users. Und wenn ein unique user sich an irgendeiner Stelle authentisiert – beispielsweise bei Google Mail oder anlässlich einer Bestellung bei einem Betreiber, der von Google Analytics zugänglich ist –, so verfügt Google anschließend sogar über die Zuordnung des unique-user-Profils zu einer konkreten Person. Über diese Person weiß Google, bei denen die mit Google Analytics gewonnenen Daten zentral gespeichert und ausgewertet werden, dann möglicherweise sehr viel, weil schon über Jahre Informationen in einem unique-user-Profil zusammengetragen wurden. Und die Verwendung des Google-Browser Chrome wird die Beobachtung der Nutzer sicher noch um vieles vereinfachen. Also, selbst wenn ein Nutzer nach dem datenschutzrechtlich ersten Sündenfall einer Authentisierung weiterhin das Web nur passiv lesend benutzt, kann er über die Charakteristik seines Schlenderns im Web, je länger es anhält, als immer wahrscheinlicher werdendes Profil genau dieses Nutzers identifiziert werden. Er ist somit nicht (nur) auf der Ebene von IP-Adressen sondern anhand seiner inhaltlichen Nutzung des Internet mit hoher Wahrscheinlichkeit identifizierbar.

Was kann getan werden?

Es ist auf zwei wichtige Entwicklungen im Rahmen der PET hinzuweisen. Zum einen auf Anonymisierungstechniken, zum anderen auf „nutzerkontrolliertes Identitätsmanagement".

Das Ziel der Anonymisierung besteht darin, dass weder ein Betreiber eines Webservers noch ein Internet-Zugangsprovider erkennen kann, wohin ein Nutzer surft oder für welche Themen sich der Nutzer interessiert. Bei den ambitionierten Anonymisierungstechniken ist zudem das Problem gelöst, auch vor den Betreibern des Anonymisierungsservice geschützt zu sein. Die konzeptionelle Kernidee der Anonymisierung im Internet besteht darin, internetgestützte Kommunikationsbeziehungen in einer möglichst großen Anonymitätsgruppe, die von den Nutzern eines Anonymitätsdienstes gebildet wird, verschwinden zu lassen. Dadurch kann auch ein technisch sehr gut ausgestatteter Beobachter im Internet keine Ereignisse auf Seiten eines Nutzers und Ereignisse auf Seiten der technischen Systeme, wie etwa Webserver, in eine kausal zweifelsfreie Beziehung setzen.[13] Grundsätzlich sollte aus Sicht des Datenschutzes jede Nutzung des Internet von Vornherein anonym erfolgen.[14] Erst bei bestimmten Kommunikationen, die eine Authentifizierung nötig machen, etwa in der Kommunikation von Bürgern und Kunden mit Behörden und Unternehmen, muss dann eine Authentifizierung der Kommunikationspartner erfolgen. Aber selbst eine Identifikation einer Eigenschaft einer Person, ob sie volljährig ist oder über einen Führerschein verfügt oder krankenversichert ist, muss nicht zwangsläufig zur Preisgabe des Namens und weiterer Daten einer bestimmten Person führen. Sehr viele Kommunikationen lassen sich auch unter Pseudonym bzw. mit „anonymen Credentials“ abwickeln.[15]

Nutzerkontrolliertes Identitätsmanagement[16] soll Nutzern helfen, im Hintergrund verschiedene Pseudonyme für verschiedene Kommunikationsituationen und Transaktionen zu verwenden.[17] Der Zweck des Pseudonymmanagements besteht zum einen darin, dass Organisationen Daten nicht auf Personen zurechnen können, wenn eine Person sich nur informieren möchte und die Zuordnung zur Person deshalb funktional nicht notwendig ist. Wichtiger aber ist die Eigenschaft von Pseudonymen zu verhindern, dass Organisationen unterschiedliche Ereignisse miteinander über den gleichen Namen oder das gleiche Pseudonym verketten können. Dafür ist es notwendig, dass für jede Kommunikation oder Transaktion ein anderes Pseudonym genutzt werden kann. Pseudonyme für das alltägliche Handling mit Organisationen muss man grundsätzlich, zu vernachlässigbaren Kosten und unter ausschließlicher Verfügungsgewalt des Nutzers, nach Belieben generieren und wegwerfen können.[18] Das anlassbezogene Aufheben der Anonymität einer Person oder die Herausgabe der Zuordnungsregel eines Pseudonyms zu einer konkreten Person darf nur unter rechtstaatlichen Bedingungen, bspw. durch Freigabe eines Richters, erfolgen. Ganz anders sieht es der aktuelle Gesetzentwurf zum Betrieb von Bürgerportalen vor: Hier soll ein Portalbetreiber selber darüber entscheiden, ob es auf Anfrage gerechtfertigt ist, ein Pseudonym aufzudecken. Dabei ist schon die Tatsache inakzeptabel, dass für den Portalbetreiber die Pseudonyme ihre Nutzer aufdeckbar sein sollen. Und das ist nur ein Indikator für die sicherheitstechnisch und datenschutzrechtlich inakzeptablen Bestimmungen dieses Entwurfs.[19]

Allerdings: Die Anonymisierung im Internet, die derzeit weitgehend darauf beruht, dass Nutzer unter einer einzigen, massenhaft genutzten IP-Adresse erscheinen, müsste um weitere Vorkehrungen ergänzt werden, die die Profilbildung von unique user auf der Anwendungsebene der Internetnutzung zumindest erschwert. So könnte der Browser im Hintergrund bspw. zufällige Seiten aufrufen, dann zufällige Links verfolgen, um so die

Klickcharakteristiken der Nutzer zu nivellieren. Der Aufwand ist allerdings absehbar beträchtlich.

Generell gilt zudem: Wer über das Internet nach dem aktuellen Stand der Technik sicher kommunizieren möchte, muss grundsätzlich Sicherheit herstellende Programme auf dem eigenen PC, im eigenen Verfügungsbereich, installieren.[20] Dies ist zum Beispiel zunehmend häufiger bei Rechtsanwälten und Notaren der Fall, die das elektronische Gerichts- und Verwaltungs-Postfach (EGVP) von Gerichten benutzen wollen oder zunehmend häufiger auch müssen.[21] Diese nutzen zum Transport von Daten die Sicherheits-Technik OSCI-Transport, die nach Stand der Technik als sicheres und revisionsfähiges Protokoll gilt und von Behörden zum Datentransfer untereinander eingesetzt wird. In dieser Form können, mit Hilfe eines angeschlossenen Kartenlesers und einer Chipkarte, auf einem sicheren technischen Niveau elektronische Unterschriften geleistet und Dateien auf eine Weise sicher verschlüsselt werden, die wirklich erst der vom Sender adressierte Empfänger wieder entschlüsseln kann.

Anstelle eines obskuren Bürgerportals sollte ein Projekt aufgesetzt werden, dass Bürger in die Lage versetzt, derartige Programme, die konzeptionell auf Sicherheit getrimmt sind, auf dem eigenen Privat-PC zu installieren, um sicher und rechtskräftig kommunizieren zu können. Es bedarf der Entwicklung einer wirklich funktionierenden Technik, die auch dann angeboten wird, wenn die Nachfrage stockt, allein damit überhaupt die Chance auf einen Migrationspfad entsteht, so dass zukünftig die bessere Technik, die sicherheitstechnisch tatsächlich hält was sie verspricht, vermehrt eingesetzt werden kann. Auch das zählt zur Infrastrukturverantwortung eines Staates. Andernfalls breitet sich schlechte Technik aus Mangel an Alternativen mit der normativen Kraft des Faktischen aus.

Und auch der EAP ließe sich intelligenter datenschutzkonform einsetzen. Hier besteht die Kernidee darin, dass der EAP den Beantragungsprozess über sämtliche Verwaltungen hinweg als Gesamtworkflow modellierte, diesen Workflow dann in seiner technischen Beschreibung, etwa in OWL oder BPEL[22] formulierte und auf den PC des Antragstellers übertrüge. Fortan kann die Kommunikation zwischen dem Antragsteller und den Verwaltungen direkt, auf der Basis von OSCI-Transport oder einem europäischen Pendant, geschehen. Der EAP verfügt zwar über eine ganze Reihe an personenbezogenen Daten und würde auch den Workflow überwachen, so wie es die EU-Dienstleistungsrichtlinie fordert[23], muss deshalb aber keinen Einblick in die Inhalte der Kommunikation zwischen Antragstellern und Behörden nehmen.[24] Controlling und Operating wären tatsächlich, gemäß reiner Lehre, weitestgehend auseinander gezogen.

Und zuletzt: Die technischen Systeme der Organisationen, insbesondere der Verwaltungen, müssen so entworfen, konfiguriert und betrieben werden, dass jederzeit Transparenz darüber hergestellt werden kann, für welchen Zweck ein System betrieben wird, welche Funktionen und welche Sicherheitslevel dem Nutzer zugesichert werden, was das System aktuell mit den Daten getan hat oder was das System in der Vergangenheit mit Daten tat. Dafür müssen die Systeme schon von vornherein konzeptionell so ausgelegt werden, dass sie derart automatisiert prüffähig sind.[25] Solche Prüfungen müssen im Prinzip von den Nutzern selbst und zumindest durch Experten anhand interner und externer Audits vorgenommen werden können. Aber vor allem müssen unabhängige und

sanktionsfähige externe Aufsichtsinstanzen diese Prüfungen, ihrerseits durch Maschinen unterstützt, vornehmen. Andernfalls wird es unter den industrialisierten Verhältnissen der europaweit zusammenarbeitenden Verwaltungen schlicht unmöglich, Betroffenen zu ihrem Recht auf informationelle Selbstbestimmung zu verhelfen.

Ein progressiver Datenschutz zielte nicht nur auf das Bewahren der vorhandenen, sondern auf die Ausweitung der Funktionstrennungen noch bis in die Organisationen selbst hinein, wie es beispielsweise das „Sozialgeheimnis“ für staatliche Leistungserbringer fordert (vgl. SGB I, §35), das allerdings derzeit in keinster Weise tatsächlich berücksichtigt wird. Dazu müsste der Datenschutz allerdings über eine Theorie verfügen, die ihn besser als bislang verstehen ließe, welche gesellschaftliche oder vielleicht genauer formuliert: welche kommunikationsökologische Funktion er mit der Beobachtung des auf den einzelnen Menschen zielenden Rechts auf informationelle Selbstbestimmung erfüllt.[26]

1 Es gibt allerdings schon einige entgegenstehende Ansätze, wenn bspw. Krankenversicherungen mit der Bepreisung ihrer Leistungen anfangen zu bestimmen, wie aus ihrer Sicht eine gesunde Lebensgestaltung auszusehen hat oder genetische Dispositionen die Lebensgestaltung des Einzelnen einschränken (vgl. Stockter, Ulrich, 2008: Das Verbot genetischer Diskriminierung und das Recht auf Achtung der Individualität, Duncker & Humblot).

2 Bislang ist deutschlandweit das Meldewesen das einzige weitgehend durchdigitalisierte Verwaltungsverfahren. An diesem Pionierprojekt wollte man in Deutschland die Standardisierung und Automation von Verwaltung lernen. So sind seit 1.1.2007 knapp 5200 deutschen Meldebehörden gesetzlich verpflichtet, Meldedatensätze ausschließlich elektronisch zu bearbeiten und zu übertragen. Dies verlangte viele Änderungen und Angleichungen im Melderecht der Bundesländer sowie die Entwicklung eines Standards zur technischen Darstellung („OSCI-XMeld“) und zum sicheren und revisionsfesten Transport („OSCI-Transport“) von Daten, damit diese auch über das unsichere Internet verschickt werden können.Vgl. OSCI-Leitstelle, auch zur Geschichte des Entstehens des „Online Services Computer Interface“: http://www1.osci.de/sixcms/detail.php?id=1181.

3 Konzept: Deutschland-Online-Projektbericht „Blaupause“ (Stand: 05.09.2008): http://www. deutschland-online.de/DOL_Internet/broker. Technikempfehlungen: von Lucke, Jörn; Eckert, Klaus-Peter; Breitenstrom, Christian, 2008: IT-Umsetzung der EU-Dienstleistungsrichtlinie, Gestaltungsoptionen, Rahmenarchitektur, technischer Lösungsvorschlag - Fraunhofer-Institut für Offene Kommunikationssysteme, Version 2.0, 5. August 2008.

4 Zur freundlichen Zielstellung des Aufbaus eines Bürgerportals: http://www.bundesregierung.de/Content/DE/Magazine/MagazinSozialesFamilieBildung/064/t6-mit-buergerportalen-fuer-sichere-und-verbindliche-elektronische-kommunikation.html; Gesetzentwurf sowie Debatte des Entwurfs: https://www.ekonsultaton.de/buergerportalgesetz/index.php?page=viewcompiler_paragraph_items&id_view=14&menucontext=3&layoutfield=misc3; Erläuterungen zum Entwurf des Gesetzes zu Bürgerportalen:https://www.ekonsultation.de/buergerportalgesetz/site/pictures/Erlaeuterungen_Buergerportalgesetz.pdf; Vortragsfolien zum technischen Entwurf: http://www.eco.de/dokumente/080716_BP_Technische_Konzeption_v02.pdf.

5 Das Bundesdatenschutzgesetz wurde noch unter dem Eindruck von Großrechnertechnologie in einigen wenigen Landesrechenzentren formuliert. Inzwischen stehen PCs auf jedem Schreibtisch, und die Rechnersysteme weiten sich ubiquitär, bis in die Körper der Menschen hinein, aus. Rechnet man dann noch die absehbare Entwicklung der Service-Oriented-Architectures ein, wonach nicht mehr im Vorhinein klar festlegbar ist, welche Daten mit welchem Prozess auf welcher Maschine verarbeitet werden, dann zeigt sich, dass das BDSG-Gutachten von 2001, und selbst die aktuellen

Novellierungsansätze zur Jahresmitte 2008 (vgl. https://www.datenschutzzentrum.de/vortraege/20080701-weichert-neuerungen-bdsg.html), in Teilen schon wieder als unzureichend gelten müssen.

6 Und damit Informationen generieren: Information definiert als „a difference that makes a difference." (Gregory Bateson).

7 Vgl. Luhmann, Niklas, 1997: Die Gesellschaft der Gesellschaft, Frankfurt am Main: Suhrkamp.

8 Appelle wie den des „Bürgers in Uniform" kennzeichnen, wie andere Appelle bspw. an den „Kunden als König", den „Bürger als Souverän" oder den „Mensch als Individuum" das latente Problem, kaum die Lösung.

9 GeburtsortGeburtszeitNachnameVorname ist, derart zusammengeschrieben, operativ eine eindeutige Personenkennziffer. Sie wird real, mit Lehrzeichen dazwischen, von Organisationen nicht anders eingesetzt.

10 Die Provider der Bürgerportale sind technisch bereits perfekt vorbereitet, um auf diese Daten zuzugreifen, nämlich über die Leitungen, über die auch die gespeicherten Vorratsdaten zugänglich sind oder sein werden.

11 Der Begriff „Verkettung" schält sich als attraktiver Begriff einer sich langsam abzeichnenden Technik, Recht und Organisation übergreifenden allgemeinen Theorie des Datenschutzes heraus, vgl. Hansen, Marit/ Meissner, Sebastian, 2008: „Verkettung digitaler Identitäten". https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

12 Was im Rahmen eines Digital Rights Managements oder bei Trustet Platform Moduls wiederum gewünschte Eigenschaften sein könnten. Zur Zweischneidigkeit vgl. Hansen, Markus: „Über die Auswirkungen von Trusted Computing auf die Privatsphäre." https://www.datenschutzzentrum.de/allgemein/trusted_computing.htm.

13 Siehe die Auflistung konzeptionell vertrauenswürdiger Anon-Platformen: http://hp.kairaven.de/bigb /asurf.html.

14 Genau so, wie Menschen, die einen Bürgersteig benutzen möchten, sich nicht zuvor erst ausweisen müssen. Die Nutzung von Straßen mit einem Auto ist dagegen eine Anwendung einer Pseudonymisierung, wobei die Aufdeckung des Halternamens streng der Polizei vorbehalten ist.

15 Vgl. das Idemix-Konzept, http://www.zurich.ibm.com/security/idemix/.

16 Hansen, Marit; Berlich, Peter; Camenisch, Jan; Clauß, Sebastian; Pfitzmann, Andreas; Waidner, Michael, 2004: Privacy-Enhancing Identity Management; Information Security Technical Report (ISTR) Vol. 9, No. 1 (2004); Elsevier Ltd, Cambridge (UK); 35-44; http://dx.doi.org/10.1016/S1363-4127(04)00014-7.

17 Vgl. das EU-Projekt PRIME zu nutzerkontrolliertem Identitätsmanagement: https://www.prime-project.eu/.

18 Pfitzmann, Andreas; Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology; http://dud.inf.tu-dresden.de/ Anon_Terminology.shtml.

19 Und wenn das Bürgerportal etabliert ist, muss man damit rechnen, dass ein faktischer Anschlusszwang für Bürger und Kunden entstehen wird, allein weil Verwaltungen und Unternehmen diesen konstengünstigeren Weg als Standard nutzen und dafür den sichereren Papierweg teurer machen werden.

20 „Cloud Computing" ist der absehbar nächste, strukturell folgenschwere Angriff auf die Privatssphäre, wenn nicht nur Dateien anstatt auf der eigenen Festplatte auf irgendwelchen Servern gespeichert sind, sondern Programme genutzt werden, die anstatt auf einem Privat-PC irgendwo draußen im Netz installiert sind. Der Nutzer hat dann noch weniger Kontrolle als derzeit darüber, was mit seinen Daten und den Verarbeitungsprozessen dieser Daten geschieht.

21 Vgl. http://www.egvp.de/.

22 OWL (Web Ontology Language) und BPEL (Business Process Execution Language) bieten formale Semantiken, mit denen sich organisatorische Ereignisse steuern lassen.

23 Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt: http://eur-lex.europa.eu/LexUriServ/site/de/oj/2006/l_376/l_37620061227de00360068.pdf.

24 Rost, Martin, 2008: Das etwas andere Modell vom Einheitlichen Ansprechpartner (EAP), in: Verwaltung und Management, 2008/ 04: 179f.

25 Hier werden die Policies, mit denen WebServices gesteuert werden, eine entscheidende Rolle spielen. Diese Policies setzen rechtliche Anforderungen in technische Anweisungen um, bei denen dann gute Chancen bestehen, dass sich deren Korrektheit, bzw. die korrekte Beachtung bei der Nutzung, mit maschineller Unterstützung feststellen lassen.

26 Ich danke M. Häuser, M. Kamp, Dr. K. Storf und W. Zimmermann für die kritische Diskussion der hier vorgestellten Thesen.