Faire, beherrschbare und sichere Infrastrukturen

Zum Verhältnis der Schutzziele des Datenschutzes und der Informationssicherheit

Martin Rost – Version 0.1

24. September 2011

Inhaltsverzeichnis

1 Integrität von Technik und Personenmodellen

Wenn Menschen zusammen sind und einander zuhören, dann zweifeln sie normalerweise nicht daran, dass das, was der eine gesagt hat, mit dem, was der andere daraufhin hört, identisch ist. In einem alltäglichen Gespräch wird die Identität von Gesprochenem und Gehörtem unterstellt. Informatiker bezeichnen diese Identität als *Integrität einer Kommunikation*. Für Techniker ist die Herstellung einer gesicherten Integrität allerdings eine große konstruktive Herausforderung. So kann beispielsweise ein Telefongespräch zusammenbrechen, weil ein Kabel in Jahrzehnten porös geworden ist oder weil die Telefongesellschaft aufgrund unbezahlter Rechnung keinen Strom mehr geliefert bekommt. Das Telefongespräch kann unbeabsichtigt verstümmelt oder, mit allerdings großem technischen Aufwand, in Echtzeit beabsichtigt von Dritten verfälscht sein. Letzteres ist wiederum bei E-Mails trivial möglich. Auch besteht das Risiko, dass Gesprächspartner nicht sicher sein können, tatsächlich mit demjenigen zu telefonieren, mit dem sie zu sprechen glauben. Abstrakt ausgedrückt: Die Sicherstellung der Integrität sowohl der Form einer Nachricht als auch der Infrastruktur zur Übertragung einer Nachricht als auch die Sicherstellung der Integrität der Beteiligten (Authentisierung) ist deshalb eines der elementaren Schutzziele, das für den Betrieb einer jeden Kommunikationsinfrastruktur angestrebt werden muss. Es ist insbesondere die Aufgabe von Experten des Datenschutzes und der Informationssicherheit, sich um die Beachtung und (den Nachweis der) Umsetzung der Integritätsanforderungen

in komplexen Systemen, die viele Organisationen und Informationstechniken umfassen können, zu kümmern.

Es gibt weitere Schutzziele die anzustreben sind, damit Kommunikation gelingen kann. Zu den sechs *elementaren Schutzzielen* zählen neben Integrität Verfügbarkeit und Vertraulichkeit sowie Transparenz, Nichtverkettbarkeit und Intervenierbarkeit.[1]Diese elementaren Schutzziele beanspruchen eine Geltung als Operationalisierung von vernünftigerweise zu stellenden Anforderungen an technisch-organisatorische Infrastrukturen. Diese Schutzziele beanspruchen insofern eine gesellschaftliche Verallgemeinerungsfähigkeit, die für alle Menschen im gleichen Maße gilt und auch von Organisationen vernünftigerweise nicht negiert werden kann. *Ich möchte die Schutzziele hier als technisch-organisatorisches Analogon zu Bürger- oder Menschenrechten ausweisen.* Was soll das bedeuten?

Zum einen bedeutet das, dass sich nicht nur IT-Experten mit der Umsetzung der Ziele konstruktiv beschäftigen, sondern dass diese Ziele auch für Laien verständlich sein müssen. Es bedarf der Kopplung dieser Ziele an das Verständnis des „normalen“ Bürgers, weil der Bürger politisch darüber befinden können muss, welchen Anforderungen eine technisch Infrastruktur genügen muss, die seinem Interesse als einem Bürger eines Staates unmittelbar entgegenkommt. Und ein Kunde sollte verstehen können, wenn Schutzvorkehrungen den Komfort bei der Nutzung von Geräten schmälern oder erhöhte Kosten durch Umsetzung dieser Ziele in Kauf zu nehmen sind. Zum zweiten sollen die Schutzziele auch für Fachleute instruktiv sein, damit diese kommunikationstechnische Komponenten und Infrastrukturen planen, kalkulieren, umsetzen, betreiben, reparieren, weiterentwickeln und nicht zuletzt effektiv überprüfbar machen können. Methodisch muss es Fachleute dann in-

[1]Während des Schreibens an einem ersten Entwurf dieses Textes starb im September 2010 viel zu jung Prof. Andreas Pfitzmann. Andreas Pfitzmann hatte den konzeptionellen Ansatz der „Neuen Schutzziele“, die untereinander in einem Spannungsverhältnis stehen, 2008 in einem arbeitsgruppeninternen Diskussionspapier erstmals angedeutet. Die sich daran anschließenden Ausarbeitungen speziell für den Datenschutz begleitete er kritisch gewogen, auf seine bedachte, inhaltlich weitsichtige und kluge sowie zwischenmenschlich angenehme Art. Neben Andreas, der die Initialzündung gab, habe ich einer ganzen Reihe an Kolleginnen und Kollegen für Gespräche, Lösungswege oder auch argumentative Abrundungen zu danken. Für den Gedankengang speziell dieses Aufsatzes wichtig waren insbesondere intensive Diskussionen mit Marit Hansen, die zur damaligen Arbeitsgruppe um Prof. Pfitzmann gehörte. Daneben gilt mein Dank insbesondere Kirsten Bock, Dr. Michael Schack, Sven Thomsen und Wolfgang Zimmermann, mit denen immer wieder das big picture des Datenschutzes in den Blick gerät sowie den Kollegen des Magdeburger Treffens von 2009: Herrn Eiermann, Herrn Ernestus, Herrn Heibey, Herrn Raugust und Herrn Wehrmann aus dem Arbeitskreis Technik der Datenschutzbeauftragten der Länder und des Bundes, mit denen eine erste Version eines Normentextes zu den Schutzzielen formuliert wurde.

teressieren, mit welchen Maßnahmen diese vernünftigerweise geltenden Ziele umsetzbar sind.

Diese elementaren Schutzziele formulieren nicht nur Anforderungen für kommunikationstechnische Infrastrukturen. Vielmehr kann man die Schutzziele auch für Daten und Prozesse, mit denen Organisationen Personen erfassen, anwenden. Damit ist das klassische Kernthema des Datenschutzes angesprochen. Die weitgehend standardisierten Kommunikationen zwischen Organisationen und Personen - also bspw. zwischen einer staatlichen Verwaltung und einem Bürger oder zwischen einem Unternehmen und einem Kunden - erfüllen jeweils eng zugeschnittene Funktionen: Es soll ein Antrag beschieden, eine Ware eingekauft oder eine Hilfe- bzw. Dienstleistung für eine Person erbracht werden. Wie den beteiligten Personen während der Kommunikation mit einer Organisation zumute ist und was sie über die Abwicklung von Anträgen oder dem Kauf einer Ware hinaus beschäftigt, ist dabei nicht relevant. Beteiligten müssen in ihrer Kommunikation gegenüber Organisationen all das Nebensächliche, und in der Regel auch die Motivation für ihr Tun, kommunizieren zu wollen unterdrücken. Das gleiche gilt für Organisationen. Die Unterdrückung der Kommunikation aller Besonderheiten einer Situation bei Übernahme einer allgemeinen stereotypen Rolle in der Kommunikation, wie die des Bürgers oder des Kunden oder des Patienten, gilt prinzipiell als weltweit verstanden und in der Regel erwünscht. Es handelt sich insofern zunächst um eine Realabstraktion (vgl. Sohn-Rethel 1978) bzw. um eine De-Kontextualisierung der Kommunikation von den konkreten Umständen der Situation und beliebigen Motiven. Diese Dekontextualisierung wird jedoch umgehend kompensiert durch eine Kontextualisierung, gemäß einer generischen Rolle in Abgrenzung zu anderen Rollen (Beispiel: Auftreten als Kunde, aber nicht als Patient, Mitglied, Mitarbeiter). Gesprächspartner reichern die zunächst dekontextualisierte, standardisierte Kommunikationen mit eigenem Wissen, mit Erfahrungen und Vermutungen oder mit Informationen aus dritter Quelle über den Kommunikationspartner wieder an. Auf diese Weise entstehen Konstruktionen von Personenmodellen. Das machen Menschen genau so wie Organisationen. Hierbei spräche man in einem Gespräch unter Personen von Vorurteilen, im Verhältnis von Unternehmen und Personen von einem Kundenbindungssystem bzw. vom „Customer-Relationship-Management“ (CRM). Und auch der Staat hat sozusagen eingebaute Personenkonstruktionen, was dieser als Pflichtkommunikation von einem Bürger mit der Verwaltung erwartet, bzw. gesetzlich geregelt: erwarten und zumuten darf.

Dynamische Personenmodelle werden von Unternehmen zunehmend automatisiert erstellt, insbesondere dann wenn die gesamte Kommunikation zwischen Personen und Organisationen über Internet erfolgt. Diese Modelle

werden typischerweise mit wissenschaftlichem Anspruch analysiert und genutzt und weiterentwickelt. Banken treffen Entscheidungen bspw. anhand von Scoring-Modellen, wonach Menschen mit unterschiedlichen Eigenschaften in unterschiedliche Kredit-Risikotypen unterteilt werden. Diese Personenmodelle sind zwangsläufig unzulänglich. Aber sie können trotzdem für den verfolgten Zweck hinreichend sein, denn Unternehmen müssen nur über Personenmodelle verfügen, die vergleichbar zu denen der Konkurrenz sind. Diese Modelle bilden dann die Grundlagen ihres Organisationshandelns gegenüber Personen. Auf die Spitze getrieben haben das die Daten für Personenmodelle, die als Profile insbesondere von Amazon, Google und Facebook angefertigt werden. facebook versucht, nun auch der gesamten Geschichte eines Menschen durch Nötigung zur Selbstauskunft habhaft zu werden.[2]

Aus Datenschutzsicht ist es keine Option zu fordern, dass die Personenmodelle der Organisationen perfekt ausgestaltet sein müssen oder im Gegenteil falsch sein sollten. Beides ist nicht nur aus Datenschutzsicht nicht wünschenswert. Wären diese Modelle in Umfang und Qualität perfekt, dann wäre eine besonders wirkungsvolle Machtausübung von Organisationen gegenüber ihrer Klientel möglich und beschränkte die Autonomieversprechen, die in den Menschenbildern vom Bürger, Kunden, Individuum enthalten sind und die, in Form informationeller Selbstbestimmung, zu schützen die wesentliche Aufgabe des Datenschutzes ist. Falsche Entscheidungen von Organisationen aufgrund falscher Personenmodelle sind für betroffene Bürger, Kunden und Patienten inakzeptabel, weil dann keine erwartungssichere Partizipation am gesellschaftlichen Leben möglich wäre. Organisationen handelten dann aus Unzulänglichkeit willkürlich. Man hat es also mit einem Optimierungsproblem zu tun, dessen Interpretationen und Bearbeitungen durch Organisationen der Datenschutz beobachtet und bewertet.[3] Aus Datenschutzperspektive gilt es deshalb, diese grundsätzlich immer gegebene Risikobehaftetheit eines jeden Personen- bzw. Entscheidungsmodells von Organisationen gegenüber Personen mit Hilfe der Schutzziele (auch den Organisationen selber)

[2] „Facebook zeigt standardmäßig jedem Nutzer eine andere, von Algorithmen berechnete Auswahl der Ereignisse in ihrem sozialen Umfeld an. Meldungen von jenen Menschen und Quellen nämlich, mit denen die Nutzer „am häufigsten interagieren“ - so die vage Facebook-Formulierung. (...) Es ist erstaunlich, wie wenigen Internetnutzern bewusst ist, dass Software auf Basis ihres Surfverhaltens, ihres Orts, ihrer Kontakte die Onlinewirklichkeit für sie vorsortiert.“ (vgl. Lischka 2011). Zur Analyse des facebook-Totalitarismuses: Rost 2011a.

[3] Das ist logisch unbefriedigend, aber soziologisch folgerichtig Die Konstruktion von Kommunikation thematisiert die Soziologie unter dem Thema der „Doppelten Kontingenz“: Jede Kommunikation schließt an Erwartungen über Erwartungen an, die als selbsttragende Konstruktionen durchaus perfekt scheitern können und sich aufgrund genau dieses sicheren Scheiterrisikos erst als System stabilisieren (vgl. Luhmann 1999).

transparent zu machen. Die benutzten Daten und deren Auswertungsprogramme müssen dafür auf das unbedingt Erforderliche und Zweckgemäße beschränkt sein. Und es ist dafür zu sorgen, dass Korrekturen an Daten und Profilen dort überhaupt nur vornehmbar sind, wo die Korrekturen für beide Seiten unerlässlich funktional sind. Organisationen sollen nicht aufgrund der immer riskanten Informationslagen in ihren Aktivitäten gegenüber ihrer Klientel, deren Autonomie sie zu respektieren haben, überziehen.

Der Schutz der Rechte und der Privatsphäre des Individuums, das zugleich eingebunden ist in Kommunikationen mit Organisationen und deren automatisierten Datenverarbeitung, ist das Thema des Datenschutzes. Damit sind die eingangs erwähnte Vertrauenswürdigkeit der von Organisationen eingesetzten Informationstechniken sowie zweitens die von den Organisationen notwendig genutzten Personenmodelle bzw. „Menschenbilder“[4], die sie für ihre Entscheidungen gegenüber ihrer Klientel heranziehen, angesprochen. Der kritische Blick des Datenschutzes konzentriert sich entsprechend auf diese beiden Themen sowie auf die Techniken und Prozesse, mit denen Organisationen ihre Daten in Bezug auf Personen verarbeiten.

Die rechtlichen Regelungen als Grundlage des institutionalisierten Datenschutzes werden nach überkommener Rechtslage flankiert von darauf abgestimmten, technisch-organisatorischen Maßnahmen und Methoden, wie sie aktuell der Anlage zu § 9 BDSG zu entnehmen sind.[5] Sowohl die materiellen Rechtsgrundlagen des BDSG als auch dessen Orientierung an technisch-organisatorischen Maßnahmen gelten allerdings lange schon als nicht mehr hinreichend.[6] Anstatt Maßnahmen vorzugeben wäre es sinnvoller, den Maßnahmen systematisch zugängliche und juristisch abwägbare Ziele voranzustellen, deren Grad des Erreichten sogar messbar wäre. Von einer systematisch gewonnenen Zielorientierung darf man sich dann versprechen, dass alle für die Systemsicherheit und den Datenschutz wesentlichen Systemeigenschaften berücksichtigt werden.

[4] „Gemeinschaftsbezogen“ heißt es soziologisch unzureichend differenziert in der typischen Rechtsprechung des Bundesverfassungsgerichts (vgl. Becker, Ulrich, 1996: Das ‚Menschenbild des Grundgesetzes' in der Rechtsprechung des Bundesverfassungsgerichts, Berlin, Duncker und Humblot, darin insbesondere die Kritik ab S. 123ff.).

[5] Schutzziele sind bislang nicht im Bundesdatenschutzgesetz (BDSG) verankert. Man findet sie jedoch in den Datenschutzgesetzen einiger Länder. In einer Entschließung der Landesdatenschutzbeauftragten vom März 2010 zur anstehenden Novellierung des BDSG wird die Aufnahme von Schutzzielen gefordert.

[6] Vgl. Garstka / Pfitzmann / Roßnagel 2001.

2 Zur Funktion des Datenschutzes

Datenschutz hat die Funktion, darauf zu achten und hinzuwirken, dass die Kommunikationen von Organisationen und Personen unter angemessenen Bedingungen stehen. Nur dann können belastbare Vertrauensbeziehungen bestehen, die Kommunikationen und Datenverarbeitungen effektiv machen. Zu berücksichtigen ist, dass Organisationen der Wirtschaft, Verwaltung und Wissenschaft informationstechnisch in der Regel ungleich mächtiger als ihre Klientel sind. Organisationen müssen deshalb im Wesentlichen gegenüber Aufsichtsbehörden nachweisen, dass sie ihre technischen Infrastrukturen rechtskonform beherrschen und auf der Grundlage von auf Fairness bedachten Menschenbildern agieren und zumindest gesetzeskonform agieren.

Datenschutz wirkt aber nicht nur in diesem Sinne auf Organisationen ein, sondern auch gesellschaftlich. Moderne Gesellschaften sind gekennzeichnet durch Märkte und Unternehmen, rechtsstaatlich gebundene Verwaltungen und unabhängige Gerichte, Demokratie und unabhängige Parteien, wissenschaftliche Diskurse verschiedener Paradigmen, durch eine freie Presse und unabhängige Blogs, Religionsfreiheit und freie Kunstszenen. Diese versorgen die moderne Gesellschaft mit produktiven Variationen an Formen und Differenzen, also: mit Risiken, die im Unterschied zu Gefahren kalkulierbar sind. Datenschutz ist immer dann ein Thema, wenn Organisationen in ihrem IT-gestützten organisierten Zugriff auf Personen deren Autonomie deformierend die Risiken der Unbestimmtheit, der Unruhe, der Variationen und riskanten, aber auch produktiven Dynamiken, die durch Märkte, Rechtsstaatlichkeit und freie Rede entstehen, einseitig formen und die darin liegenden Risiken präventiv zu bearbeiten versuchen.[7] Die gesellschaftliche Funktion des Datenschutzes besteht insofern vor allem darin, Märkte, Rechtsstaatlichkeit sowie freie Diskurse und die grundsätzliche Ergebnisoffenheit des durch sie getriebenen Wandels auch beim Einsatz von IT, die die Welt trivialisierend berechenbar zu machen verspricht, zu verteidigen, indem sie die latent „beunruhigende“ Autonomie des Bürgers, des Kunden, des Individuums Ernst nimmt und verteidigt.

Die durch Datenschutz formulierten Schutzziele entfalten Wirkungen, die Personen vor latent unfair agierenden Organisationen schützen sollen. Datenschutz schützt Organisationen auch vor sich selbst, indem dieser diese daran hindert, in einer funktional-differenzierten Gesellschaft mit den eigenen Modellen einer trivialen Kontextualisierung von Mitarbeitern und Bürgern, Kunden, Klientel zu scheitern. Datenschutz thematisiert die Risiken eines

[7] Wie eine datenschutzferne Tyrannei in der Moderne aussähe illustriert Zeh 2009.

Rückfalls einer Gesellschaft der „funktionalen Differenzierung“[8] in vormoderne, hierarchische Verhältnisse mit an Personen orientierten Abhängigkeiten einiger weniger Organisationen, die die Gesellschaftsstruktur allzuständig-totalitär bestimmten. Das Niveau des Datenschutzes zur Sicherung der funktionalen Differenzierung ist deshalb wahrscheinlich einer der verlässlichsten Indikatoren für die „Modernität“ einer Gesellschaft in Bezug auf Demokratie, Rechtsstaatlichkeit, soziale Marktwirtschaft und freie Diskurse.[9]

3 Schutzziele

Gesellschaftsweit implementierte Infrastrukturtechnik, wie z. B. das Telefon, muss vorsätzlichen Angriffen auf Integrität und Vertraulichkeit, insbesondere durch die Organisation die die Infrastrukturtechnik betreibt, robust widerstehen können. Bedrohlich kann aber auch die schiere Größe einer Infrastruktur werden, wenn auch die Organisation die Technik einer Infrastruktur mehr beherrscht. Das ist insbesondere dann der Fall, wenn sich Systemgrenzen nicht mehr eindeutig ziehen lassen, etwa beim Vernetzen von PCs in lokalen Netzen mit den Netzwerken der Internetprovider und mit dem globalen Netzevernetzungsnetz Internet. Hier hilft Datenschutz, rechtlich verantwortbare Grenzen vorzugeben, an denen entlang Systeme nachgewiesenermaßen beherrschbar betrieben werden. Kommunikationstechniker müssen dafür Techniken entwickeln, um vorsätzlich-aggressive Angriffe auf Daten und Systeme sowie auf unkontrollierbar gewordene Systeme erkennbar zu machen. Dieses Schutzziel hatten wir eingangs bereits als „Sicherung der Integrität“ bezeichnet.

Bevor die Integrität von Gesprächen relevant wird, müssen Personen erst einmal füreinander gesprächsbereit und ersichtlich verfügbar sein. Sie müssen ihren Gesprächsinhalt aufeinander ausrichten können, entsprechend der Art und dem Maß an gewünschten vertraulich-sozialen Situation. Wollen sie unter sich sein, dann suchen sie eine entsprechend vertrauliche Umgebung auf. Schutzziele formulieren diese alltäglichen, in der Regel ebenfalls nicht-reflektierten operativen Anforderungen an Gesprächssituationen. So bezeichnet Verfügbarkeit die Anforderung, dass Informationen und Systeme zeitgerecht zur Verfügung stehen und ordnungsgemäß verwendet werden können. Und Vertraulichkeit bezeichnet die Anforderung, dass nur Befugte auf Informationen und Systeme zugreifen bzw. von Informationen Kenntnis nehmen können sollen, die ihnen zugedacht sind. Verfügbarkeit von technischen Infrastrukturen wird bspw. durch intelligente Reparaturstrategien und Redundanz bei technischen und organisatorischen Komponenten sichergestellt.

[8] Vgl. Luhmann 1999.
[9] Vgl. Rost 2008.

Vertraulichkeit von Kommunikationen über große Netze wird z. B. durch Verschlüsselungsverfahren und differenzierte Rollen und Rechte in Organisationen durchgesetzt.

Eine Voraussetzung zur Auswahl von Maßnehmen zur Umsetzung von Schutzzielen ist die Transparenz der Abläufe, der Daten, der Prozesse. Deshalb ist Transparenz insbesondere von Organisationsprozessen ein anzustrebendes Schutzziel. Transparenz muss herstellbar sein, um die verschiedenen Ebenen einer Technik und einer Organisation für Überprüfungen zugänglich zu machen. Das Schutzziel Transparenz verpflichtet Organisationen dazu, dass die Erhebung, Verarbeitung, Weitergabe, Aufbewahrung und Löschung von Daten in personenbezogenen Verfahren geplant werden und mit zumutbarem Aufwand nachvollziehbar, kontrollierbar und bewertbar sind. Inhaltlich besteht das Ziel darin zu erkennen, ob die Strategien und Regeln einer Organisation bzgl. der Betriebssicherheit und der Kontextualisierungen zweckgemäß und fair sind. Informationsfreiheit ist insofern ein Bestandteil des Datenschutzes, und genau nicht das Gegenteil von Datenschutz. Konkret zählt zu den Transparenz-Maßnahmen das Anfertigen von Konzepten und der Zugriff auf zweckgebunden erzeugte Monitoring-, Log- und Protokoll-Daten, die Dokumentation von Datenflüssen, Prozessen und Systemen, Inventur- und Netzpläne, der Zugriff auf die Konfigurationen der Datenbanken der Data-Warehouses und des Data-Mining oder die Modellbildungen zum Scoring von Risiken, sowie die Vereinbarungen und Regeln einer Organisation oder die Rechtsgrundlagen und Verträge mit Dienstleistern im Rahmen einer Auftragsdatenverarbeitung. Die Grenze des Transparentmachens speziell von Technik bilden oftmals die Bibliotheken von Programmiersprachen oder die Maschinenbefehle, die zu verstehen einer kleinen Expertengruppe vorbehalten bleibt, sowie Betriebsgeheimnisse von Unternehmen, insbesondere auf der Ebene der Konstruktion von Mainboards oder Prozessoren. Die Grenzen des inhaltlichen Transparentmachens der Modellbildungen bestehen bei privaten Unternehmen in den Geschäftsgeheimnissen und bei staatlichen Verwaltungen in der Organisation der inneren Sicherheit.

Die „eigentliche“ Schutzwirkung eines funktionierenden Datenschutzes geht jedoch von der Begrenzung des Zugriffs von Organisationen auf Personen aus. Anders als in früheren Zeiten kann eine Organisation keine Allzuständigkeit für Personen mehr beanspruchen. Gleichwohl wird das immer wieder versucht, wenn man als Beispiele an Komplettversorgungspakete von Versicherungen und Banken oder an Social-Web-Betreiber wie Facebook denkt. Organisationen dürfen im Normalfall, zumindest gegenüber ihrer externen Klientel, nur mit einem schmalen, funktional begrenzten, zweckmäßigem Ausschnitt auf eine Person zugreifen. Eine nur punktuell zugespitzte Ankopplung von Personen an Organisationen entspricht der in-

formationellen Gewaltenteilung bzw. der funktionalen Differenzierung, die mit dem Schutzziel der Nichtverkettbarkeit von Daten und Verfahren umgesetzt wird.[10] Eine technisch-organisatorische Festlegung des Zwecks eines Verfahrens muss alltagspraktisch in Kenntnis der Abgrenzung zu verwandten Verfahren und zu solchen Verfahren erfolgen, die die Daten zu Forschungszwecken oder zur klientelspezifischen Werbung nutzen wollen. Mit Zwecken lassen sich die Kontexte, in denen spezifisch kommuniziert wird, abgrenzen und bestimmen.[11] Das Maßnahmenbündel zur Umsetzung dieses Ziels umfasst organisatorisch vor allem Rollen-, Rechte- und Strukturkonzepte sowie die intelligente Nutzung von Pseudonymen, etwa im Rahmen des Identitätenmanagements und nicht verkettbarer Einmalausweise, sogenannter „anonymer Credentials".[12] Systeme können voneinander technisch gekapselt und Daten von „Schutzmänteln" oder Containern umgeben sein. Funktional ist auch der Einsatz von Programmen zur Durchsetzung von Zugriffsrechten bis in die Rechnerstruktur hinein.[13]

Als sechstes elementares Schutzziel des Datenschutzes ist Intervenierbarkeit anzusprechen. Intervenierbarkeit dient der operativen Umsetzung der Betroffenenrechte und damit der Einzelfallgerechtigkeit angesichts der zunehmenden Praxis massenhaft automatisierter Einzelfallentscheidungen. Dieses Schutzziel vereint solche Maßnahmen, die den Betreiber in die Lage versetzen, ein technisches System zu steuern, sowie dem Betroffenen die wirksame Ausübung der ihm zustehenden Rechte. Dafür müssen Betroffenen integre Wirkungsanker in den Organisationen und deren IT zur Verfügung gestellt werden. Das kann im Extremfall heißen, dass beim Fehlen einer Einwilligung oder einem gesetzlichen Erhebungs-, Verarbeitungs- oder Übermittlungsrecht der Betroffene auf die Datenverarbeitung der Organisation direkt zugreifen kann, um die Daten zu seiner Person zu bearbeiten. Es sind schließlich seine Daten, die von einer Organisation unberechtigt erhoben und angeeignet

[10] Vgl. Hansen / Meissner 2007.

[11] Hier schließt das Konzept von „contextual integrity" an (vgl. Nissenbaum 2004). Die Idee ist, dass der Kontext, in der eine Kommunikation stattfand und der technisch zugänglich ist, zusammen mit der eigentlichen „Nutznachricht" gespeichert und im Sinne einer „Kontextnachricht" zusätzlich übermittelt wird. Dies ist eine Inanspruchnahme solcher Techniken, die bei der absehbar allgegenwärtigen Überwachung durch Computer („ubiquitäres computing") eingesetzt werden, um diese Technik selber zumindest gegen eine beliebige Verwendung und Auswertung von Daten einzusetzen. Kontextuelle Integrität zu sichern könnte die nächste große Strategie im Rahmen von Privacy-Enhancing-Technology sein, als dritter Schritt nach Datenminimierung und Nutzerkontrolle. (vgl. Borcea-Pfitzmann / Pfitzmann / Berg 2011).

[12] Vgl. PRIME / FIDIS sowie die Entwicklungen unter den Stichworten „UProove" (Microsoft) oder „Idemix" (IBM).

[13] Vgl. ReCoBS / RSBAC.

wurden. Eine kontrollierte Steuerung der Prozesse des Erhebens, Nutzens, Weitergebens und Löschens von personenbezogenen Daten durch eine Organisation ist Voraussetzung für die Durchsetzung der gesetzlichen Betroffenenrechte. Sinnvoll ist auch die Einrichtung von Prozessen, mit denen sachlich und zeitlich beschränkte anstatt pauschale Einwilligungen möglich sind.

Diese sechs elementaren Schutzziele (Integrität, Verfügbarkeit, Vertraulichkeit sowie Transparenz, Nichtverkettbarkeit und Intervenierbarkeit) sind heranzuziehen, wenn neue IT-Konzepte, -Infrastrukturen und -Organisationen, -Systeme und -Verfahren geplant, sicher betrieben und auf Wirtschaftlichkeit, Umweltverträglichkeit sowie Rechtskonformität hin gesteuert und – intern wie extern – überprüft werden können.[14] Schutzziele bieten ein wirksames Instrument zur Umsetzung des „Rechts auf informationelle Selbstbestimmung“ im Hinblick auf Beratung, Kontrollierbarkeit und Bewertung von Datenverarbeitungen. Schutzziele spielen deshalb auch in den Kriterienkatalogen für Datenschutz-Gütesiegel und -Audits eine maßgebliche Rolle.

4 Informationssicherheit und Datenschutz

Die Schutzziele der Verfügbarkeit, der Integrität und der Vertraulichkeit dienen seit den 1980er Jahren der „Datensicherheit“[15], die heute als „Informationssicherheit“ bezeichnet wird.[16] Sie beziehen sich vor allem auf die Sicherung des Betriebs der IT von Organisationen. Informationssicherheit steht vor der Aufgabe, dass Organisationen ihre Prozesse sicher betreiben können, sicher aus der Sicht der Organisation. Die Prozesse, mit denen eine Organisation entweder Geld verdient oder Ordnung sichert oder mit denen unwahrscheinliche Kommunikationen ermutigt werden, müssen stabil verfügbar gemacht werden und vor etwaigen unerwünschten Nebenwirkungen gesichert werden. Als Risikofaktoren Nummer eins gelten dabei Menschen, insbesondere inkarniert als Hacker oder Cracker, als Computerkrimineller, als Terrorist, Industriespion oder Innentäter.[17] Im Unterschied zur Datensicherheit nimmt Datenschutz den Betrieb von Organisationen zunächst aus der Perspektive der von diesem Betrieb betroffenen Personen wahr. Dabei kann es

[14] Am Beispiel von Ambient Assistet Living und der aktuell einsetzenden Industrialisierung der Pflege von hilfebedürftigen Menschen habe ich exemplarisch die Nützlichkeit des Schutzzielekonzepts für die Modellbildung einer datenschutzgerechten Architektur vorgeführt (vgl. Rost 2011).

[15] Vgl. Federrath / Pfitzmann 2000.

[16] Vgl. BSI 2008

[17] Vgl. Clipper 2011: 47.

zu Konflikten zwischen den Perspektiven der Datensicherheit und des Datenschutzes kommen. Zugespitzt formuliert betrachtet die Informationsicherheit methodisch den Menschen als Angreifer auf die Organisation und der Datenschutz umgekehrt die Organisation als Angreifer auf die Person. Eine perfekt gesicherte Kommunikationsinfrastruktur ohne Berücksichtigung von Datenschutzanforderungen führt sehr wahrscheinlich dazu, dass sich bspw. sämtliche Aktivitäten von Nutzern perfekt miteinander verketten lassen, weil sich jeder Nutzer ausweisen musste und anschließend jede Tätigkeit von ihm protokolliert wird, um ihn zu entmutigen, als Hacker zu agieren. Eine perfekt abgesicherte Kommunikationsstruktur bietet insofern keinerlei Schutz vor den Wirkungen von Kontextierungen, die zwar perfekt sicher gespeichert sind aber inhaltlich falsch sein können oder auf unrechtmäßig erhobenen Daten basieren. Personen und Organisationen haben ihre je eigenen Interessen der Risikominimierung gegeneinander. Aus diesem Grunde müssen die speziellen Datenschutz-Schutzziele der Transparenz, der Intervenierbarkeit und der Nichtverkettbarkeit zu denen der Informationssicherheit hinzugenommen werden. Sowohl Datenschutz als auch Datensicherheit betrachten, weil sie beide das Organisation-Personen-Verhältnis thematisieren, die gleichen sechs Schutzziele, allerdings mit unterschiedlich zugespitzten Aufgabenstellungen. Datenschutz und Datensicherheit müssen dafür gegenseitig füreinander profiliert werden. Es kann genau nicht darum gehen, dass die eine Disziplin die andere zwangsläufig mit abdecken soll. Methodisch empfiehlt es sich, die Schutzziele der Datensicherheit zu Attributen des Datenschutzes zu machen, und umgekehrt. Konkret heisst das bspw. den Unterschied herauszuarbeiten zwischen einer integren Transparenz und einer transparenten Integrität, oder einer vertraulichen Intervention von einer intervenierbaren Vertraulichkeit usw. usw., alles in Bezug zum Verhältnis von Personen und Organisationen.[18]

Die universelle Bedeutung der Schutzziele ist dabei kaum zu überschätzen. Denn erstens steht hinter jedem Schutzziel ein Katalog mit technischen und organisatorischen Maßnahmen, mit denen ein Schutzziel in unterschiedlichem Ausmaß wirkungsvoll umgesetzt werden kann. Aber genau so bedeutsam wie die Kopplung der Ziele an technisch-organisatorische Schutzmaßnahmen ist zweitens die rechtliche Abwägbarkeit der Schutzziele untereinander. Die Schutzziele sind immer vollständig auf einen konkreten Sachverhalt zu beziehen, weil diese in einem systematischen Spannungsverhältnis zueinander stehen, das rechtlich abzuwägen und zu konditionieren ist. So geht eine recht-

[18]Ich überlasse es gern dem Leser, nun sämtliche Permutationen der Schutzziele der Datensicherheit mit denen des Datenschutzes in diesem Sinne durchzuprobieren. Was ich hier so großzügig zum Spielen freigebe, ist eine eigentlich von den Datenschützern und den IT-Sicherheitsexperten in den nächsten Jahren vorzulegende konzeptionelle Arbeit.

lich gebotene besonders herauszuhebende Bedeutung eines Schutzziels dann zumeist einher mit einer geringer einzuschätzenden Bedeutung eines oder auch mehrerer anderer Schutzziele. Und drittens lassen sich die Schutzziele, über automatisiert vermessbare Schutzmaßnahmen, als Stellgröße zur Regulation von Prozessen, etwa für die Prozesse des nutzerkontrollierten Identitätenmanagements[19] oder des Datenschutzmanagements einer Organisation[20] verwenden.

Gibt es neben den sechs elementaren Schutzzielen weitere Schutzziele? Ja, die gibt es. Aus den bislang aufgeführten sechs elementaren Schutzzielen sind weitere Schutzziele wie Verdecktheit, Findbarkeit, Abstreitbarkeit, Kontingenz, Authentizität, Zurechenbarkeit, Verbindlichkeit, Erreichbarkeit, Ermittelbarkeit, Anonymität und Unbeobachtbarkeit ableitbar.[21] Diese Schutzziele lassen sich in eine systematisch kontrollierbare Beziehung zueinander bringen, wenn man zunächst von den drei Schutzzielen der Datensicherheit ausgeht. So ergänzen sich in bestimmten Konstellationen Verfügbarkeit und Vertraulichkeit, in anderen schließen sie einander aus: Eine Information ist dann nicht mehr vertraulich, sobald sie verfügbar ist, und umgekehrt. Wenn man eine analog strukturierte widersprüchliche Komplementarität für das dritte Schutzziel Integrität sucht, dann gelangt man zum Schutzziel Intervenierbarkeit: In bestimmten Konstellationen sollen sowohl Nichtänderbarkeit wie Änderbarkeit von Daten, Prozessen und Systemen eine Eigenschaft sein. Ein einwandfrei funktionierender integrer Automatismus soll ebenso beständig funktionieren wie auch jederzeit durch Betroffene unterbrochen werden können. Es muss dabei auf Systeme und Daten transparent zugegriffen werden können, um deren Verfügbarkeit und Integrität feststellen zu können. Insofern ist Transparenz eine Voraussetzung für einen kontrollierbaren Betrieb. Sucht man wiederum nach einer Dualität zum Schutzziel Transparenz, dann ist diese mit dem Schutzziel Nichtverkettbarkeit ausdrückbar. Mit dem Schutzziel Nichtverkettbarkeit lassen sich Gewaltenteilungen und Funktionstrennungen operativ durchsetzen. Lässt man darüber hinaus methodisch Selbstbezüge von Schutzzielen zu – bspw. lassen sich Findbarkeit als verfügbare Verfügbarkeit oder Unbeobachtbarkeit als anonyme Anonymität auffassen – und unterscheidet Informationsinhalt (Nutzdaten) und Informationsumfeld (Kontextdaten), dann ergibt sich ein Tableau der Schutzziele (Abb. 1).

Diese Ausführungen sollen zeigen, dass zur Planung und Beurteilung technisch-organisatorischer Infrastrukturen immer diese sechs elementaren

[19] Vgl. Meints / Zwingelberg 2009.

[20] Vgl. Meints 2007.

[21] Vgl. grundlegend: Rost / Pfitzmann 2009; vgl. in Bezug zu den Grundsätzen des „Privacy By Design“ und den „Global Privacy Standards“: Rost / Bock 2011.

Schutzziele einzubeziehen und gegeneinander abzuwägen sind, um angemessene Systemeigenschaften in Bezug auf Sicherheit und Datenshcutz zu finden und über die Auswahl der dafür angemessenen Maßnahmen zu entscheiden. Die Festsetzung bzw. Einigung auf den Zweck einer Informationsverarbeitung und Kommunikation regelt, welche Art und welches Ausmaß an Transparenz, Nichtverkettbarkeit und Intervenierbarkeit auf Seiten einer Organisation und ihrem Klientel für beide Seiten dann beherrschbar und fair und dadurch vertrauenswürdig sind.

5 Vernünftige Infrastrukturen für vernünftige Kommunikationen

Bürger, Kunden und Patienten erwarten, dass Organisationen ihre Prozesse beherrschen und im Grundsatz an einem fairen Umgang orientiert sind, als Voraussetzung dafür, dass sie in deren Aktivitäten vertrauen und dass umgekehrt Organisationen ein solches Vertrauen auch voraussetzen oder klar abfordern. Ein Arzt ist zunächst vor allem ein Arzt, dem man in dieser Funktion vertrauen kann. Dem Arzt ist wie dem Patienten daran gelegen, dessen Gesundheit wieder herzustellen. Dafür muss der Arzt genau kein Freund des Patienten sein und er sollte erst in zweiter Linie Kaufmann sein müssen. Der Patient kann dann anstatt in Personen in Prinzipien vertrauen. Diese Art des funktionalen, nicht-personalisierten Vertrauens zu gewähren und zu beanspruchen, macht moderne Gesellschaften effektiv; moderne Gesellschaften sind in einem ganz besonders hohen Maße insofern auf nichtpersonalisierte Vertrauensbeziehungen angewiesen.[22] Aber es macht sie auch katastrophenanfällig, insbesondere wenn sich die strukturell mächtigere Seite nicht an die Regeln hält. Dann implodieren Märkte, entsteht Korruption der Verwaltung , sind keine an Wahrheit orientierte Diskurse oder Hilfeleistungen erwartbar.

Die im Alltag bestehenden Ansprüche an eine verläßlich-vernünftige technische Infrastruktur lassen sich, dies sei zum Schluß noch kurz angesprochen, zu den „Geltungsansprüchen an eine vernünftige Rede“, gemäß der Theorie des kommunikativen Handelns, in Beziehung setzen.[23] Gemäß dieser Theorie müssen Menschen, die miteinander sprechen, immer schon be-

[22]Zum Begriff des Vertrauens: Luhmann 1975.

[23]Habermas 1981. Durch das Einpassen des Datenschutzes in die soziologische Theorie der funktionalen Differenzierung (Luhmann) sowie die Analogiebildung der Schutzziele zu den Anforderungen an eine vernünftige Kommunikation (Habermas) oder auch zu den symbolisch generalisierten Kommunikationsmedien (Luhmann) wird ein Begründungszusammenhang für Datenschutz freigelegt, der sich nicht mit einem postulierten

stimmte Ansprüche als vernünftigerweise für beide Seiten im gleichen Maße geltend voraussetzen, soll ihr Miteinander funktionieren. Bei der Nutzung moderner Kommunikationstechniken, ob Telefon oder Internet, werden diese verallgemeinerbaren Anforderungen an eine vernünftige Rede und deren Inhalte weiterhin als erfüllbar bzw. erfüllt vorausgesetzt. Vor diesen Vernunft-Unterstellungen der Rede müssen jedoch die latenten Anforderungen an ein vernünftiges Funktionieren der technisch-organisatorischen Infrastrukturen erfüllt sein! In diesen Bezugsrahmen eingespannt, können die Schutzziele als vernünftige Anforderungen bzgl. der Beherrschbarkeit von Prozessen und Fairness in Interaktionen gelten. Umgesetzte Schutzziele sind die Basis für gewährtes und beanspruchtes Vertrauen in die technischen Infrastrukturen moderner Gesellschaften. Datenschutz macht diese Anforderungen in Form der Schutzziele insofern sichtbar, für Akteure konstruktiv zugänglich und für die Gesellschaft bewertbar. Datenschutz kann es deshalb nicht akzeptieren, wenn Organisationen Anforderungen an Integrität und Vertraulichkeit, an Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als falsch oder historisch überholt diskreditieren, um sie dann ignorieren und vorsätzlich verletzen zu können. Inwieweit in diesem Sinne somit bspw. Google und Facebook die Schutzziele umsetzen, das einmal anhand der Schutzziele durchzuspielen, um anschließend die verallgemeinerungsfähige Vernünftigkeit dieser Infrastrukturen für die Nutzer zu beurteilen, überlasse ich nun gern der Leserin und dem Leser.

6 Literatur

- Borcea-Pfitzmann, Katrin / Pfitzmann, Andreas / Berg, Manuela, 2011: Privacy 3.0 := Data Minimization + User Control + Contextual Integrity; in: Information Technology, Nr. 53, Oldenbour Verlag, München: 34-40.

- BSI 2008: IT-Grundschutz, https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html.

- Clipper, Sebastian, 2011: Information Security Risk Management - Risikomanagement mit ISO/IEC27001, 27005 und 31010, 1. Auflage, Vieweg+Teubner

privaten Bedürfnis nach Schutz von Privatheit als Ausgangspunkt bescheidet, sondern diesen Ausgangspunkt selber noch theoretisch zugänglich macht.

- Federrath, Hannes / Pfitzmann, Andreas, 2000: Gliederung und Systematisierung von Schutzzielen in IT-Systemen; in: DuD – Datenschutz und Datensicherheit, Heft 12, Dezember 2000: 704-710.
- Habermas, Jürgen, 1981: Theorie des kommunikativen Handelns (Band 1: Handlungsrationalität und gesellschaftliche Rationalisierung, Bd. 2: Zur Kritik der funktionalistischen Vernunft), Frankfurt am Main, Suhrkamp.
- Hansen, Marit / Meinser, Sebastian (Hrsg.), 2007: Verkettung digitaler Identitäten, https://www.datenschutzzentrum.de/projekte/verkettung/.
- Lischka, Konrad, 2011: Die ganze Welt ist meiner Meinung, Vorgefiltertes Web, Spiegel Online vom 11.03.2011, http://www.spiegel.de/netzwelt/web/0,1518,750111,00.html).
- Luhmann, Niklas, 1975: Vertrauen, Frankfurt am Main, Suhrkamp.
- Luhmann, Niklas, 1999: Gesellschaft der Gesellschaft, Frankfurt am Main, Suhrkamp.
- Meints, Martin, 2007: Datenschutz durch Prozesse, Musterprozesse für das Datenschutzmanagement; in: DuD - Datenschutz und Datensicherheit, 31. Jahrgang, Heft 2: 91-95.
- Meints, Martin / Zwingelberg, Harald, 2009: Identity Management Systems – recent developments; http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf.
- Nissenbaum, Helen, 2004: Privacy as contextual integrity; in: Washington Law Review, http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.
- Pfitzmann, Andreas / Garstka, Jürgen / Roßnagel, Alexander, 2001: Modernisierung des Datenschutzrechts (Gutachten im Auftrag des Bundesministerium des Innern, http://www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf.
- PRIME / FIDIS, Privacy and Identity Management for Europe, https://www.datenschutzzentrum.de/projekte/idmanage/.

- ReCoBS / RSBAC, http://www.rsbac.org, sowie: https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/Gefaehrdungen/AktiveInhalte/schutzmoeglichkeiten/recobs/loesungsansatz.html.

- Sohn-Rethel, Alfred, 1978: Warenform und Denkform, 1. Auflage, Frankfurt am Main, Suhrkamp.

- Rost, Martin, 2008: Gegen große Feuer helfen große Gegenfeuer, Datenschutz als Wächter funktionaler Differenzierung; in: Vorgänge, Heft 4/2008, Nr. 184: 15-25, http://www.maroki.de/pub/privacy/Vorgaenge0804_cla.pdf.

- Rost, Martin / Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6: 353-358.

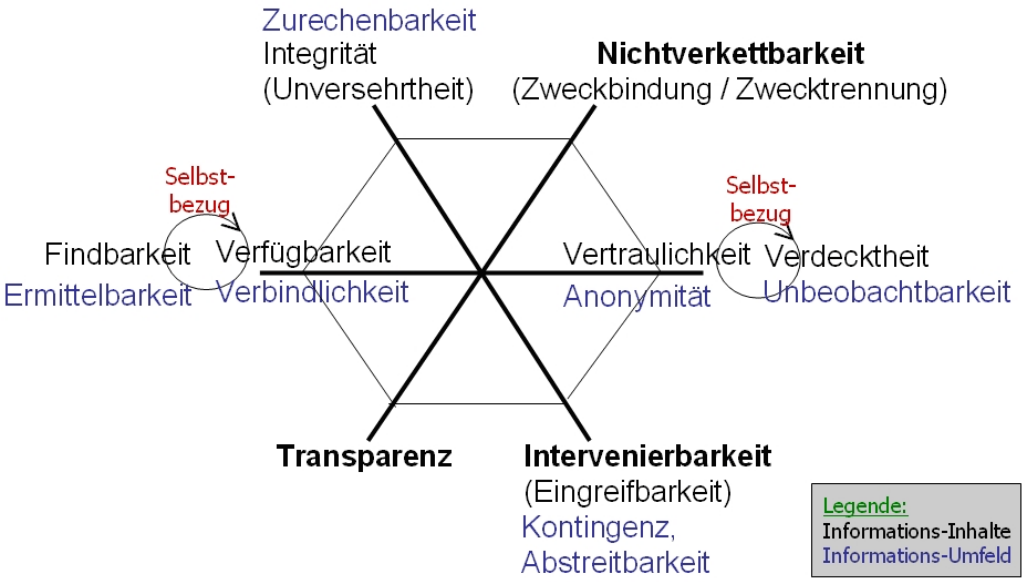
- Rost, Martin / Bock, Kirsten, 2011 Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-34.

- Rost, Martin, 2011: Datenschutz in 3D - Daten, Prozesse und Schutzziele in einem Modell; in: DuD - Datenschutz und Datensicherheit, 35. Jahrgang, Heft 5: 351-355.

- Rost, Martin, 2011a: Das facebook-Problem, in: „Mitteilungen“ der Humanistischen Union e.V., vereinigt mit der Gustav Heinemann-Initiative, Nr. 214 (im Erscheinen), siehe: http://www.maroki.de/pub/privacy/HU-Mitteilungen-facebook.pdf.

- Zeh, Juli, 2009: Corpus Delicti, Frankfurt am Main, Schöffling & Co.

7 Anhang



Die Systematik der Datenschutzziele (angelehnt an: Rost/ Pfitzmann 2009)