Zur Konditionierung von Technik und Recht mittels Schutzzielen

Martin Rost
Dr. Katalin Storf

Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
martin-rost@web.de

Abstract: Die Vermittlung von Recht und Technik darf dann auf beiden Seiten als gelungen gelten, wenn einerseits deren Eigenlogiken des Normativen und des Funktionalen bewahrt bleiben und andererseits Aktivitäten der einen Sphäre in der anderen Sphäre stimmig in die spezifische Eigenlogik eingepasst werden können. Diese Anforderung müssen Datenschutzbehörden in ihren alltäglichen Aufsichtstätigkeiten gesellschaftlich überzeugend erfüllen. Deshalb lohnt gerade auch für theoretisch geleitete generellen Fragen zur „Vermittlung“ ein Blick auf das aktuell unter den Aufsichtsbehörden diskutierte standardisierte Prüfkonzept für die Datenschutzpraxis.

1 Technik und Recht[1]

Was bedeutet es, wenn bei einer Datenschutzprüfung eines Verfahrens TechnikerInnen und JuristInnen zusammenarbeiten?[2] Die unerfahrene Juristin eines Prüfteams fordert ein „Löschen“ von Daten und erwartet darunter ein „Zerstören“ mit anschließendem „Nicht mehr da sein“, weil die fortgesetzte Speicherung eines Datums nicht mehr erforderlich ist. Was für die Datenschutz-Juristin damit als hinlänglich operationalisiert und dadurch verfahrenstechnisch geklärt gelten mag, erzeugt beim Datenschutz-Techniker offene Fragen. Dem Techniker bleibt dann häufig genug die Entscheidung darüber zu treffen, ob mit dem geforderten „Löschen“ ein Sperren, ein „Rüberschieben auf das Mülleimersymbol“, ein Austragen aus der Dateisystemtabelle, ein mehrfaches Überschreiben eines Festplattenbereiches oder ein physikalisches Zerstören eines magnetischen Datenträgers angemessen ist. Wobei er auch mehrere Kopien von Backups bedenkt, die im Tresor eines Nachbargebäudes oder auf einem in das Dateisystem eingebundenen Cloud-Laufwerk gespeichert sein könnten. Kontrollierte, standardisierte Löschprozesse kosten Geld. Was ist angemessen? Selbst wenn Juristin und Techniker gemeinsam erörtern, welche Qualität eines „Löschens“ der zu prüfenden Organisation aufzuerlegen angemessen ist, wie steht es bspw. um die Integrität und Transparenz dieser Entscheidungsfindung gegenüber der

[1] Die dieser Publikation zugrundeliegende Arbeit wurde teilweise vom FutureID-Projekt (www.futureid.eu) unterstützt, das im 7. Forschungsrahmenprogramm der europäischen Union gefördert wird (Grant Agreement No. ICT-318424).

[2] Wir benutzen fortan abwechselnd weibliche und männliche Wortformen.

geprüften Organisation, betroffenen Personen, anderen Organisationen sowie den KollegInnen der Datenschutzaufsicht in einem anderen Bundesland, die möglicherweise vor zwei Jahren in einem etwas anders gelagerten Kontext zu einem anderen Ergebnis gekommen waren? Zusammenarbeit bzw. Interdisziplinarität bezeichnet insofern erst einmal ein weiteres Kommunikationsproblem als schon die Lösung.

Realistisch betrachtet agieren Experten unterschiedlicher Disziplinen bzw. Sphären, die wie bei einer Datenschutzaufsichtsbehörde zusammen arbeiten müssen, wechselseitig im Modus pragmatischer Dilettanten. Im besten Falle gelingt es mit der Form des „unmittelbaren Aufeinanderprallen“ als Zusammenarbeit die „No Gos“ der beiden Disziplinen zu klären, was bei einfachen Anforderungen an eine Prüfung ausreichen kann. Was dadurch jedoch nicht gelingt, sind Prüfungen und insbesondere Beteiligungen bei der Planung von Verfahren mit komplexen Abhängigkeiten und vielen Unwägbarkeiten, bei denen beide Seiten, etwa im Sinne eines proaktiven „Privacy By Design“, auf unterschiedlichen Ebenen mit unterschiedlichen Auflösungen der Probleme konstruktiven Einfluss auf ein Verfahren nehmen [Boc11]. Durch den Rückgriff auf die (Systematik der) Schutzziele, als einem gemeinsamen Dritten von Technik und Recht, wird es möglich, beide Sphären systematisch so aufeinander zu beziehen, dass diese einerseits ihre jeweiligen Eigenlogiken bewahren und dadurch bei einer Verfahrensprüfung ihre volle Leistungsfähigkeit ausspielen können, und zugleich ihren Einfluss auf die jeweils andere Sphäre wirksam geltend machen können.

Schutzziele spannen einen Rahmen auf, in dem als erstes juristisch abgewogen und rechtliche Entscheidungen getroffen werden können. Im Anschluss der durch Schutzziele kanalisierten Abwägungen können dann die entsprechenden Funktionen eingerichtet und diese mit Schutzmaßnahmen ausgestattet werden, im besten Falle anhand eines standardisierten Maßnahmenkatalogs, der dem „Stand der Technik“ entspricht [Ros12b]. Die Vermittlung von Recht und Technik gelingt insofern dadurch, dass die Schutzziele einerseits mit Katalogen von technischen und organisatorischen Maßnahmen verbunden sind [Pro12] und Schutzziele andererseits a) die wesentlichen Anforderungen des Datenschutzrechts enthalten – wie die Sicherstellung der Zweckbindung, der Transparenz, der Erforderlichkeit, der Datensparsamkeit und der Umsetzung der Betroffenenrechte – und b) die verbleibende Abwägung der rechtlichen Anforderungen durch die Systematik der Schutzziele kanalisieren [Mei12]. Das soll nachfolgend erläutert werden.

2 Das generelle Problem von „Vermittlung“

Abstrahiert man Technik als ein „Sein“ – und denkt als Beispiele an Gegenstände, Maschinen und Software –, und Recht als ein „Sollen“ – und denkt als Beispiele an die ersten Artikel des Grundgesetzes oder an die Straßenverkehrsordnung oder an den Arbeitsvertrag –, so kann man mit dem schottischen Philosophen David Hume gut begründet zunächst behaupten, dass aus einem Sein kein Sollen folgt. Ein Sollen kann man nicht erkennen, man kann sich nur bekennen. Auch Immanuell Kant bestätigte bekanntlich die Vorstellung einer tiefen Kluft zwischen den beiden Sphären, die in Deutschland über den einflussreichen Rechtsphilosophen Gustav Radbruch bis in die heutige Diskurstheorie des Rechts

hineinreicht, wonach unter Recht vornehmlich ein (wenn auch sachgerecht zu führender) normativer Diskurs verstanden wird [Ale08]. Nimmt man Bezug auf aktuelle Theoriedesigns, wie das der soziologischen Systemtheorie, dann schärft diese Theorie die Vorstellungen darüber, wie „Vermittlung“ möglich sein kann, die eher die Differenz belässt als die Identität des Vermittelten erzwingt. Das Vermittlungs- bzw. Transformationsproblem darf theoretisch betrachtet nicht dann als bewältigt angenommen werden, wenn a) das eine im anderen vermeintlich aufgelöst ist; wenn b) das Problem der Transformation mit Begriffen wie Zusammenarbeit, Interdisziplinarität oder Transdisziplinarität eigentlich nur benannt bzw. versteckt wird; oder wenn c) das Problem in das Irgendwie der Psyche von „Doppel-Experten“, die sich in beiden Sphären gut auskennen, verlagert wird.

Entsprechend der soziologischen Systemtheorie fungiert Recht als ein „geschlossenes soziales Funktionssystem der Gesellschaft“ [Luh93] neben anderen Funktionssystemen, dessen Kommunikationen sich ausschließlich entlang der kommunikativ reproduzierten Differenz „Recht“ und „Nicht-Recht“ verketten. Die Orientierung an Rechtstexten (Gesetzen, Verträgen usw.) lassen Kommunikationen zwischen den beiden Seiten oszillieren. Die Referenz des Rechts zur „Welt“ geschieht insofern über „Gesetze“. Entscheidend ist: Das Recht entfaltet sich im Recht und mit rechtlichen Mitteln. Alle anderen Einflüsse – also auch aus dem Bereich der Technik, der Wirtschaft, der Wissenschaft, der Kunst, der Religion –, gelten als Störungen, die in eine rechtliche, normative Form zu bringen sind, wenn sie als Recht behandelt werden sollen. So wie es einer Transformation von Störungen ins Recht bedarf, gilt auch umgekehrt, dass andere gesellschaftliche Sphären Recht nicht sozusagen unmittelbar und direkt verstehen. Auch die anderen Sphären nehmen das Recht als Störungen wahr und sind gezwungen, diese mit ihren eigenen Strukturen als Informationen für sich zu verketten.

In Bezug zur Bestimmung von „Technik“ notiert Halfmann: „Technik kann wie Recht als eine Form sozialer Zukunftsbindung verstanden werden. Allerdings manifestiert sich die Bindung der Technik in Installationen und nicht in Normen. “ [Hal11, 97] Wir verzichten nach Durchsicht vieler ähnlich lautender Definitionsangebote ohne erkennbaren Abstraktionsgewinn und bezeichnen mit Technik übergreifend handfeste Artefakte, Werkzeuge, Maschinen und „großtechnische Systeme“ [Hug88] sowie Automaten und Algorithmen [Kem89].

Über das Verhältnis von Technik und Recht ist bereits viel geschrieben worden. Als aktuelle Referenz sei das „Handbuch des Technikrechts“, aus dem auch das Halfmann-Zitat entnommen ist, zumindest genannt [Sch11]. Am Beispiel der Problemlage des Verhältnisses von Verwaltungsrechtswissenschaft und Gesellschaftstheorie bzw. Soziologie diskutiert Lüdemann drei Modelle von Bezugnahmen verschiedener Sphären untereinander und unterscheidet das Abstinenz-, vom Konvergenz- und Divergenzmodell, die auch für die kurze Diskussion unserer Problemstellung heranzuziehen nützlich ist [Lüd09]. Im Abstinenzmodell behilft sich der Laie mit ad-hoc gebildeten Alltagstheorien. Der Laie bleibt und agiert als Laie in der Sphäre des Experten. Allerdings besteht hier das latente Risiko, dass die berechtigte Reputation als Experte aus der einen Sphäre auf die andere Sphäre ausgedehnt wird. Im Konvergenzmodell wird eine der beiden Sphären als die dominierende ausgegeben, der sich die andere Sphäre unterordnet. Dabei werden dann typisch Methoden der anderen Sphäre übernommen. Im besten Falle agiert der Experte einer Sphäre dann als

methodischer Quasi-Experte der anderen Sphäre, nur gemeinhin auf einem vorläufigeren Niveau. Das Divergenzmodell liegt zwischen den beiden anderen Modellen. Dies denkt Lüdemann in der Form, dass der Quasi-Experte nur über eine „allgemeinere Theorie aus der Nachbarwissenschaft“ verfüge. Lüdemanns Ausführungen zu diesem Modell sind zwar wortreich, bleiben aber im Ausweis der spezifischen Differenz blass, welche spezielle Vermittlungsleistung von diesem Modell bzw. von den Beteiligten erwartet werden darf. Unser Vorschlag im gegenüber Lüdemann erweiterten Sinne des Divergenzmodell wird darin bestehen, dass es sowohl eine funktionale Segmentierung im Sinne des Abstinenzmodells erlaubt und zugleich auf etwas Drittes als etwas gemeinsam Imaginiertes referenziert, und dadurch Konvergenzeffekte auslöst. In Bezug auf dieses Dritte können Vertreter beider Sphären dann sowohl den Experten- als auch den Laienstatus einnehmen. Als dieses gemeinsame Dritte werden, am Beispiel des Datenschutzes, nachfolgend Schutzziele diskutiert.

2.1 Das Divergenzmodell zur Vermittlung von Recht und Technik

Im Fokus der nachfolgenden Ausführungen steht nicht ein Nachzeichnen der aktuellen Diskussion zu den Bedingungen der Möglichkeit von Interdisziplinarität zwischen verschiedenen Fachwissenschaften. Uns geht es vornehmlich um die Bearbeitung von Problemlagen speziell von Datenschutzaktivitäten – also Prüfungen und Beratungen von Organisationen in Bezug auf deren Beachtung der Grundrechte von Bürgern, Kunden, Individuen –, die mit der stets riskant bleibenden Vermittlung speziell zwischen technischen Artefakten und Normentexten ringen. Es ist dabei nicht ins wissenschaftlich-diskursive Belieben gestellt, wie Datenschützer dabei mit dieser Vermittlung umgehen, sie müssen gesellschaftliche akzeptable Entscheidungen bei ihren praktischen Tätigkeiten finden.

Im Sinne des Konvergenzmodells gilt es, die „Eigenlogik“ der Sphären Technik und Recht jeweils anzuerkennen – hier die Sphäre vorwiegend kausal kontrollierbarer Funktionen, in denen Organisationsentscheidungen letztlich materiell gebunden sind, dort die Sphäre normativer Anforderungen – und von einer der beiden Sphären dann die Führung zu behaupten. So fordern die Anwälte des Rechts gegenüber der Technik (und deren Anwälten), dass Technik dem sich im Recht ausdrückenden kollektiven Willen, der über die politische Wahl des Gesetzgebers ermittelt wird, der Menschen bzw. der Gesellschaft schlicht zu folgen habe. Hiernach soll(!) Recht also die Technik, deren Gestaltung und Anwendung, führen.[3] Diese Vorstellung vom rechtlichen Primat bildet, wie bei allen anderen Verwaltungen auch, die Arbeitsgrundlage der Aktivitäten der Datenschutzaufsichtsbehörden in Deutschland. Wie Techniker diese Normen dann in der alltäglichen, rauhen Prüf- und Beratungspraxis operationalisieren, also wie sie Normen in Wirkungen übersetzen bzw. bestehende Verfahren auf Normengerechtigkeit hin bewerten, bleibt erfahrungsgemäß weitgehend den Technikern überlassen.

Auf der anderen Seite entwickeln Techniker Techniken, die viele Menschen nützlich finden, und in denen sich faktisch durch Nutzung ein kollektiver Wille ausdrückt. Dieser

[3] Stellvertretend für viele dieser Vorstellungen [Gus89].

kollektive Wille besteht auch dann, wenn diese Techniken von Organisationen betrieben werden, die mit Hilfe der Technik datenschutzrechtlich betrachtet Grundrechte und Datenschutz missachten und insofern der politischen und rechtlich objektiven Interessenslage der Menschen entgegenlaufen.[4] Insbesondere erwarten Techniker, dass das Recht nicht an der technischen Praxis vorbei etwas regelt, was möglicherweise gesellschaftlich wünschenswert sein mag aber technisch nicht umsetzbar ist.[5] Oder die Technik ist überholt oder disfunktional oder funktioniert sogar effektiver als normativ gefordert.

Eine andere Variante des Konvergenzmodells besteht darin, nicht nur Führung einer Sphäre zu behaupten, sondern eine der beiden Sphären in der jeweils anderen aufzulösen. So sind Informatiker erfahrungsgemäß vielfach entsetzt, wenn sie nach erstmaliger systemanalytischer Befassung mit Gesetzestexten gewahr werden, dass diese nicht der von ihnen geforderten Anforderung nach zumindest aussagenlogischer Widerspruchsfreiheit genügen – oder anders formuliert: dass Normentexte nicht wie Algorithmen und Gerichte nicht wie Automaten funktionieren – und halten diese Eigenschaften für eine in Zukunft dringlich zu behebende Schwäche. Man findet im Umfeld des Datenschutzes außerdem die Gegenposition dazu vertreten, wonach Technik eine Materialisierung von politischer Macht bzw. des Rechts begriffen wird, gemäß der Vorstellung, dass die Führung menschlicher Handlungen durch Automaten als Handlungsnorm ohne Freiheitsgrade zu interpretieren. In Technik geronnene Macht durch Normen drückt sich bspw. in Industrienormstandards oder auch der populären Formel „Code is Law“ [Les01] aus.

Wir halten eingedenk dieser hier nur ganz grob skizzierbaren Positionen die unsere Position, im erweiterten Sinne des Divergenzmodells wie folgt fest: Technik und Recht sind sowohl analytisch als auch faktisch unterschiedliche Sphären mit unterschiedlichen Objekten und Eigenlogiken. Sowohl durch Gesetze als auch durch die „normative Kraft des Faktischen“ (Luhmann) drückt sich kollektive Selbstbestimmung bzw. ein „Interesse und Wille“ aus. Beide Sphären beeinflussen einander, sie führen wechselseitig, wobei die geführte Sphäre die Führung mit ihrer Logik spezifisch reflektiert. Nicht dem Recht allein sondern auch der Technik ist zweifelsfrei „Technikgestaltung“ zuzugestehen, so wie auch andere Funktionssysteme der Gesellschaft Technikentwicklungen beeinflussen.[6] Wir folgen beim Verständnis von „Vermittlung“ der allgemeinen soziologischen Systemtheorie und deren Paradigma von der „Offenheit durch Geschlossenheit“, sowie im Speziellen dem Ansatz von Helmut Willke, der Steuerungswirkungen in Bezug auf geschlossene Sinnsysteme in der Form der „Kontextsteuerung“ und der „Anregung zur Selbststeuerung“ ausweist [Wil99].

Wie riskant es ist, ein rechtlich einwandfreies Urteil für technisch gestützte Verfahren zu fällen, zeigte sich eingangs beim vermeintlich trivialen Beispiel des „Löschens“. Es zeigt

[4] Man denke insbesondere an die Aktivitäten von Amazon, Apple, Facebook, Google, Microsoft, Twitter sowie an die Möglichkeit staatlicher Sicherheitsbehörden – Stichwort „PRISM “und „TEMPORA“ –, die inzwischen erwiesenermaßen über ihre eigenen Datensammlungen hinaus sich jederzeit auch Zugriff auf diese Privatdatenbestände verschaffen können [gD12].

[5] Man denke an den „digitalen Radiergummi“ des X-Pire-Projekts. Seit 2011 ist es erwiesen, dass diese Anforderung im Internet technisch nicht umsetzbar ist [Fed11]; trotzdem ist in der aktuellen Version der EU-Verordnung ein Recht auf „Recht auf Vergessen“ auch im Internet nach wie vor enthalten [Hof13, Wac13].

[6] Eine faire und sensible Darstellung der Eigenlogiken der verschiedenen Funktionslogiken findet sich bei [Ste93], der zwar das Problem und die Notwendigkeit zu deren Vermittlung in Bezug auf Datenschutz aufzeigte, aber keine überzeugende Lösung anzubieten wusste.

sich insbesondere bei der datenschutzrechtlich zentralen Anforderung nach „Zweckbindung“ einer Datenverarbeitung mit Personenbezug. Diese Anforderung wird, noch auf juristischer Seite leidlich insbesondere durch „Trennung“ bzw. „Aufrechterhalten von Grenzen“ operationalisiert, zumeist begleitet von einer Aufzählung von Verarbeitungszwecken, die thematisch benachbart liegen und genau deshalb nicht erlaubt sind.[7]. Wie erzeugt man nun technisch angemessen wirkungsvolle Grenzen, die auch nachhaltig aufrecht erhalten bleiben?

2.2 Beispiel „Zweckbindung“ – Wie setzt man eine gesetzliche Anforderung technisch um?

Gegeben sei folgende Konstellation: Die Landesbeauftragte für Datenschutz sieht sich aufgefordert, ein Verfahren zu bewerten, das als Vorgangsbearbeitungssystem von der Polizei betrieben wird. Die Datenschutzbeauftragte weist zwei Mitarbeiter an, eine Technikerin und einen Juristen, die Eigenschaften des Verfahrens im Hinblick auf Vereinbarkeit mit dem Datenschutzrecht zu prüfen. Die Mitarbeiter stellen fest, dass die IT des zu prüfenden Polizei-Verfahrens im Rechenzentrum (RZ) des Landes betrieben wird, das außerdem die IT für die Landtagsabgeordneten, die Parteibüros im Landeshaus, die General-Staatsanwaltschaft sowie einiger Gerichte unterschiedlicher Instanzen sowie sämtlicher Kreise und Kommunen und den oberen Landesbehörden sowie des Landesverfassungsschutzes gemeinsam hostet und administriert. Und auch die Datenschützer der Landesbeauftragten für den Datenschutz arbeiten auf Maschinen in diesem Rechenzentrum. Unter dem Aspekt der Gewaltenteilung und Sicherstellung der Zweckbindung einer jeden Datenverarbeitung mit Personenbezug sowie der Aufsicht darüber stellt das Rechenzentrum somit einen zweifelsfrei riskanten operativen Kurzschluss dar, der sich für Betroffene negativ auswirken kann.

Aus der Prüfperspektive stellt sich die Frage, welche normative Soll-Vorgabe besteht, mit der die verfassungsgemäß gebotene Zweckbindung bzw. Zwecktrennung von Verfahren, die letztlich den Bürger vor staatlicher Willkür schützen soll, nun tatsächlich wirksam und angemessen durchgesetzt wird. Aus der Technikperspektive gibt es verschiedene Möglichkeiten, eine semantisch dominierte Definition von Zweckbindung durch formale Trennungen auf verschiedenen Ebenen sicherzustellen. Trennung kann bedeuten, dass die Daten-Erhebung, die Speicherung und Verarbeitung, die IT-Systeme sowie die Verarbeitungs-, Administrations- und Sicherungs-Prozesse physikalisch getrennt betrieben werden. Die Datenschützer könnten insofern fordern, dass für Teile des Verfahrens bzw. generell für jedes Verfahren eigenes Personal, untergebracht in unterschiedlichen Räumen bzw. Gebäuden, vorzusehen ist. Doch gäbe es auch mit dieser Lösung genügend weitere operative Kurzschlüsse, etwa organisatorischer Art über die Leitung des Rechenzentrums. Das unbedingt zu beachtende Gebot der Trennung wäre insofern noch zuverlässiger um-

[7] Mit dem Einzug des Internet als weltweitem „Verbreitungsmedium“ [Luh97, S. 202ff] steht derzeit ganz generell die Suche nach gesellschaftlichen Lösungsmodellen für das Problem an, wie einzelne Systeme sicher gekoppelt aber ebenso sicher getrennt und isoliert voneinander betrieben werden können. Dies ist die operative Voraussetzung für die Durchsetzung von Gewaltenteilung, Märkten und freien wissenschaftlichen und ästhetischen Diskursen [Ros97, Ros13b]

gesetzt, wenn unterschiedliche Rechenzentren innerhalb eines Landes oder besser noch: in unterschiedlichen Bundesländern oder über die Welt verteilt zum Einsatz kämen. Als eine rechtskonforme Trennung von Gewalten und Verfahren innerhalb eines Rechenzentrums könnte es allerdings ausreichen, wenn unterschiedliche Verfahren auf unterschiedlicher Hardware, die im gleichen Raum untergebracht ist, liefen. Oder wenn sie auf derselben Hardware, aber mit virtualisierten Betriebssystemen und Servern, mit verschlüsselten Datenspeichern und Backupservern liefen. Das wäre auf jeden Fall die preiswerteste Lösung und stellte den Betriebswirt zufrieden. Wobei der Betriebswirt vielleicht sogar die noch günstigere Lösung vorschlüge, entweder jedes Verfahren als einen Mandanten innerhalb einer großen Datenbank zu implementieren oder eine Verfahrenstrennung allein durch das Management von Zugriffsrechten in der Datenbank herbeizuführen.

Der Jurist des Prüfteams könnte allein aus der normativen Perspektive argumentierend fordern, dass die IT der Polizei nicht im Landesrechenzentrum betrieben werden darf, weil dadurch die Gewaltenteilung auf der operativen Ebene durchbrochen und die Zweckbindung der Datenverarbeitung zu leicht operativ auszuhebeln sei. Als Kompromiss zeichnete sich ab, dass jede der drei Gewalten ihr eigenes Rechenzentrum betriebe, ebenso der Bund, die Länder und jede einzelne Kommune sowie jedes Ministerium für sich. Die Sicherheit der Trennung hängt dann im Grunde von der persönlichen Integrität der Leitungsebenen der verschiedenen RZen ab. Allerdings teilt ihm die Polizei dann möglicherweise mit, dass diese sehr froh darüber sei, ihre IT nicht mehr wie in den vergangenen Jahrzehnten dilletantisch selber administrieren zu müssen, sondern endlich den ungleich professioneller gesicherten Betrieb des landesweit genutzten RZ nutzen zu können. Die Technikerin sieht unter diesen Bedingungen das Trennungsgebot hinreichend umgesetzt, wenn eine ganze Reihe von Schutzmaßnahmen der IT-Sicherheit und des operativen Datenschutzes, nachweislich und jederzeit überprüfbar, eingehalten werden, weil es faktisch heute keine Alternative zum professionellen zentralen RZ-Betrieb mehr gibt. Außerdem kommt es der notorisch unterbesetzten Datenschutzaufsicht durchaus gelegen, im RZ an zentraler Stelle konzentriert die Ordnungsmäßigkeit der Datenverarbeitung überwachen zu können. Wie können nun die politischen Entscheider, das IT-Steuerungsgremium des Landes, das Innenministerium, die Polizei, das Rechenzentrum, die IT-Sicherheitsbeauftragten und die Datenschützer sich nun so einigen, ohne dass eine der beiden Sphären vernachlässigt wird bzw. ohne dass der normative Gehalt der Grundrechte verloren geht? Mit methodischer Perspektive gefragt: Wie lässt sich das unausweichlich immer bestehende Transformationsrisiko zwischen Technik und Recht, das der Datenschutz praktisch bearbeitet, vernünftig beherrschen?

Die von uns vorgeschlagene methodische Lösung dieses Problems besteht nicht darin zu zeigen, dass es am Ende kein Problem mehr gibt. Es bleibt selbstverständlich weiterhin das Transformationsproblem zwischen Technik und Recht bestehen, weshalb wir insofern für das Divergenzmodell votieren. Die Systematik der sechs „elementaren Schutzziele“ macht es beiden Sphären jedoch möglich, ihren gegenseitigen Einfluss mit den eigenen Mitteln kontrollierbar geltend zu machen. Insofern formulieren die Schutzziele gerade an den Transformationprozess seinerseits zu erfüllende Anforderungen. Auf diese Weise wird aus dem schlecht kalkulierbaren Vertrauensproblem ein allseits besser kalkulierbares Entscheidungsproblem.

3 Die Systematik der sechs elementaren Schutzziele des Datenschutzes

Schutzziele spielen seit Ende der 1980er Jahre eine Rolle in der Gestaltung technischer Systeme, deren Sicherheit gewährleistet sein muss.[8] Hiernach zählen zu den „klassischen" Schutzzielen der Datensicherheit (oder Informationssicherheit) und auch des Datenschutzes:

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit.

Diese Schutzziele formulieren Anforderungen an einen sicheren Betrieb insbesondere von Organisationen in Bezug auf Geschäftsprozesse. Organisationen müssen sich vor Angreifern schützen, die als externe oder interne Hacker auf Daten und Prozesse der IT einer Organisation zugreifen wollen. Ein sicherer Betrieb von Behörden, Unternehmen und Forschungsinstituten ist dabei zweifelsfrei auch im Interesse von Bürgern, Kunden, Patienten und Mandanten. Datenschutz ist insofern ohne Datensicherheit nicht möglich. Aber Datenschutz nimmt primär die Perspektive von betroffenen Personen gegenüber Organisationen ein. Insofern verfolgen Datensicherheit und Datenschutz teilweise einander widersprechende Ziele. Deshalb bedarf es, zusätzlich zu den genannten drei Schutzzielen der Datensicherheit, spezifischer Schutzziele, die die Risiken betroffener Personen gegenüber Organisationen thematisierbar machen. Diese Datenschutz-Schutzziele im engeren Sinne sind

- Transparenz,
- Intervenierbarkeit und
- Nichtverkettbarkeit.

Das Schutzziel *Verfügbarkeit* bezeichnet die Anforderung, dass ein gesicherter Zugriff auf Informationen innerhalb festgelegter Zeit bestehen muss. Hiernach sollen also Informationen zeitgerecht zur Verfügung stehen und ordnungsgemäß verwendet werden können. Umgesetzt wird dieses Schutzziel technisch vor allem dadurch, dass von Daten Sicherheitskopien gemacht werden und getestet wird, ob solche Sicherheitskopien auch wieder eingespielt werden können. Verfügbarkeit eines Systems bedeutet, dass bei einem Ausfall ein anderes System ersatzweise einspringen kann, bevorzugt ohne dass die Nutzer von diesem Ersatz etwas bemerken. Organisatorisch lässt sich dieses Ziel umsetzen, indem man bspw. Reparaturstrategien einrichtet oder Vertretungsregelungen für ausfallende Mitarbeiter bestehen.

[8] Zur Einführung in eine erste Konsolidierung der Systematisierung der Schutzziele siehe [Pfi00] sowie den Systematisierungsversuch der 2. Generation, der bereits den Unterschied von IT-Sicherheit / technisch-organisatorischem Datenschutz markierte, siehe [Pfi09].

Das Schutzziel *Integrität* bezeichnet die Anforderung, dass ein System ausschließlich seine zweckbestimmte Funktion verlässlich und erwartungsgemäß erfüllt. Etwaige Nebenwirkungen müssen dabei wenn möglich ausgeschlossen oder aber berücksichtigt sein. Daten müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Umgesetzt wird dieses Schutzziel dadurch, dass von gespeicherten oder versendeten Daten Prüfsummen vor und nach einer Aktion erzeugt und miteinander verglichen werden. Wenn die Prüfsummen nach einem Vergleich übereinstimmen, darf man sichergehen, dass die Daten in der Zwischenzeit nicht verändert wurden. Die Integrität technischer oder organisatorischer Prozesse und Systeme überprüft man dadurch, dass man die Ist-Werte eines Prozesses misst und diese mit den vorher festgelegten Soll-Werten eines Prozesses vergleicht. Wenn die Ist-Werte innerhalb der oberen und unteren Soll-Werte liegen, funktioniert ein Prozess so, wie er funktionieren soll.

Das Schutzziel *Vertraulichkeit* bezeichnet die Anforderung, dass nicht zuständige, unbeteiligte Dritte keine Möglichkeit haben, von Daten unbefugt Kenntnis zu bekommen oder ein System einzusehen und Betroffene identifizieren zu können. Umgesetzt wird dieses Schutzziel in Bezug auf Daten durch Verschlüsselung von gespeicherten oder transferierten Daten. Im Hinblick auf Prozesse und System sorgt vor allen Dingen eine physikalische Abschottung von Räumen oder Netzbereichen voneinander dafür, dass niemand unerlaubt Zugriff auf andere Prozesse und Systeme nehmen kann.

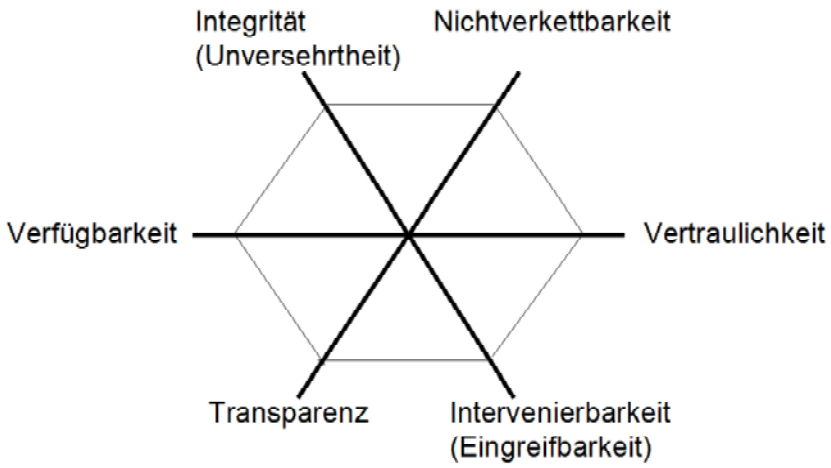

Abbildung 1: Systematik der Schutzziele: Die 3 Dualpaar-Achsen sich widersprechender und deshalb abzuwägender Schutzziele (in Anlehnung an [Boc11, 32]).

Das Schutzziel *Transparenz* bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wem die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung gehören. Der Eigentümer von Daten, Prozessen oder Systemen ist verantwortlich für die korrekte Datenverarbeitung. Durch Transparenz der gesamten Datenverarbeitung werden oftmals Regelungslücken deutlich. Transparenz ist auch für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung

bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese von Betroffenen eingewilligt werden kann. Umgesetzt wird dieses Schutzziel durch das weitgehend automatisierte Kontrollieren von Systemen durch Monitoring-Systeme, durch Protokollierung, durch Dokumentation der Daten, der Datenflüsse und der gesamten technischen und organisatorischen Systeme und Prozesse.

Das Schutzziel *Intervenierbarkeit* bezeichnet die Anforderung, dass sowohl Betroffene als auch Betreiber von Systemen jederzeit in der Lage sind, die Datenverarbeitung, vom Erheben bis zum Löschen von Daten, ändern zu können. Schon bei der Konstruktion einer Datenverarbeitung muss dafür gesorgt werden. Umgesetzt wird dieses Schutzziel, indem für Betroffene und Betreiber an Systemen Vorrichtungen installiert sind, mit denen Systeme verändert und gestoppt werden können.

Das Schutzziel *Nichtverkettbarkeit* bezeichnet die Anforderung, dass für Prozesse und Systeme sichergestellt ist, dass deren Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden. Zu bedenken ist, dass generell große Datenbestände Begehrlichkeiten mit ganz anderen Interessen an diesen Daten wecken können. Umgesetzt wird dieses Schutzziel bei personenbezogenen Daten durch Datensparsamkeit sowie von spezifischen, Datenschutz verbessernden Techniken, wie die Nutzung von Anonymisierungsserverketten, anonymen Credentials[9] oder Pseudonymen, wie sie von nutzergesteuerten Identitätenmanagement-Applikationen bereitgestellt werden. Es empfiehlt sich, System(teile) voneinander zu separieren, damit sich bspw. Fehler in einem System nicht in einem anderen System fortpflanzen (Funktion einer Brandmauer). Die Nichtverkettbarkeit ist der technische Ausdruck der Anforderung an Zweckbindung und Zwecktrennungen, die als Funktionstrennungen einen wesentlichen Mechanismus zur Umsetzung von Checks & Balances der Gewaltenteilung in einem modernen Rechtsstaat darstellen.

Die Datenschutzgesetze der Neuen Bundesländer, sowie die von Berlin, Hamburg und Nordrhein-Westfalen, enthalten die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, teilweise auch Transparenz. Das Landesdatenschutzgesetz von Schleswig-Holstein enthält seit Januar 2012 in §5 LDSG den vollständigen Satz der oben aufgeführten sechs elementaren Schutzziele. Auch das Bundesverfassungsgericht hat im Februar 2008 Bezug auf Schutzziele genommen, indem es das Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ formulierte.[10] Man kann insofern berechtigt sagen: Die Schutzziele sind im Recht angekommen.

Die einzelnen Schutzziele enthalten die wesentlichen Bestimmungen des Datenschutzrechts und weisen technischen und organisatorischen Schutzmaßnahmen dadurch einen systematisch fokussierten Ort zu. Darüber hinaus vermögen Schutzziele die für das Recht wesentliche Funktion des Abwägens von Anforderungen dadurch zu unterstützen, indem sie anzeigen, welche Schutzziele mit besonderer Aufmerksamkeit gegeneinander ab-

[9] Siehe das EU Forschungsprojekt *ABC4Trust* (Attribute-Based Credentials for Trust), indem entlang der hier vorgestellten Schutzzielesystematik entwickelt wird, https://abc4trust.eu/ .

[10] BVerfG, 1 BvR370/07 vom 27.02.2008. Dass die Schutzziele Vertraulichkeit und Integrität betont werden, schließt nicht die Berücksichtigung weiterer Schutzziele aus, beispielsweise wenn Anforderungen für möglicherweise notwendige Unschärfen oder weitergehende Datensparsamkeit (als Teil von Nichtverkettbarkeit) bestehen [Han12]. Zudem spielen Transparenz und Intervenierbarkeit bereits im Volkszählungsurteil von 1983, in dem das Recht auf informationelle Selbstbestimmung begründet wurde, eine entscheidende Rolle.

zuwägen sind. Dies ist die wesentliche These dieses Artikels, weil dieser Aspekt der rechtlichen Abwägungsfokussierung in der bisherigen Diskussion kaum beachtet wurde. So lassen sich drei Schutzziel-Paare herausheben, deren Beziehungen sowohl komplementär ergänzend als auch in den Wirkungen gegenläufig („dual“) sind:

- Verfügbarkeit – Vertraulichkeit
- Integrität – Intervenierbarkeit
- Transparenz – Nichtverkettbarkeit

Man kann rein logisch begründet von einem Verfahren nicht die Eigenschaft fordern, dass dessen Daten sowohl perfekt verfügbar im Sinne genereller semantischer Verwendbarkeit und zugleich perfekt vertraulich im Sinne von semantisch nicht verwendbar vorgehalten werden. Es muss für die praktische Anwendbarkeit eines Verfahrens zwischen den beiden Maximal-Anforderungen ein Kompromiss gefunden werden. Die rechtlich typischerweise daraufhin gefundene Lösung läuft darauf hinaus, dass seitens des Verfahrensverantwortlichen sicherzustellen ist, dass nur verfahrensseitig Befugte Zugriff auf ein Datum haben. Auch das Verhältnis von Integrität und Intervenierbarkeit ist ein Dual. Die Integrität eines Datums, Prozesses oder Systems soll einerseits kontrolliert korrekt und dauerhaft stabil gegen mögliche Störungen von Außen funktionieren, das Funktionieren muss andererseits aber auch durchbrochen werden können, weil das eine wesentliche Eigenschaft ist, um Daten und Systeme verwalten und ändern zu können. Und auch Transparenz und Nichtverkettbarkeit stehen dual zueinander: Ein Datum, das transparent ist, kann grundsätzlich mit anderen Daten verkettet werden. Erst eine Grenze verhindert, dass Daten miteinander verarbeitet werden, und sorgt insofern für Intransparenz auf der anderen Seite einer Grenze. Daher gilt es anhand dieser drei Achsen abzuwägen und dann zu entscheiden, in welchem Grad der Perfektion eine Anforderungen umzusetzen ist.[11]

Wenn eine datenschutzrechtliche Beurteilung orientiert an diesen drei Achsen erfolgt, kann auch die technische Umsetzung daraus anhand abgestimmter, standardisierter Maßnahmenkataloge für die einzelnen Schutzziele im richtigen Maße geschehen. Die Vollständigkeit der rechtlichen Beurteilung innerhalb des von diesen sechs Zielen aufgespannten Rahmens nimmt die Freiheitsgrade bei der konstruktiven Gestaltung der technischen und organisatorischen Maßnahmen weitgehend heraus. Vollständigkeit der Abwägungen ist eine Voraussetzung dafür, dass das Recht die Gestaltung eines Verfahrens und dessen Sicherheitsmaßnahmen tatsächlich dominieren kann. Dieses Vorgehen, die Schutzziele der Abwägbarkeit halber in eine gegenseitig bestimmbare Beziehung zu setzen, ist bislang in der Datensicherheit keine gängige Praxis.[12]

Im Sinne des Abstinenzmodell lässt sich nun folgendes behaupten: Der Juristin reicht eine grob bleibende Formulierung aus der Alltagsperspektive aus, mit welchen technischen

[11] Die Systematik der sechs elementaren Schutzziele untereinander entstand entlang dieser drei Achsen, nachdem in den ersten Entwürfen zur Systematisierung der Versuch einer eindimensionalen Anordnung gescheitert war. Aus den sechs elementaren Schutzzielen lassen sich außerdem acht weitere Schutzziele ableiten, wenn man die Unterscheidung von Nachrichteninhalt und Kontext von Inhalten unterscheidet und Selbstbezüge zulässt (wonach bspw. auch für Vertraulichkeit noch Vertraulichkeit zu sichern ist) [Pfi09].

[12] Zum Verhältnis von Datensicherheit und Datenschutz siehe [Ros12a, Ros13a].

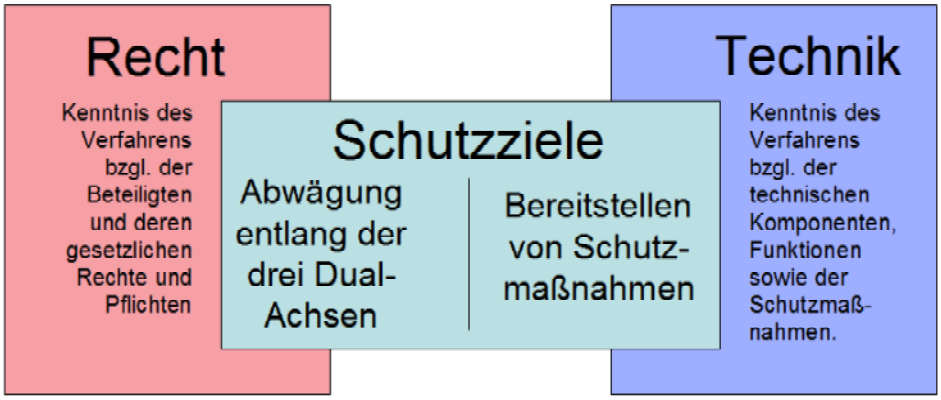

Abbildung 2: Die Vermittlung von Recht und Technik durch Referenz auf Schutzziele

und organisatorischen Maßnahmen diese Ziele umsetzbar sind oder umgesetzt werden. Dass bspw. Transparenz durch Dokumentation der Systeme und Protokollierung der Prozessabläufe umsetzbar ist, ist weitgehend allgemein verständlich. Dem Techniker reicht im Gegenzug eine grobe Alltagsvorstellung davon, welche normativen Anforderungen bestehen und wie sie gegeneinander abzuwägen sind.[13] Im Sinne des Konvergenzmodells lässt sich somit festhalten, dass soziologisch funktional allein schon der Umstand ist, dass diese Ziele für Organisationen offen erklärt sind, Aufmerksamkeit und Handlungen kanalisieren, die Ausdauer der Bearbeitung erhöhen und Strategien und Aktionspläne fördern [End04]. Insofern ist mit dieser Verbindung beider Modelle eine Synthese im Sinne des Divergenzmodells geglückt.

Die Schutzziele ermöglichen darüber hinaus auch die Einbeziehung der anderen Funktionssysteme der Gesellschaft, nämlich Wirtschaft, Wissenschaft und Politik.[14] Die von den Schutzzielen organisierten Schutzmaßnahmen lassen sich insofern betriebswirtschaftlich kalkulieren, nachdem die datenschutzrechtlichen Abwägungen getroffen und die technischen Zuordnungen der Funktionen, deren technische Gestaltung sowie über die Standard gemäß zu treffenden Schutzmaßnahmen entschieden wurde. Die wissenschaftliche Befassung mit den Schutzzielen verspricht darüber hinaus die theoretische Erfassung anderer Möglichkeiten sowie die Entwicklung von Methoden zur Entscheidungsfindung. Wissenschaftliche Forschung ist der Referenzrahmen, in dem sinnvollerweise Privacy-Impact-Assessments (PIA) durchgeführt werden, in denen, stellvertretend für die Gesellschaft, auch unwahrscheinliche Modellsimulationen überprüft werden können.

Eine gesellschaftlich beherrschbare Technik ist eine Voraussetzung dafür, dass Kommunikation und soziales Miteinander der Menschen gelingen kann. In diesen allgemeinen Rahmen eingespannt sind die Schutzziele nicht „nur“ Anforderungen, die sich aus dem Persönlichkeitsrecht ableiten lassen und vom Datenschutz betreut werden. Vielmehr

[13] In der Praxis sind beide zusammen aufgefordert, gemeinsam mit dem Verfahrensverantwortlichen die Prozesse und Datenflüsse eines Verfahrens zu klären.

[14] Das zeigt sich in Konzepten zu neuen Techniken, die bereits mit Orientierung an den sechs Datenschutz-Schutzzielen erarbeitet wurden: Ambient Assistet Living [VDE12, 56], Cloud Computing [AD12, 10f], Cyber-physical Systems [Thi12], Smart Meter [DüK12].

handelt es sich um verallgemeinerungsfähige, vernünftige Anforderungen bzgl. der Beherrschbarkeit, Fairness und Vertrauenswürdigkeit technischer Infrastrukturen moderner Gesellschaften überhaupt. Die Funktion der Schutzziele lässt sich insofern als notwendige Ergänzung der Geltungsforderungen an eine vernünftige Rede, die Jürgen Habermas in seiner Theorie des „kommunikativen Handelns“ [Hab85] entwickelte, auf der infrastrukturell-operativen Ebene begreifen.

Um es in Bezug auf die Funktion des Datenschutzes noch genauer zuzuspitzen: Der Geltungs- und Begründungszusammenhang der Schutzziele ist weder dem Recht noch der Technik als dominante Sphäre zu entnehmen. Vielmehr folgt(!) das Datenschutzrecht den Geltungsanforderungen der Schutzziele als etwas Drittem, deren Umsetzung eine gesellschaftliche Voraussetzung dafür ist, dass Gewaltenteilung, Demokratie, Markt und wissenschaftliche und ästhetisch freie Diskurse vorliegen und die „Geltungsanforderungen einer vernünftigen Rede“ einlösbar sind. Datenschutz thematisiert insofern anhand der Schutzziele – im Datenschutzrecht inkarniert als Zweckbindung, Beachtung der Betroffenenrechte und Transparenz –, die notorisch von Organisationen bedrohten Rollenkonzepte des Bürgers, Kunden, Subjekts und damit letztlich die Beschädigungen dieser Kontingenz steigernden Strukturen in modernen „funktional-differenzierter Gesellschaften“ (Luhmann) [Ros12a, 33f.].[15] In diesem Sinne lässt sich behaupten: Im Datenschutzrecht zeigte sich mit den normativen Instrumenten des Verbots mit Erlaubnisvorbehalt, den Geboten der Zweckbindung, Erforderlichkeit und Zweckbindung, Transparenz und Interventionen aus der Betroffenperspektive, eine frühe Ahnung bzgl. der Anforderungen, die an kritische gesellschaftliche Infrastrukturen für eine moderne Weltgesellschaft zu erfüllen sind.

4 Schutzziele anwenden

Die Systematik der elementaren Schutzziele bildet den wesentlichen Rahmen zur gegenseitigen Vermittlung von rechtlichen Anforderungen sowie technischen Funktionen und Schutzmaßnahmen. Wenn darüber hinaus zwei methodische Aspekte hinzu genommen werden, die sich im Bereich der Datensicherheit gemäß „IT-Grundschutz nach BSI“ bewährt haben, dann lassen sich differenzierte Abwägungen und skalierbare Funktionen und Datenschutz-Schutzmaßnahmen miteinander verbinden [BSI13]. Zum einen sind die Komponenten von Verfahren zu betrachten, zum anderen ist der Schutzbedarf eines Verfahrens festzulegen.

4.1 Verfahrenskomponenten: Daten, IT-System und Prozesse

Das Datenschutzrecht geht in Bezug auf technisch-organisatorische Schutzmaßnahmen typischerweise von einem „personenbezogenen Datum“ aus, das es zu schützen gilt. Auch

[15] Mit systemtheoretischer Orientierung drängt sich die Forschungsfrage auf zu prüfen, ob sich Schutzziele als eine Untergruppe „symbolisch generalisierter Kommunikationsmedien“ (Luhmann) ausweisen lassen, weil sich deren Konvergenzreproduktionen zumindest ähneln.

die Datensicherheit fokussiert zunächst den Schutzbedarf auf die Daten. Dann gilt die Regel, dass alle Verfahrenskomponenten, mit denen diese Daten verarbeitet werden – also die Hardware, die Programme und Prozesse – den Schutzbedarf der Daten erben. Diese Strategie zur methodischen Beschränkung auf die Analyse zunächst der Daten ist in vielen Fällen sinnvoll, insbesondere wenn bei Forschungs- und Entwicklungsprojekten der Privacy-Impact und die Verantwortlichkeiten in den verschiedenen Rollen einer Neuentwicklung nur schlecht abzuschätzen sind. Dann empfiehlt es sich, sich zunächst wie gehabt auf die unterschiedlichen Schutzbedarfe der anfallenden Daten zu konzentrieren, diese Bedarfe an die System und Prozesse zu vererben und über die Schutzziele die entsprechenden Schutzmaßnahmen auszuwählen, die die verschiedenen Beteiligten (Betroffener, Hersteller, Dienstleister aber eventl. auch Versicherungen, Rechenzentren, Cloudanbieter, Internetprovider, Sicherheitsbehörden usw.) umzusetzen haben [Ros11].

Für Planungen und Prüfungen von Verfahren macht es aus Datenschutzsicht Sinn, über klare Soll-Vorgaben für sämtliche Komponenten eines Verfahrens zu verfügen, auf die die Schutzziele dann zu beziehen sind. Deshalb werden die folgenden Komponenten eines Verfahrens unterschieden:

- Daten und Datenstrukturen (Formate)
- IT-Systeme und Schnittstellen
- Prozesse und Rollen (Adressen)

4.2 Schutzbedarfe – aus der Betroffenenperspektive!

Mit dem bereits angesprochenen Konzept des Schutzbedarfs wird es möglich, eine Skalierbarkeit im Sinne eines „Mehr oder weniger“ der zu treffenden Maßnahmen zu erreichen. In der Praxis der Umsetzung des IT-Grundschutzes hat sich für die Festsetzungen des Schutzbedarfs die Dreiertypologie „normal“, „hoch“ und „sehr hoch“ bewährt. Verfahren mit Personenbezug müssen grundsätzlich sicher gestaltet sein, weil es durch die bloße Existenz, also auch bei rechtlicher Ordnungsmäßigkeit und nicht erst im Schadensfalle, bereits ein Risiko für einen Betroffenen darstellt.

Die Definition der Schutzbedarfe bzw. deren Differenzierung untereinander kann, wegen der unterschiedlichen Angreifermodelle von Datensicherheit und Datenschutz, nicht vom methodischen Vorbild des „IT-Grundschutzes“ übernommen werden. Aus Datenschutzsicht muss die Definition aus der Perspektive des Betroffenen erfolgen:

- Die Schutzbedarfskategorie *normal* ist grundsätzlich als Grundbedarf festzulegen. Zusätzlich mögliche Schadensauswirkungen sind darüber hinaus begrenzt und überschaubar und etwaig eingetretene Schäden für den Betroffenen relativ leicht zu heilen.
- Die Schutzbedarfskategorie *hoch* ist dann zu wählen, wenn die Schadensauswirkungen von einer Person als beträchtlich eingeschätzt werden, z.B. weil bei Wegfall

einer von einer Organisation zugesagten Leistung – wie das Zurverfügungstellen von Strom oder Kommunikationsdiensten, die materielle Voraussetzungen sind, um in einer modernen Gesellschaft informationelle Selbstbestimmung ausüben zu können –, die Gestaltung des Alltags nachhaltig veränderte und der Betroffene auf zusätzliche Hilfe angewiesen wäre.

- Die Schutzbedarfskategorie *sehr hoch* bleibt solchen Fällen vorbehalten, in denen Schadensauswirkungen ein existentiell bedrohliches, katastrophales Ausmaß erreichen können.

Es ist der Schutzbedarf, mit dem dann bspw. die angemessene Qualität des Löschens bestimmt wird. Ab hohem Schutzbedarf muss der seinerseits gesicherte Nachweis darüber geführt werden können, dass zum Löschen bspw. eines Magnetspeichers zumindest ein mehrfaches Überschreiben durchgeführt wurde.

4.3 Das Standard-Datenschutzmodell anwenden

Die juristische Expertise erfasst die rechtlich relevanten Eigenschaften eines Verfahrens sowie die Verantwortlichkeiten und Zuständigkeiten der Verfahrensbeteiligten. Es werden die gesetzlich gültigen bzw. die vertraglichen Regelungen, in Form von „Codes of Conduct“ oder Dienst- und Betriebsvereinbarungen oder von Vertragswerken zur Auftragsdatenverarbeitung, zusammengestellt. Außerdem sind die Organisationsstruktur mit Rollen und Verantwortlichkeiten sowie die Schnittstelle zur Fachlichkeit eines Verfahrens mit der Abklärung der einzelnen Daten bzw. Datenfelder einer zur Verarbeitung genutzten Applikation zu erheben. Die Abschätzung des Verfahrenszwecks und der Erforderlichkeit, sowie Thesen bzgl. der Möglichkeiten, Datensparsamkeit walten zu lassen und den frühest möglichen Löschtermin ausfindig zu machen oder zur Notwendigkeit einer Vollidentifikation einer Person, all das muss auch fachlich begründet werden und ergibt sich nicht zwingend allein aus juristischer oder technischer Perspektive. Nach der Klärung der rechtlich relevanten Eigenschaften lassen sich die Abwägungen und Entscheidungen in das Medium der Schutzziele übersetzen, sofern die Abwägungen nicht bereits innerhalb der Schutzziele geschehen ist.

Die technische Expertise erfasst Verfahrenseigenschaften jeweils für die drei Verfahrenskomponenten. Diese Eigenschaften werden zusammengestellt und typisiert und zu Maßnahmenbündeln aggregiert, die der Sicherstellung der Datensicherheit und des Datenschutzes dienen. Dabei wird auch die durch die vorgefundenen Maßnahmen erzielte Intensität der Schutzwirkungen festgestellt.

Die Erfassung des Ist-Zustands eines Verfahrens sowie der festgestellten Datenschutz-Schutzmaßnahmen und deren Schutzbedarfsdeckung lassen sich dann mit den aus der Schutzziele-Modellierung abgeleiteten Soll-Schutzmaßnahmen in Beziehung setzen. In der Praxis sind vielfach andere Schutzmaßnahmen anzutreffen als sie das Referenzmodell vorgibt. Neben dem Nachweis der funktionalen Äquivalenz dieser Maßnahmen ist auch damit zu rechnen, dass eine Maßnahme mit geringerer Schutzbedarfsdeckung durch

andere Maßnahmen kompensiert wird.

Insgesamt wird durch dieses Modell eine Bilanzierung von Soll und Haben ermöglicht, die eine transparente Begründung des Urteils erlaubt, ob ein Verfahren mit seinen Verfahrenskomponenten datenschutzgerecht eingerichtet und mit den angemessenen Schutzmaßnahmen betrieben wird. Darüber hinaus können, aufgrund der Modellierung der Soll-Maßnahmen, bei festgestellten Mängeln vielfach konkrete Vorschläge zur Mängelbehebung gemacht werden.[16]

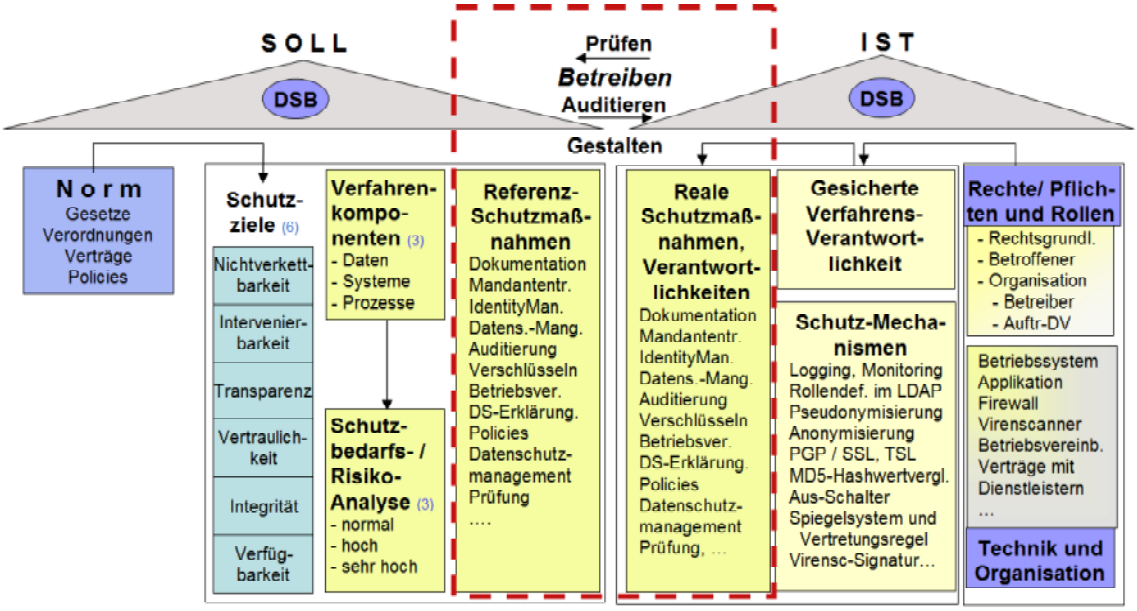

Abbildung 3: Das Standard-Datenschutzmodell (in Anlehnung an [Ros12b]).

5 Fazit

Es sind drei Eigenschaften, die die (Systematik der) Schutzziele als Mittler zwischen den Sphären Technik und Datenschutzrecht im Sinne des Divergenzmodells geeignet machen: Schutzziele entsprechen den wesentlichen normativen Anforderungen des Datenschutzrechts, sie fokussieren deren rechtlichen Abwägungen auf drei Hauptachsen und sie organisieren die technischen und organisatorischen Schutzmaßnahmen des Datenschutzes und der Datensicherheit. Schutzziele können diese Vermittlung von Technik und Recht deshalb leisten, weil sie dazu eine dritte Bezugsgröße im Sinne universeller gesellschaftlicher Geltungsanforderungen bilden.

[16] Erste Schritte zur Umsetzung dieses Modells wurden inzwischen vollzogen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben auf der Sitzung am 13./14.3.2013 in Bremerhaven den Ausbau der ersten vorgelegten Entwürfe des Standard-Datenschutzmodells [Ros12b] beauftragt.

Literatur

[AD12] Artikel-29-Datenschutzgruppe. Opinion on Cloud Computing – 03/12/EN WP 196, 06 2012.

[Ale08] Robert Alexy. *Theorie der juristischen Argumentation. Die Theorie des rationalen Diskurses als Theorie der juristischen Begründung*. Suhrkamp, Frankfurt am Main, 3. Auflage, 2008.

[Boc11] Martin Rost; Kirsten Bock. Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen. *DuD – Datenschutz und Datensicherheit*, 35(1):30–35, 2011.

[BSI13] BSI. IT-Grundschutz – Übersicht, 2013.

[DüK12] DSBK & DüKreis. Orientierungshilfe datenschutzgerechtes Smart Metering – Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis, 2012.

[End04] Günter Endruweit. *Organisationssoziologie*. UTB, Stuttgart, 2. Auflage, 2004.

[Fed11] Hannes Federrath. Digitaler Radiergummi und seine Folgen, 2011.

[gD12] Indra Spiecker gen. Döhmann. Die Durchsetzung datenschutzrechtlicher Mindestanforderungen bei Facebook und anderen sozialen Netzwerken. *Kommunikation & Recht*, 11:717, 11 2012.

[Gus89] Christoph Gusy. Techniksteuerung durch Recht – Aufgaben und Grenzen. In Hartwig Donner; Georgios Magoulas; Jürgen Simon; Rainer Wolf, Hrsg., *Umweltschutz zwischen Markt und Recht*, Schriftenreihe Recht, Ökonomie und Umwelt, Seiten 241–268. Nomos, Baden-Baden, 1. Auflage, 1989.

[Hab85] Jürgen Habermas. *Theorie des kommunikativen Handelns*, Jgg. 1. Suhrkamp, Frankfurt am Main, 1. Auflage, 1985.

[Hal11] Jost Halfmann. Technikrecht aus der Sicht der Soziologie. In *Handbuch des Technikrechts*, Seiten 93–107. Martin Schulte; Rainer Schröder, 2011.

[Han12] Marit Hansen. Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter. *DuD – Datenschutz und Datensicherheit*, 36(6):407–412, 2012.

[Hof13] Gerrit Hornung; Kai Hofmann. Ein „Recht auf Vergessenwerden?“ Anspruch und Wirklichkeit eines neuen Datenschutzrechts. *JZ – Juristenzeitung*, 68(4):193–171, 2013.

[Hug88] Renate Mayntz; Thomas P. Huges. The Development of Large Technical Systems. In Renate Mayntz; Thomas P. Hughes, Hrsg., *The Development of Large Technical Systems*. Campus, Frankfurt am Main, 1. Auflage, 1988.

[Kem89] Eggert Holling; Peter Kempin. *Identität, Geist und Maschine. Auf dem Weg in die technologische Zivilisation*. Rowohlt, 1. Auflage, 1989.

[Lüd09] Jörn Lüdemann. Rechtsetzung und Interdisziplinarität in der Verwaltungsrechtswissenschaft. *Preprints of the Max Planck Institute for Research on Collective Goods*, (30), 2009.

[Les01] Lawrence Lessig. *Code und andere Gesetze des Cyberspace*. Berlin Verlag, Berlin, 1. Auflage, 2001.

[Luh93] Niklas Luhmann. *Das Recht der Gesellschaft*. Suhrkamp, Frankfurt am Main, 1. Auflage, 1993.

[Luh97] Niklas Luhmann. *Die Gesellschaft der Gesellschaft*. Suhrkamp, Frankfurt am Main, 1. Auflage, 1997.

[Mei12] Kirsten Bock; Sebastian Meissner. Datenschutz-Schutzziele im Recht – Zum normativen Gehalt der Datenschutz-Schutzziele. *DuD – Datenschutz und Datensicherheit*, 36(6):425–431, 2012.

[Pfi00] Hannes Federrath; Andreas Pfitzmann. Gliederung und Systematisierung von Schutzzielen in IT-Systemen. *DuD – Datenschutz und Datensicherheit*, 24(12):704–710, 2000.

[Pfi09] Martin Rost; Andreas Pfitzmann. Datenschutz-Schutzziele – revisited. *DuD – Datenschutz und Datensicherheit*, 33(6):353–358, 2009.

[Pro12] Thomas Probst. Generische Schutzmaßnahmen für Datenschutz-Schutzziele. *DuD – Datenschutz und Datensicherheit*, 36(6):439–444, 2012.

[Ros97] Martin Rost. Anmerkungen zu einer Soziologie des Internet. In Lorenz Gräf; Markus Krajewski, Hrsg., *Soziologie des Internet. Handeln im elektronischen Web-Werk*, Seiten 14–38. Frankfurt am Main: Campus, 1. Auflage, 1997.

[Ros11] Martin Rost. Datenschutz in 3D – Daten, Prozesse und Schutzziele in einem Modell. *DuD – Datenschutz und Datensicherheit*, 35(5):351–355, 2011.

[Ros12a] Martin Rost. Faire, beherrschbare und sichere Verfahren. In Heinrich Kersten;Falk Peters; Klaus-Dieter Wolfenstetter, Hrsg., *Innovativer Datenschutz*, Seiten 17–37. Duncker & Humblot, 1. Auflage, 2012.

[Ros12b] Martin Rost. Standardisierte Datenschutzmodellierung. *DuD – Datenschutz und Datensicherheit*, 36(6):433–438, 2012.

[Ros13a] Martin Rost. Eine kurze Geschichte des Prüfens. In BSI, Hrsg., *Informationssicherheit stärken – Vertrauen in die Zukunft schaffen*, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, Seiten 25–35. Secumedia-Verlag, Gau Algesheim, 1. Auflage, 2013.

[Ros13b] Martin Rost. Zur Soziologie des Datenschutzes. *DuD – Datenschutz und Datensicherheit*, 37(2):85–91, 2013.

[Sch11] Martin Schulte; Rainer Schröder, Hrsg. *Handbuch des Technikrechts*. Springer, 3. Auflage, 2011. Allgemeine Grundlagen, Umweltrecht – Gentechnikrecht – Energierecht Telekommunikations- und Medienrecht, Patentrect – Computererecht.

[Ste93] Wilhelm Steinmüller. *Informationstechnologie und Gesellschaft – Einführung in die Angewandte Informatik*. Wissenschaftliche Buchgesellschaft, Darmstadt, 1. Auflage, 1993.

[Thi12] Marit Hansen; Christian Thiel. Cyber-Physical Systems und Privatsphärenschutz. *DuD – Datenschutz und Datensicherheit*, 1:26–30, 2012.

[VDE12] VDE. *Die deutsche Normungsroadmap AAL*. VDE, 2012.

[Wac13] Silke Jandt; Olga Kieselmann; Arno Wacker. Recht auf Vergessen im Internet. *Datenschutz und Datensicherheit – DuD*, 4:235–241, 2013.

[Wil99] Hellmut Willke. *Systemtheorie II: Interventionstheorie. Einführung in die Theorie der Intervention in komplexe Sozialsysteme*. Fischer UTB, Stuttgart, 3. Auflage, 1999.

GI-Edition

Lecture Notes in Informatics

Matthias Horbach (Hrsg.)

INFORMATIK 2013

Informatik angepasst an Mensch, Organisation und Umwelt

16.–20. September 2013
Koblenz

Matthias Horbach (Hrsg.): INFORMATIK 2013

220

Proceedings

Matthias Horbach (Hrsg.)

INFORMATIK 2013

Informatik angepasst an Mensch, Organisation und Umwelt

16.–20. September 2013
Koblenz, Germany

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-220

ISBN 978-3-88579-614-5
ISSN 1617-5468

Volume Editors
Dr. Matthias Horbach
Formale Methoden und Theoretische Informatik
FB4 Informatik, Universität Koblenz-Landau
56070 Koblenz, Germany
Email: horbach@uni–koblenz.de

printed by Köllen Druck+Verlag GmbH, Bonn