Martin Rost, Andreas Pfitzmann

Datenschutz-Schutzziele – revisited

Die Arbeit mit Schutzzielen hat sich grundsätzlich bewährt. Sie sind so formuliert, dass sie die Anforderungen an technische und organisatorische Systeme sowohl abstrakt überblickbar als auch in Form von Maßnahmen hinreichend konkret faßbar machen. Der Beitrag empfiehlt, sie in Datenschutzgesetze und Verträge aufzunehmen, als Leitlinien für den Entwurf und Betrieb von IT-Infrastrukturen heranzuziehen und in Mechanismen transformiert als WebService-Policies auszudrücken – und unterbreitet einen Strukturierungsvorschlag.

1 Schutzziele integrieren

Schutzziele bieten Systemdesignern Maßstäbe zur Entwicklung technischer und organisatorischer Infrastrukturen. Schutzziele bieten sich als Bestandteile von Gesetzen und Verträgen an und sind dadurch für Compliance-Prüfungen relevant. Über Kosten-Nutzen-Analysen für entsprechend getroffene Maßnahmen lässt sich zudem deren Wirtschaftlichkeit beurteilen. Und Schutzziele werden absehbar in den Policies der WebServices ihren Niederschlag finden.[1] Schutzziele entfalten somit eine integrative Funktion für die verschiedenen Anforderungen an Wirtschaftlichkeitsberechenbarkeit [8], Rechtskonformitätsprüfbarkeit, Technik- und Organisationsfunktionalität, ohne dass die „Eigenlogik" eines dieser Bereiche die Eigenlogiken anderer Bereiche dominiert.[2]

Prof. Dr. Andreas Pfitzmann

Lehrstuhl Datenschutz und Datensicherheit, Institut für Systemarchitektur, Fakultät Informatik, TU Dresden
E-Mail: pfitza@inf.tu-dresden.de

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz" beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.
E-Mail:
martin.rost@datenschutzzentrum.de

1 Vgl. den Beitrag von Rost/Speck in diesem Heft sowie [17].

2 Zur Struktur von Schutzzielen

Dieser Beitrag unterbreitet einen Systematisierungsvorschlag, um eine Struktur in den Raum der Schutzziele zu bringen, die eine Untersuchung der Wechselwirkungen von Schutzzielen, von deren Vollständigkeit wie auch von Erzeugendensystemen erlaubt.[3] Diese Themen fehlen den bisherigen Beschreibungen von Schutzzielen, die sich über die Zeit zu immer unübersichtlichere Sammlungen auswuchsen (vgl. [2, 3, 4, 14, 24]).[4]

Die „elementaren" Schutzziele sollen wie folgt definiert sein:

- *Verfügbarkeit*: Gesicherter Zugriff auf Information innerhalb einer festgelegten Zeit.
- *Vertraulichkeit*: Gesicherter Nichtzugriff auf Information (ggf. beschränkt auf eine festgelegte Zeit).
- *Integrität*: Information ist (ggf. beschränkt auf eine festgelegte Zeit) gesichert echt.

Verfügbarkeit und Vertraulichkeit stehen hiernach, in Bezug auf Informationen, dual zueinander: Zugreifbarkeit und zugleich Nichtzugreifbarkeit auf Informationen bezeichnet einen Widerspruch. Das bedeutet, dass es durchaus auf ein konzeptionelles Problem hinauslaufen kann, diese beiden Schutzziele unproblematisiert als gemeinsam anzustreben auszuweisen. Aus diesem inhärenten Zusammenhang stellt sich die Frage, ob nicht auch zu Integrität ein Dual formulierbar ist. Diesen systematisch gewonnenen Dual wollen wir mit „Kontingenz" bezeichnen:

- *Kontingenz*: Information ist (ggf. beschränkt auf eine festgelegte Zeit) gesichert nicht gesichert echt.

Zunächst zum Konzept der Dualität, das sich wie folgt verstehen lässt: Zwei Entitäten können sowohl in einem widersprüchlichen als auch in einem ergänzenden Bezug zueinander stehen. Wenn der Bezug beider Entitäten auf eine gemeinsame Referenz geschieht, führt dies zu einem Widerspruch. In Bezug auf unterschiedliche Referenzen kann das Verhältnis der Entitäten untereinander dagegen eine Ergänzung sein. Beispiel: In einem Datenverarbeitungssystem sollen die Prozesse verfügbar, die damit verarbeiteten Daten dagegen vertraulich sein.

Nun zu Kontingenz. Kontingenz soll als ein Schutzziel gegen Einengungen durch

2 Dies ist eine wesentliche Eigenschaft funktional differenzierter Systeme (vgl. [15]).

3 Bisherige systematische Untersuchungen vgl. [5], [23].

4 Das vorliegende, in diesem Beitrag angerissene, Konzept verdankt viele Ideen den Diskussionen mit Kirsten Bock, Rainer Böhme, Katrin Borcea-Pfitzmann, Elke Franz, Marit Hansen, Benjamin Kellermann, Stefan Köpsell, Immanuel Scholz, Sandra Steinbrecher und Sven Thomsen sowie dem UAK „Technische BDSG-Novelle" unter Leitung von Walter Ernestus.

Tabelle 1 | Entsprechungen von Inhalts- und Umfeldschutzzielen

Inhalte	Umfeld
Verdecktheit	Unentdeckbarkeit Unbeobachtbarkeit
Vertraulichkeit	Anonymität
Kontingenz	Abstreitbarkeit
Integrität	Zurechenbarkeit
Verfügbarkeit	Verbindlichkeit Erreichbarkeit
Findbarkeit	Ermittelbarkeit

Technik fungieren.[5] Was bedeutet das? Trotz des Einsatzes von Technik sollen Inhalte und Umstände, beispielsweise einer technisch vermittelten Kommunikation, offen in der Schwebe gehalten werden können und nicht inhaltlich sinn-verengend, ohne Freiheitsgrade für Interventionen, technisch bereits vorentschieden sein. Während die Sicherung der Integrität von Daten und Umständen darauf hinausläuft zu bestätigen, dass „etwas so ist, wie es ist", erlaubt das Schutzziel Kontingenz die Feststellung, dass „etwas anders sein könnte, als es scheint". Technik soll dem Menschen (oder einer Organisation) grundsätzlich so dienlich sein können, wie der Mensch (oder eine Organisation), der Technik nutzt, bestimmt. Menschen (oder Organisationen) sollen ggf. in die Lage versetzt sein, aussichtsreich abstreiten zu können, selbst wenn etwas von respektabler Seite unterstellt wird oder das Ergebnis einer automatisierten – und genau deshalb nicht zweifelsfreien! – Überprüfung gegen sie sprechen mag.

Unter diesem Schutzziel sollen Maßnahmen entwickelt und an die Hand geben werden, um Technik trotz ihres intensiven Einsatzes so auf Distanz halten zu können, dass Technik grundsätzlich unter Bedingungen gestellt werden kann.[6] Technik soll nicht das Recht auf informationelle Selbstbestimmung unter der Hand automatisch beschneiden beim Versuch, dieses Recht auf organisatorischer Seite durch zunehmend perfekt integre Techniksysteme durchzusetzen.

Aus dieser inhärenten Widersprüchlichkeit zweier Schutzziele, die bislang typischerweise unproblematisiert nebeneinander bestehend aufgeführt werden, sowie der Konstruktion eines neuen Schutzziels lassen sich weitere bekannte Schutzziele ableiten. Wenn man Verfügbarkeit selbstbezüglich auf sich selber bezieht, also nach der Verfügbarkeit der Verfügbarkeit fragt, so läßt sich diese als „Findbarkeit" bezeichnen. Und auf der anderen Seite bezeichnet die Vertraulichkeit der Vertraulichkeit „Verdecktheit" oder „Unentdeckbarkeit":

- *Findbarkeit*: Gesicherter Zugriff innerhalb einer festgelegten Zeit selbst auf vertraulichen Nachrichteninhalt.
- *Verdecktheit/Unentdeckbarkeit*: Gesicherter Nichtzugriff (ggf. beschränkt auf eine festgelegte Zeit) auf die Information, ob vertraulicher Nachrichteninhalt überhaupt existent ist.

Findbarkeit muss, sozusagen als verwaltete Verfügbarmachung, konstruktiv hergestellt werden. Technisch bedarf es zur Umsetzung dieses Schutzziels eines standardisierten Namespaces, also Bezeichner bzw. Adressen, die zu erhalten technisch trivial, organisatorisch aber höchst aufwändig und kostenintensiv ist.

Das Schutzziel Verdecktheit spielt beispielsweise eine Rolle, wenn nicht nur die Inhalte nicht bekannt werden sollen, sondern auch der Umstand, dass vertrauliche Kommunikation stattfand. Kommunikationstechnisch könnte dieses Schutzziel mit den Mitteln der „Steganographie" umgesetzt werden.

Die bislang genannten vier elementaren und zwei abgeleiteten Schutzziele sind auf den Schutz von Inhalten bezogen. Die nachfolgenden Schutzziele betreffen dagegen das Umfeld einer Information. Diese lassen sich aus den elementaren Schutzzielen entwickeln:

- *Verbindlichkeit/Erreichbarkeit*: Verfügbarkeit der Kommunikationsumstände.
- *Anonymität*: Vertraulichkeit der Identität einer Entität.
- *Zurechenbarkeit*: Integrität der Kommunikationsumstände, d. h. Verpflichtungen einer Entität sind überprüfbar.

Das zu Kontingenz korrespondierende Schutzziel lässt sich als „Abstreitbarkeit" bezeichnen:

- *Abstreitbarkeit*: Kontingenz der Kommunikationsumstände, d. h. Verpflichtungen einer Entität sind abstreitbar.

Zuletzt fehlen dann noch die Entsprechungen für die Inhalte-Schutzziele Findbarkeit und Verdecktheit in Bezug auf Umfeld-Schutzziele, nämlich „Ermittelbarkeit" und „Unbeobachtbarkeit":

- *Ermittelbarkeit*: Verfügbarkeit einer Entität, d. h. gesicherter Zugriff auf Entität innerhalb einer festgelegten Zeit.
- *Unbeobachtbarkeit*: Unentdeckbarkeit für alle an der Kommunikation Unbeteiligten (alle außer Sender und Empfänger) und Anonymität gegenüber an der Kommunikation Beteiligten (beides gegebenenfalls beschränkt auf eine festgelegte Zeit).

Auf diese Weise entsteht ein Schutzzielekatalog, der aus *vier Elementarschutzzielen* heraus methodisch entwickelbar ist (vgl. Tab. 1).

3 Datenschutz-Schutzziele

Der Umstand, dass sich die drei oftmals genannten speziellen Datenschutz-Schutzziele Transparenz, Revisionsfähigkeit und Authentizität [1] nicht aus den drei konventionellen elementaren Datensicherheits-Schutzzielen ableiten lassen, und dass die drei konventionellen Datenschutz-Schutzziele zudem nicht trennscharf zueinander sind, zugleich aber wiederum ein Bezug zu den klassischen Datensicherheits-Schutzzielen gegeben sein muss, allein weil Datensicherheit für Datenschutz eine Voraussetzung ist, ermutigt zu einem weiteren Schritt der Systemati-

5 Es adressiert beispielsweise den Konflikt, ob eine Maschine einen Menschen oder ein Mensch (Pilot) die Maschine (vollautomatisiertes Passagierflugzeug) toppen können soll. Die aktuellen Lösungen halten diesen klassischen Kontrollkonflikt neuerdings unentschieden offen, eben: kontingent.

6 Ein Beispiel hierfür ist die Antwort auf die an eine Frau während eines Bewerbungsgespräches gerichtete Frage: „Sind Sie schwanger?" Hier hat die Frau nicht nur das Recht, eine Antwort zu verweigern, sie hat auch das Recht zu lügen, da sie beim Verweigern einer Antwort vermutlich die gleichen Konsequenzen träfen wie bei einem „ja". In einer zunehmend technisierten Welt müsste die Technisierung auch die falsche Antwort glaubhaft unterstützen, was beispielsweise eine bei der Entwicklung der Gesundheitskarte nicht bedachte Eigenschaft sein dürfte – weil das entsprechende Schutzziel, Kontingenz, nicht bedacht wurde.

sierung, nämlich die Datenschutz-Schutzziele als dritte Dimension den bisherigen Überlegungen hinzuzufügen. Dafür müssen zuvor die bisherigen Datenschutz-Schutzziele kondensiert werden.

Revisionsfähigkeit lässt sich problemlos unter Transparenz subsumieren und *Authentizität* als Integritätsaspekt einer Entität neu formulieren. So bleibt Transparenz übrig. Aber Transparenz allein ist materiell-inhaltlich in datenschützerischer Absicht unzureichend. Zudem gilt die methodische Vorgabe, ein Dual zur Transparenz auszuweisen. Beide Anforderungen sollen durch das Datenschutz-Schutzziel der „Unverkettbarkeit" erfüllt werden.

Transparenz und Unverkettbarkeit bezeichnen Datenschutz-Schutzziele, mit denen Maßnahmen auf dem „Stand der Technik" verbunden sind. Diese Schutzziele sollen aber nicht nur einen inhaltlich bestimmten Zweck beziehungsweise die inhaltlich begründete Erforderlichkeit einer Datenverarbeitung und Kommunikation datensparsam aufnehmen können, sondern ihrerseits strukturierenden Einfluss auf diese Formulierungen nehmen. Transparenz ermöglicht die Prüffähigkeit von Verkettbarkeiten und Verkettungen im Hinblick auf deren Beherrschbarkeit und Gesetzeskonformität.[7]

3.1 Schutzziel Transparenz

- *Transparenz*: Transparenz eines Systemteils S bezeichnet seine Durchsichtigkeit für Entität E im Sinne einer Blickdurchlässigkeit für E mit dem Zweck, S für E beobachtbar beziehungsweise erkennbar zu machen.

Transparenz ist die wichtigste Voraussetzung für Beobachtbarkeit, Kontrollierbarkeit und Prüfbarkeit von Systemen. Kontrolle bedeutet, einen Soll-Wert mit einem Ist-Wert zu vergleichen.[8] Eine Beobachtung verfügt nicht zwingend über einen Soll-Wert, vielmehr kann auch etwas Unvermutetes entdeckt werden. Eine Prüfung bewertet Kontrollergebnisse und erzeugt so die für Organisationen essentielle Entscheidungsfähigkeit.[9] Transparent ist ein Medium dann, wenn es eine Form ausgebildet hat, in der sich, außer an den Rändern, keine Form erkennen lässt. Transparenz ist skalierbar, bis hin zur „intransparenten Opazität". Man denke als Beispiel an den Vorhang eines Fensters: Transparenz kann in diesem Sinne dann eine perfekte, kontroll-neutrale[10] Durchsichtigkeit bezeichnen. Opazität bleibt dagegen als Bezeichnung der Skalierbarkeit von Undurchsichtigkeit vorbehalten. Man kann hierbei wiederum unterscheiden, ob die Undurchsichtigkeit als solche transparent ist, also ob man beispielsweise erkennen kann, dass ein Vorhang vorgezogen wurde; oder ob die Undurchsichtigkeit als solche ebenfalls noch undurchsichtig und etwas dadurch unbeobachtbar ist.

- *Intransparenz*: Intransparenz bezeichnet opake Transparenz.
- *Beobachtungsunmöglichkeit*: Beobachtungsunmöglichkeit bezeichnet intransparente Opazität.

Diese Unterscheidung zu treffen ist relevant in Bezug auf den Zweck, den Funktionstrennungen erfüllen. Transparenz ist eine Eigenschaft, die sowohl den konstruktiven Aspekt der beobachtenden Entität als auch den konstruktiven Aspekt der beobachteten Entität anspricht. Transparenz ist nur herstellbar, wenn die beteiligten, funktional separierten Seiten konstruktiv bereit sind oder durch eine übergeordnete Instanz darauf verpflichtet werden, sich beobachtbar bzw. überprüfbar zu entwerfen.

Auf Maßnahmen zur Durchsetzung von Funktionstrennungen zielt Unverkettbarkeit als zweites spezifisches Datenschutz-Schutzziel.

3.2 Schutzziel Unverkettbarkeit

- *Unverkettbarkeit (von Daten und Entitäten)*: „Die Unmöglichkeit der Verkettung von Daten und Entitäten untereinander und miteinander." (vgl. [12], erweitert um Entitäten)

Über den Begriff der (Un-)Verkettbarkeit müssen materielle Datenschutzanforderungen formuliert werden können.[11] Dies gelingt dann, wenn man die Aktivitäten des Datenschutzes so begreift, dass dieser (politisch, rechtlich, organisatorisch, technisch) darauf hinwirkt, dass Kommunikationen und Datenverarbeitungen[12] im Verhältnis von Organisationen und deren Mandanten unter Bedingungen gestellt werden. In diesem Sinne darf es aus Datenschutzsicht keine gesellschaftlich relevante Kommunikation in Bezug auf Organisationen (staatliche Verwaltungen, Unternehmen, wissenschaftlich orientierte Dienstleistungen durch „Praxen") und deren Datenverarbeitung geben[13], für die kein rechtlicher und operativer Zugriff besteht.[14] Die zwischen Organisationen und externen Mandanten (und internen Arbeitnehmern) entstehenden Ereignisse dürfen nicht einseitig „ausbeutbare", also: unfair einstreichbare Gewinne gegenüber Betroffenen erzeugen, insbesondere nicht durch Intransparenz der Datenverarbeitung mit Personenbezug. Damit gesetzliche Regelungen und Einwilligungen bei Datenverarbeitungen und Kommunikationen für Bürger, Kunden und Patienten fair gestaltet werden können, muss der Zweck im Sinne einer unverrückbaren Objekteigenschaft einer Informationsverarbeitung oder Kommunikation, objektiv vorgegeben sein.[15]

7 Folgerichtig agieren Datenschutzbeauftragte auch als Beauftragte für Informationsfreiheit.

8 Und ebenfalls folgerichtig wäre die Entwicklung von KPIs für die Steuerung von Datenschutzmanagement-Prozessen.

9 Beobachtung bezeichnet die Einheit von Unterscheidung und Bezeichnung (vgl. [15]). Inwieweit „Realität" mental oder kommunikativ angemessen rekonstruiert wird und mit welchen „Transformationsverlusten", die zu behaupten wieder einen eigensinnigen Beobachter voraussetzt, dabei zu rechnen ist, kann hier nicht Gegenstand der Ausführungen sein. Zwischen allgemeiner Beobachtung und spezifischer Kontrolle ließe sich „noch unbewertete" Erkenntnis ansiedeln. Daran zeigt sich, wie weit man hier eigentlich theoretisch ausholen müsste: „Alles Beobachtbare ist Eigenleistung des Beobachters, eingeschlossen das Beobachten von Beobachtern. Also gibt es in der Umwelt nichts, was der Erkenntnis entspricht; denn alles, was der Erkenntnis entspricht, ist abhängig von Unterscheidungen, innerhalb derer sie etwas als dies und nicht das bezeichnet." ([16], S. 15 f.)

10 Perfekte Beobachtungsneutralität kann dagegen kein Medium bieten: Ein perfekt durchsichtiges Fenster hält bspw. Wind, Gerüche, leise Geräusche oder auch Gelegenheitsdiebe außen vor.

11 Verkettbarkeit gilt schon länger als Kandidat eines zentralen Begriffs innerhalb einer noch immer ungeschriebenen Theorie des Datenschutzes (vgl. zur Theorie [9], vgl. zur Verkettbarkeit [20]).

12 Datenverarbeitung bezieht sich auf Daten, die als Informationen gelten, die kommunizierbare Beobachtungen einer Organisation in Bezug auf deren Umwelt „aktualisieren".

13 Verkettungen in Form von Scorings und Profilen, die der Katalogisierung einer Persönlichkeit entsprechen, verletzen nach Auffassung des BVerfG (65, 1, 42, 53) die Menschenwürde.

14 Als Abfallprodukt werden dann auch wirtschaftliche und wissenschaftliche Zugriffe auf verkettete Ereignisse möglich. Datenschutz fungiert so gesehen als ein Wächter funktionaler Differenzierung und ist deshalb ein modernes Projekt der Moderne (vgl. [22]).

15 Wir können in diesem heiklen Konfliktfeld die Diskussion hier nicht vertiefen, kritisch bzgl. der Objektivität der Zweckbindung vgl. [7].

Tabelle 2 | Wesentliche Begriffe im Umfeld von Verkettung [12]

	Tatsächliche Aktion	Möglich	Nicht möglich
Verketten?	Verkettung	Verkettbarkeit	Unverkettbarkeit
Verkettetes wieder entketten?	Entkettung	Entkettbarkeit	Unentkettbarkeit

Unverkettbarkeit, das in den Common Criteria als Schutzziel der Klasse „privacy" definiert ist (vgl. [3], dazu auch [19]), perfekt umzusetzen ist vermutlich nicht möglich. Wenn aber eine Verkettung als Bürger hingenommen werden muss beziehungsweise als Kunde gewünscht wird oder als Patient in einer Mischform aus wissenschaftlichem Zwang und Freiwilligkeit auftritt, dann sollte „(…) ein potenzieller Verketter durch eine Beobachtung keine neuen Erkenntnisse über eine etwaige Zugehörigkeit von Daten zueinander (bzw. zur selben Person) gewinnen." [12].

Eine systematische Untersuchung von Verkettbarkeit zeigt, dass sich auf Datenschutz bezogene Tätigkeiten innerhalb des begrifflichen Feldes bewegen, das von Verkettung bis Unverkettbarkeit, von Entkettung bis Unentkettbarkeit von Ereignissen und Entitäten reicht (vgl. Tab. 2): Bestehende Verkettbarkeiten und Verkettungen sollen unter Bedingungen stehen oder gestellt werden, indem Maßnahmen für Entkettungen bis zur Unverkettbarkeit von Daten und Entitäten, beispielsweise Ereignisse und Datenverarbeitungen, angewandt oder entwickelt werden.

Bislang waren die Datensicherheits-Schutzziel-Definitionen begrifflich eindeutig, aber semantisch durchaus problematisch auf *Informationen* zugespitzt. Wir weiten die Perspektive nun analog systematisch, aber kategorial ebenfalls problematisch auf *Ereignisse, Systeme* (Hardware, Applikationen, Protokolle, Organisationen) und *Prozesse* aus – dies wird natürlich durch Informationen beschrieben, so dass in diesem Sinne die Zuspitzung auf Informationen nach wie vor angemessen ist. Denn Sicherheitsanforderungen sind beispielsweise auch und gerade an Prozesse, Server und Applikationen – und aus Datenschutzsicht an Organisationen überhaupt – zu stellen.[16] Dessen eingedenk lässt sich nun behaupten, dass Ereignisse, die unter allumfassenden Transparenzbedingungen beobachtet werden, grundsätzlich auch verkettbar sind. Nicht verkettbar sind Ereignisse beispielsweise, wenn sie aufgrund perfekter Opazität nicht beobachtet werden (können).[17]

Kurz angemerkt: Die beiden Datenschutz-Schutzziele konzentrieren die beiden Duale der Datensicherheits-Schutzziele: Findbarkeit, als Verfügbarkeit der Verfügbarkeit, ist auch als transparente Verfügbarkeit neu formulierbar. Verdecktheit und Unbeobachtbarkeit lassen sich als unverkettbare Vertraulichkeit bezeichnen.[18]

4 Schutzmaßnahmen

Zum Konzept der Schutzziele gehört der Ausweis von Schutzmaßnahmen zum Erreichen der Ziele. Deshalb auch dazu noch einige Anmerkungen bezüglich der Schutzziele Kontingenz, Transparenz und Unverkettbarkeit.

Erste Überlegungen zu Maßnahmen, die die Umsetzung des Schutzziels *Kontingenz* betreffen, laufen nahe liegender Weise auf den bewussten Verzicht auf Integritäts-Sicherungsmaßnahmen hinaus. So kann in einem verteilten System Kontingenz durch den Verzicht auf digitale Signaturen, eventuell sogar Authentikationscodes generell, oder Authentisierung nur der verschlüsselten Nachricht (und nicht des Klartextes) erreicht werden. Ist die Verschlüsselung so gewählt, dass bei passend gewähltem Entschlüsselungsschlüssel aus der verschlüsselten Nachricht jeder Klartext entsprechender Länge entstehen kann – wie dies beim One-Time-Pad bekanntermaßen der Fall ist – dann schränkt die Authentisierung der verschlüsselten Nachricht die Kontingenz nicht ein. Darüber hinaus kann das verteilte System nicht nur zur Erhaltung, sondern sogar zur Erzeugung von Kontingenz genutzt werden: Werden Nachrichten in viele Teile zerlegt und dabei so codiert, dass erst etliche Teile zusammen anfangen, Sinn zu ergeben und dieser Sinn durch Hinzunahme weiterer Teile detailliert wird (ähnlich wie bei einem Hologramm ein größerer Teil des Hologramms mehr Details offenbart), dann können diese Teile nacheinander oder auch parallel an unterschiedliche Instanzen des verteilten Systems gesendet werden. So kann der Inhalt am Anfang oder bei Kooperation nur weniger Instanzen in der Schwebe gehalten werden. Als weitere, schlichter einzurichtende Maßnahmen ist an ein gesichertes Stornieren und Korrigieren von Informationen nach bereits erfolgten Transaktionen zu denken. Diese könnten sogar als ein Durchgriff des Sendersystems auf (zumindest) ein Subsystem des Empfängersystems ausgelegt sein, um einen Vollzug einer „Beschwerde" oder eines Korrekturantrags oder eines Widerrufs zu vollziehen.

Transparenz wird im Datenschutz konventionell durch Anforderungen bezüglich der Dokumentation, des Monitorings und insbesondere des automatisierten Protokollierens von Prozessen der Organisation und IT, beispielsweise nach ITIL, CoBIT, FCAPS, operationalisiert [21]. Diese drei Formen der Systemdokumentation zur Herstellung von Beobachtbarkeit enthalten durchgängig Adressen von Entitäten, deren Operationen sowie Angaben zur Zeit: In Konzepten wird festgelegt, welche Entität welche Operationen bis wann durchführen wird (Zukunftsbezug). Ein Monitoring gibt Auskunft darüber, welche Entität welche Operation soeben ausgeführt hat (Gegenwartsbezug). Und Protokolle geben Auskunft darüber, welche Entitäten welche Operationen ausführten (Vergangenheitsbezug). Entsprechend kann ein Datenschutzbeauftragter heutzutage mit Verweis auf Transparenzanforderungen verlangen, dass die Konzeptionsphase eines Verfahrens von einem funktionierenden, seinerseits transparenten Projektmanagement getragen wird; dass ferner ein auf Datenschutz bezogenes Systemmonitoring so ausgelegt ist, dass

16 Eine solche definitorische Ausweitung mag bei primär akademischem Interesse Konsistenzprobleme aufweisen, von denen wir allerdings glauben, dass sie lösbar sind. Außerdem: Transparenzbedingungen nur an manche Systembereiche und/oder nur bzgl. mancher anderen Entitäten zu stellen, eröffnet einen großen und lohnenden Gestaltungsbereich für IT und Organisation.

17 In Beziehung zueinander gesetzt sind bspw. Fragestellungen spannend, in welchem Ausmaß latent unfaire Verkettung durch besonders bemühte Transparenz „kompensiert" werden kann. Genau das ist ja die Lösung im Staat-Bürger-Verhältnis.

18 Weil die Schutzziele Findbarkeit und Verdecktheit aus den Schutzzielen Verfügbarkeit und Vertraulichkeit ableitbar sind, müssen diese nicht in den Kanon elementar unverzichtbarer Schutzziele aufgenommen werden. Sie sind systematisch nachrangig, aber in der Praxis unverzichtbar.

Betroffenenrechte tatsächlich unmittelbar wirksam umgesetzt werden können; oder dass Protokolldaten revisionssicher und beweisfest die wesentlichen Ereignisse des Betriebs in Bezug auf die Verarbeitung personenbezogener oder personenbeziehbarer[19] Daten widerspiegeln. Um nicht auf die Selbstauskünfte der Organisationen angewiesen zu sein, zählen ferner unangekündigte Prüfungen, externe Auditierungen, Produktgütesiegel sowie verdeckte Konformitätstests von Produktivsystemen zu den Transparenzgenerierungsmethoden der Datenschützer.[20]

Authentisierungs- und Autorisierungsmechanismen, Rollen- und Administrationskonzepte, Zugriffsrechte, Mandantentrennungen, geregelte Zuständigkeiten und Verantwortlichkeiten sind wesentliche Bestandteile der Umsetzung von Nicht-Verkettungsanforderungen innerhalb von Organisationen. Funktionstrennungen erzeugen, wie jede Grenze, einerseits Beobachtbarkeit allein qua Trennung, und erzeugen zugleich eine Form der Intransparenz der einen Seite gegenüber der anderen Seite des Getrennten.[21] Vieles lässt sich organisatorisch einrichten, technisch abbilden und dann „nur" normativ über eine Festsetzung des Zwecks regulieren. Protokolldaten dürfen beispielsweise oftmals nur zum Zweck der Datensicherheits- und Datenschutzüberwachung, nicht aber zur Leistungs- und Verhaltenskontrolle von Mitarbeitern ausgewertet werden. Mautdaten dienen dem Zweck der Abrechnung der Straßenbenutzung, nicht aber der Verfolgung von Straftätern.

Wesentliche Instrumente zur Regulation von *Verkettungen* sind Regelungen zur Erheben und Speicherung, zum Verändern und Nutzen, zur Übermittlung und zum Löschen von Daten, zumal wenn sie in Technik auskristallisieren. Datenschutzgerechtes Verkettungsmanagement ist dabei die Domäne des „nutzerkontrollierten Identitätsmanagements Typ 3" (vgl. [12], S. 169; [13]), das insbesondere im Verhältnis von Organisationen und ihren externen Mandanten eine Rolle spielt. Hierbei besteht die wesentliche konzeptionelle Idee darin, dass, auf einer bereits Anonymität gewährenden kommunikationstechnischen Infrastruktur, Mandanten unter Pseudonymen, die unterschiedliche Eigenschaften aufweisen (von Transaktions- bis Personenpseudonym vgl. [19]), mit Organisationen kommunizieren. Erst wenn ein Personenbezug unabdingbar wird, werden die entsprechenden personenbezogenen Daten ausgetauscht (vgl. [6], kritisch zu den Möglichkeiten der Pseudonymverwendung gegenüber Verwaltungen: [10]).

5 Zwei Seitenblicke

Die Orientierung an den Datenschutz-Schutzzielen hilft Datenschützern, die angemessenen Maßnahmen zur Generierung von Transparenz auszuwählen, um im Verhältnis von Organisationen und deren Mandanten oder Mitarbeitern bestehende Verkettungen und Verkettbarkeiten von Daten und Entitäten, im Hinblick auf deren Rechtskonformität und funktionale Beherrschbarkeit sowie generell auf Grundrechtvereinbarkeit und Fairness, zu überprüfen oder zu planen, um auf eine korrekte Implementierung der Verfahren hinzuwirken.

Wenn Menschen direkt miteinander kommunizieren, unterstellen sie, dass sich das Gesprochene auf dem Weg zwischen Sender und Empfänger im Luftmedium nicht verändert (Integritätsunterstellung), es wird nur bei Hörweite gesprochen (Verfügbarkeitsunterstellung) und man richtet das Gesagte allein auf den Empfänger aus (Vertraulichkeitsunterstellung). Die gesellschaftsweit verbindliche Nutzung von Kommunikationstechnik zeigt auf, dass die drei, für Interaktionssysteme unproblematischen, Unterstellungen für Organisationssysteme explizit gemacht und dadurch problematisierbar werden müssen. Schutzziele formulieren somit basale Voraussetzungen an eine jede Kommunikation, die operativ gelingen soll.[22]

6 Fazit

Transparenz und Unverkettbarkeit sind genuine Datenschutz-Schutzziele auf dem Stand der aktuellen Datenschutz-Diskussion. Sie lassen sich in die Systematik der Datensicherheits-Schutzziele der Dual-Paare Verfügbarkeit/Vertraulichkeit und Integrität/Kontingenz einpassen. Diese Systematik zusammen mit der langen Erfahrung in der Anwendung von Schutzzielen rechtfertigt ein Zutrauen, dass die aufgeführten Schutzziele valide und für die Entwicklung weiterer Ziele und Maßnahmen geeignet sind.

Der Ausweis von Schutzzielen macht die Risiken, insbesondere moderner IT-Infrastrukturen, umfassender prüfbar, kommunizierbar und bearbeitbar. Deshalb sollten zumindest diese sechs Schutzziele in Gesetzes- und Vertragstexten sowie in systemarchitektonischen Leitlinien enthalten sein sowie als unmittelbar technisch zugängliche WebService-Policies umgesetzt werden.

Literatur

[1] AG „Technische und organisatorische Datenschutzfragen": *Empfehlungen für die Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz*. Düsseldorf, 1999.

[2] CAN: *The Canadian Trusted Computer Product Evaluation Criteria*. Version 3.0e, April 1992.

[3] IST/IEC 15408: *Common Criteria*, http://www.bsi.bund.de/literat/faltbl/F06CommonCriteria.htm

[4] DoD: *Department of Defense Trusted Computer System Evaluation Criteria*. December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225, 711

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

[6] FIDIS: *Große Sammlung an aktuellen Publikationen zu „Future of Identity in the Infor-*

19 Das Google-Imperium schickt sich an, global sämtliche Internet gestützten Ereignisse zu verketten und zu typisieren: So muss man vermuten, dass Google Nutzeraktivitäten in Google-Mail mit Daten aus Google-Streetview und mit Google-Maps sowie Google-Suchmaschinen-Nutzung verketten kann. Es entstehen damit hochgenaue, umfangreiche Nutzerprofil-Typen, die sofort personenbezogen sind, wenn eine Person hinter dem aggregierten Typ den Fehler begeht, sich an irgendeiner von google (mit-) kontrollierten Stelle zu authentifizieren (vgl. [22]).

20 Langsam breitet sich ein Verständnis von Datenschutzmanagement aus, das als wesentliches Element des Qualitätsmanagements dafür sorgt, durch Prozess-Transparenz die Lenkbarkeit einer Organisation zu verbessern.

21 Hier ein Optimum in der Evolution (Variation, Selektion, Stabilisierung) der Informationsverarbeitung von Organisationen entlang der Differenz „verkettbar/ nichtverkettbar" gesamtgesellschaftlich zu finden, ist die latente Funktion von Datenschutz als sozialer Bewegung.

22 Damit ergänzen die üblicherweise nur technizistisch interpretierten „Schutzziele" auf operativer Ebene die normativen, instrumentellen und expressiven Anforderungen, die Habermas in seiner „Theorie des kommunikativen Handelns" [11] an vernünftig gelingende Kommunikationen stellt. Über die „Funktionalität" der Schutzziele sollte auch soziologisch dringlich geforscht werden.

mation Society" http://www.fidis.net/publications/fidis-publications/#c2560

[7] Forgo, Nikolaus; Krügel, Tina: *Die Subjektivierung der Zweckbindung*. In: Datenschutz und Datensicherheit (DuD), 12/2005, S. 732 ff.

[8] Fritsch, Lothar; Abie, Habtamu: *Towards a Research Road Map for the Management of Privacy Risks in Information Systems*. In: Alkassar, Ammar; Siekmann, Jörg (Hrsg.): Konferenzband SICHERHEIT 2008, LNI 128, Gesellschaft für Informatik, Bonn 2008, S. 1-15.

[9] Gräf, Lorenz: *Privatheit und Datenschutz. Eine soziologische Analyse aktueller Regelungen zum Schutz privater Bereiche auf dem Hintergrund einer Soziologie der Privatheit*. Dissertationsdruck, Köln 1994.

[10] Gundermann, Lukas: *Sozialhilfe für Dagobert Duck*. In: Datenschutz und Datensicherheit (DuD), 5/2003, S. 282-286.

[11] Habermas, Jürgen: *Theorie des Kommunikativen Handelns*. Band 1, Suhrkamp, Frankfurt am Main 1981.

[12] Hansen, Marit; Meissner, Sebastian (Hrsg.): *Verkettung digitaler Identitäten*. Version 1.0, Projekt gefördert vom Bundesministerium für Bildung und Forschung, 2007 https://www.datenschutzzentrum.de/projekte/verkettung/

[13] Hansen, Marit: *User-controlled identity management: the key to the future of privacy?* In: International Journal of Intellectual Property Management (IJIPM), Special Issue on Identity, Privacy and New Technologies, Part 2, Vol. 2, No. 4, Inderscience Publishers, Olney 2008 (UK), S. 325-344

[14] ITSEC: *European Communities – Commission: ITSEC: Information Technology Security Evaluation Criteria*. Provisional Harmonised Criteria, Office for Official Publications of the European Communities, Luxembourg, Version 1.2, 28 June 1991.

[15] Luhmann, Niklas: *Soziale Systeme*. Suhrkamp, Frankfurt am Main 1984.

[16] Luhmann, Niklas: *Erkenntnis als Konstruktion*. Westdeutscher Verlag, Bern 1988.

[17] OSCI-Steering-Office: *OSCI-Transport 2.0: Web Services Profiling and Extensions Specification*. 2009 http://www.osci.eu/transport/osci20/specification/OSCI2_WS-Profiling AndExtension-Specification_EN.pdf

[18] Pfitzmann, Andreas: *Multilateral Security: Enabling Technologies and Their Evaluation*. In: Günter Müller (Ed.): Emerging Trends in Information and Communication Security (ETRICS 2006), Freiburg, LNCS 3995, Springer-Verlag, Heidelberg 2006.

[19] Pfitzmann, Andreas; Hansen, Marit: *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*. Version 0.31, 15.02.2008 http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (abgerufen am 2009-05-13).

[20] Rost, Martin: *Verkettbarkeit als Grundbegriff des Datenschutzes?* In: Innovativer Datenschutz, Für Helmut Bäumler 2004, S. 315-334 http://www.maroki.de/pub/privacy/fgb_www.pdf

[21] Rost, Martin (Hrsg.): *Schwerpunktheft Protokollierung*, Datenschutz und Datensicherheit (DuD), 10/2007.

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

[23] Wolf, Gritta; Pfitzmann, Andreas: *Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen*. In: Informatik Spektrum, 2000/06, S. 173-191.

[24] Zentralstelle für Sicherheit in der Informationstechnik – ZSI (Hrsg.): *IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)*. 1. Fassung vom 11.1.1989; Köln.