Martin Rost

Die Ordnung der Schutzziele

Dieser Artikel stellt verschiedene Anordnungen von Datenschutz-Schutzzielen vor, die für den operativen Datenschutz von vielfach überraschender Bedeutung sein können.

1 Einleitung

Schutzziele bzw. Gewährleistungsziele verankern das Standard-Datenschutzmodell (SDM) in der Datenschutz-Grundverordnung (DSGVO).[1] Drei Fragen zur Genese und Struktur von Schutzzielen warten seit langem darauf, beantwortet zu werden: 1. Was ist das „generative Prinzip" für neue Schutzziele und welche Instanz darf diese berechtigt als „verbindlich geltend" ausrufen? 2. Lässt sich eine Vermutung zur Vollständigkeit von Schutzzielen anstellen? 3. In welchem Verhältnis stehen Schutzziele zueinander? Diese drei Fragen stellte Andreas Pfitzmann, Professor für technischen Datenschutz und Datensicherheit an der Technischen Universität Dresden, 2008 in einem arbeitsgruppeninternen Arbeitspapier.[2] Inzwischen lassen sich darauf erste Antworten geben.

2 Erste Antwort-Versuche

Die *Frage 1* nach dem generativen Prinzip für Schutzziele und der Instanz, die berechtigt Schutzziele ausrufen darf, lässt sich inzwischen relativ leicht beantworten.

Für Pfitzmann waren Schutzziele noch ein Regulationsinstrument speziell für IT-Sicherheit. Schutzziele wurden 1983 im „Orange Book" zur Bewertung und Zertifizierung der Sicherheit von Computersystemen formuliert, die 1996 in die Common Criteria (heute ISO/IEC 15408) überführt wurden. Inzwischen kennen Behörden und Unternehmen in Deutschland diese drei Schutzziele (Sicherung der Verfügbarkeit, Integrität, Vertraulichkeit) insbesondere aus dem Kontext des IT-Grundschutzes des BSI. Man nutzt sie in den Sicherheitskonzepten als normative Anker. Schutzziele gelten, wenn sich eine Organisation, wie etwa das Department of Defense im „Orange Book", zu ihnen bekennt. An dieser schwachen Legitimation ändert sich auch dann nichts, wenn etwa eine weltweit agierende Organisation, wie die ISO, ein bestimmtes Set an Schutzzielen als den Stand der Technik repräsentierend behauptet. Soziologisch betrachtet formulieren Schutzziele in diesem Sinne allein Interessen von Organisationen.

Organisationen kennen das Instrument der Zielvereinbarungen, die dann sowohl in Form von inputorientierten „Konditionalprogrammen" und outputorientierten „Zweckprogrammen" umgesetzt werden (vgl. Luhmann 2000). Ziele bieten Organisationen ein Medium, die arbeitsteiligen Differenzen übergreifend normativ-regulativ zu fokussieren, mit denen sowohl Gesetze als auch selbstgesetzte Maßstäbe organisationsintern verständlich angeschlossen werden. Seit der Jahrtausendwende sind Schutzziele auch Bestandteil bspw. in vielen Landesdatenschutzgesetzen, im Artikel 5 der DSGVO (vom 25. Mai 2016) sowie im § 8a des IT-Sicherheitsgesetzes (vom 17. Juli 2015). Inzwischen ist der Katalog von Schutzzielen ausgeweitet, auf Anforderungen des Datenschutzes angepasst und im Rahmen des Standard-Datenschutzmodells operationalisiert worden. Die Aufnahme von Schutzzielen in Gesetzestexte verwischt notwendig deren bislang technisch dominierte Definitionen, führt aber auch zu einer breiteren Legitimation und Durchsetzbarkeit von Schutzzielen in Organisationen.

Die *Frage 2* nach der „Vollständigkeit des Sets von Schutzzielen" verschiedener (ausufernder) Schutzzielkataloge – Pfitzmann kritisierte in dem internen Arbeitspapier den Wildwuchs beim Ausrufen immer neuer Schutzziele durch immer neue Organisationen -, ist naturgemäß ungleich schwieriger zu beantworten. Ein erster und konzeptionell schlichter Versuch soll hier unternommen werden, auch wenn man außerhalb mathematischer Konstruktionen oder analytisch trivialer Systeme mit der Behauptung einer Vollständigkeit nur scheitern kann.[3]

Die Inkorporation des Sets an Schutzzielen in Datenschutzgesetze erlaubt es, diese Ziele mit anderen bestehenden Normengefügen in ein, mit juristischen Methoden gesichertes, Verhältnis zu setzen. So lässt sich die normative Nachrangigkeit von Schutzzielen gegenüber Grundrechten feststellen, wonach Schutzziele nur eine die Grundrechte zu operationalisierende Funktion innehaben können und insofern keinem Selbstzweck unterliegen. Dann stellen sich zwei Fragen: Erfassen die Schutzziele vollständig die gegenwärtig vom Datenschutz umfassten Grundrechte, und führt die Umsetzung der Schutzziele zu einer ebenso vollständig wirksamen Umsetzung der Anforderungen von Grundrechten?

In Bezug auf die Operationalisierung von Grundrechtsanforderungen kann man vermuten, dass die sechs elementaren Schutzziele des Datenschutzes – Sicherung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung[4] und Intervenier-

1 SDM, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

2 Andreas Pfitzmann starb im September 2010. Diese Fragen entstanden vermutlich während seiner Beratungen des Bundesverfassungsgerichts im Vorfeld der Erarbeitung des Vertraulichkeits- und Integritätsurteils (siehe BVerfG 2008).

Martin Rost

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

E-Mail:
martin.rost@datenschutzzentrum.de

3 Wegen der offenen Zukunft gesellschaftlicher Entwicklungen kann das Set der Datenschutz-Schutzziele nur als „historisch" oder „aktuell" vollständig behauptet werden (Kloepfer 2015).

4 Die normativ wichtige Anforderung der Datenminimierung wird in diesem Artikel als Untermenge des Schutzziels Nichtverkettung behandelt, weil die

barkeit von personenbezogenen Verfahren aus der Sicht von Betroffenen und bezogen auf die EU-Grundrechte-Charta sowie das deutsche Grundgesetz als vollständig angenommen werden können. Diese Vermutung speist sich aus einer Großzahl an inzwischen durchgeführten Prüfungen von Verfahren sowie aus der Entdeckung der Fruchtbarkeit der verschiedenen Formen der Anordnung der Schutzziele und den Diskussionen darüber. Es lassen sich weitere, spezifische Schutzziele aus den schon bestehenden elementaren Schutzzielen heraus entwickeln. Hiernach ist das Schutzziel „Belastbarkeit" (Art. 5 DSGVO) als „gesichert integre Verfügbarkeit" interpretierbar und mit entsprechend kombinierten Maßnahmen umzusetzen. Dazu gleich mehr.

Bevor auch die *Frage 3* nach der „Ordnung der Schutzziele untereinander" behandelt werden kann, muss die soziologisch wesentliche kommunikative Funktion von Schutzzielen beleuchtet werden.

3 Die kommunikative Funktion von Schutzzielen

Schutzziele erlauben Organisationen, unterschiedliche Anforderungen und Logiken in ihren Verfahren und Datenverarbeitungen punktuell aufeinander zu beziehen. Bei Organisationen denke man an Unternehmen, Behörden, Forschungsinstitute, an Arztpraxen und Kanzleien, an Vereine und Parteien, Schulen, Krankenhäuser, Armeen, Gefängnisse, Access- und Contentprovider; bei Logiken denke man bspw. an rechtliche, finanzielle und wissenschaftliche Anforderungen und Strategien. TechnikerInnen legen dabei auf andere Verfahrenseigenschaften gesteigerten Wert als JuristInnen, Betriebswirte oder SystemarchitektInnen. In der rechtlichen Domäne formt die Differenz der Rechtskonformität/Nichtrechtskonformität die Kommunikationen. Es ist jedenfalls nicht die Differenz der Ingenieurinnen, die ihrerseits entlang der Beobachtung, ob etwas funktioniert oder nicht-funktioniert, agieren und kommunizieren. Und Ökonomen beobachten ihre Umwelt letztlich allein anhand der Differenz der Zahlungen/ Nichtzahlungen.

Schutzziele fokussieren die wesentlich zu lösenden Probleme und Konflikte, ohne dass durch die Fokussierung bereits eine der beteiligten Logiken, etwa die technische – die anderen beiden Logiken – etwa die rechtliche oder betriebswirtschaftliche – strukturell vorentschieden dominiert. Schutzziele koppeln punktuell bestimmte Leitaspekte und entkoppeln die prozessualen Abfolgen der beteiligten Logiken und Steuerungshierarchien.

Wenn man diese Eigenschaft noch etwas generalisierter formuliert, dann lässt sich behaupten: Schutzziele fokussieren Kommunikationen innerhalb und zwischen unterschiedlichen Fachgebieten mit ihren unterschiedlichen Logiken, die sich in modernen Gesellschaften arbeitsteilig in Organisationen herausgebildet haben. Keine Domäne kann dabei aussichtsreich beanspruchen, die Letztdefinition für einzelne Schutzziele zu formulieren, die die anderen Domänen dann schlicht zu übernehmen haben. Die Definition eines übergreifend verständlichen Zieles muss dabei derart verallgemeinert formuliert sein, dass das Ziel spezifisch für die eigenen Domäne leiten kann, und in allen anderen Domänen dennoch in die gleiche Richtung weist.[5] Schutzziele müssen insofern mehr umfassen, als nur juristisch geprägte Normen etwas umformuliert zu wiederholen.[6]

Man kann sich der Frage, was Schutzziele leisten, auf eine andere Weise nähern und deren Beantwortung, und damit auch die Begründung für den Datenschutz, soziologisch tiefer legen. Die soziologische These lautet, dass die Schutzziele das Habermas'sche Set der sinnhaften Geltungsanforderungen an eine vernünftige Rede um operative Anforderungen ergänzen. Schutzziele wären analog dazu als Geltungsanforderungen an „ein vernünftiges Funktionieren von Systemen" zu verstehen. Diese Geltungsanforderungen sind an technisch vermittelte Kommunikationsinfrastrukturen wie bspw. das Internet – und alle darauf aufsetzenden Dienste – zu stellen. Die Organisationen, die Verfahren, Dienste, Plattformen, Netze und die darunter zum Einsatz kommenden technischen Komponenten müssen allesamt den von den Schutzzielen formulierten Anforderungen genügen, damit die sinnhaften Geltungsanforderungen tatsächlich operativ einlösbar werden. *Ohne die funktionalen Maßnahmen des Datenschutzes für personenbezogene Verfahren und Kommunikationstechniken ist das Habermas'sche Diskursmodell für eine moderne Gesellschaft, in denen Kommunikationen technisch übermittelt werden, obsolet.* Hiernach lautet die These, dass sich Schutzziele evolutionär herausgebildet haben, weil eine moderne Gesellschaft auf ein tatsächliches Gelingen von Kommunikationen in Bezug auf Wahrheit, normative Richtigkeit und Wahrhaftigkeit im Kontext von Organisationen angewiesen ist (vgl. Rost 2013).[7]

4 Die Ordnung der Schutzziele

Wie lässt sich nun, um auf die Frage 3 zurück zu kommen, das Verhältnis von Schutzzielen untereinander bestimmen? Die These lautet, dass die Plausibilität einer Reihenfolge der Schutzziele beobachterabhängig ist. So wird eine Technikerin eine andere Reihenfolge plausibel finden als ein Datenschutzjurist oder eine Betriebswirtin. Eine allgemeine, abstrakt gültige hierarchische Anordnung lässt sich nicht formulieren.

Wenn man sich zunächst wieder auf die drei konventionellen Schutzziele – Sicherung der Verfügbarkeit, Integrität und Vertraulichkeit – konzentriert, dann drängt sich typisch zunächst ein Dreieck als Abbildung auf. Mit einer solchen Struktur vor Augen stellt sich nicht zwingend die Frage, ob sich die Schutzziele sinnvoll auch paarweise widerstreitend oder hierarchisch oder selbstbezüglich anordnen lassen.

Bei näherer Befassung zeigt sich, dass eine radikal einseitige Umsetzung eines dieser Schutzziele zu Lasten der anderen

Datenminimierung im Hinblick auf den Zweck des Verfahrens, der die Verkettung von Daten als erforderlich und angemessen legitimiert und limitiert, geschehen muss. Diese Ansicht bzgl. der nachrangigen Positionierung der Datenminimierung wird nicht von allen der sich am Diskurs über Schutzziele beteiligenden Kollegen geteilt.

5 Dieser Anspruch auf abstrakt übergreifende Geltung ist in der gegenwärtigen Definition der Schutzziele, wie sie im Standard-Datenschutzmodell explizit vorgenommen wird, noch nicht hinreichend eingelöst, einige Definitionen sind juristisch dominiert. So wird bspw. Transparenz dort als „Herstellung von Prüf- und Beurteilbarkeit" definiert. Das versteht man als Informatiker natürlich, insofern leitet diese Definition bei der Operationalisierung nicht fehl. Jedoch wird in der Informatik unter Transparenz ein Durchgriff eines Nutzers auf ein System verstanden, bei dem der Nutzer, die Aktivitäten die er im System auslöst, selber gar nicht bemerkt, und der Nutzer gerade nicht in einen hemmend-reflektierenden Modus des Prüfens versetzt werden soll.

6 Wie es beim Schutzziel „Datenminimierung" im SDM gegenwärtig leider der Fall ist.

7 Die gegenwärtige Situation nährt Vermutungen, dass die Moderne regrediert.

Schutzziele geht. So riskiert bspw. eine gesicherte Verfügbarkeit eines Datums, etwa das Anfertigen von Backups, grundsätzlich immer die Sicherung der Vertraulichkeit eines Datums, weil das Risiko unbefugter Kenntnisnahme mit jeder weiteren Kopie eines Datums steigt. Umgekehrt führt eine intensive Sicherung der Vertraulichkeit eines Datums, umgesetzt etwa durch Verschlüsselung, dazu, die Sicherung der Verfügbarkeit eines Datums zu riskieren, weil bspw. eine Passphrase verloren gehen kann. Nimmt man das vollständige Set der sechs Datenschutz-Schutzziele in den Blick, werden sofort weitere Konflikte ähnlicher Art deutlich: Ein hohes Maß an Transparenz eines Verfahrens, die bspw. durch Dokumentation und Protokolldaten hergestellt wird, riskiert, dass diese Daten unbefugt oder zweckdehnend zur Verhaltens- und Leistungskontrolle von Mitarbeitern genutzt werden können.

Die Widersprüchlichkeit der Schutzziele untereinander mit ihren je für sich zugleich unabweisbaren Anforderungen verweist darauf, dass Schutzziele keine Dimensionen sind. Für die Behauptung von Dimensionen wäre zu verlangen, dass die Schutzziele unabhängig voneinander sind. Das sind sie jedoch nicht. So sichert man bspw. durch Maßnahmen der Vertraulichkeit in der Praxis auch deren Integrität zumindest für bestimmte Angriffe mit.

Nachfolgend werden drei Typen der Anordnung von Schutzzielen kurz diskutiert:[8]

1. Die elementaren Schutzziele lassen sich als drei Dual[9]-Achsen ordnen. Hiernach wird behauptet, dass zwei zugleich verfolgte Schutzziele, die ein Dual bilden, bei ihrer Umsetzung in die Praxis die Schutzwirkung des je anderen Schutzziels verringern. Diese Vorstellung war es, die 2009 zur Entwicklung der sechs elementaren Schutzziele und letztlich zum Standard-Datenschutzmodell führte. Die Anordnung als Dual gestattet eine ganz spezifische Verschränkung von Recht und Technik.
2. Die Schutzziele lassen sich selbstbezüglich zueinander anordnen. Bei sechs Schutzzielen hat man es demnach formal mit 36 analysierbaren Schutzzieldualen zu tun. Bei der Entwicklung des SDM hat sich gezeigt, dass wechselseitiges Beziehen von Schutzzielen eine fruchtbare Regel zum Generieren eines vollständigen Katalogs an Schutzmaßnahmen für hohen Schutzbedarf ist.
3. Die Schutzziele lassen sich hierarchisch anordnen. Die Plausibilität der Reihenfolge der Schutzziele hängt vom Organisationstyp ab, in dem diese umzusetzen sind. Die Möglichkeit der Ausweisung typischer Schutzziele-Hierarchien würde es für einen Großteil von Organisationen erlauben, standardisierte Datenschutzanforderungen bzw. Schutzmaßnahmenkataloge auszuweisen.

4.1 Duale Anordnung von Schutzzielen

Die Anordnung von Schutzzielen als Dual gestattet eine ganz spezifische Verschränkung von Recht und Technik. Die beiden Sphären – funktionale Technik und verbindlich geltende Normen – werden mittels Schutzzielen entkoppelt, ein Übergreifen der einen Fachlogik auf die andere wird vermieden. Zugleich werden punktuell Fokussierungen und Berührungen beider Logiken durch Schutzziele bereitgestellt. Die Zusammenarbeit zwischen dem Juristen und der Technikerin besteht insofern darin, dass der Jurist anhand des Datenschutzrechts als normatives Regelwerk die Abwägung zwischen den Schutzzielen, bzw. den exponierten Schutzziel-Paaren, trifft und die Technikerin dann das Arsenal an möglichen Schutzmaßnahmen überblickt, die nach dieser normativ getriebenen Abwägung auf das spezielle Verfahren angepasst zu implementieren sind.

Der erste Entwurf einer systematischen Anordnung der elementaren Schutzziele von Pfitzmann und Rost wies drei solcher Dual-Achsen auf: Verfügbarkeit / Vertraulichkeit, Integrität / Intervenierbarkeit, Transparenz / Nichtverkettbarkeit (Rost/Pfitzmann 2009). Durch dieses Hervorheben dreier Paare wird es der Juristin erleichtert, den operativ zu bewältigenden Lösungsraum vollständig zu berücksichtigen. Normenexperten bedürfen bei der Prüfung der operativen Ebene von Verfahren des methodischen Halts bei der Frage, welche Prinzipien (Schutzziele) insgesamt und gegenseitig abzuwägen sind.

Neben der Gleichgewichtigkeit zwischen drei privilegierten Dualpaaren kann es sich für das konkrete Verfahren als gerechtfertigt erweisen, ein Schutzziel innerhalb eines Duals als führend auszuweisen. So kann bspw. bei der Rettung oder Verteidigung von Menschenleben die Sicherung der Verfügbarkeit von Rettungsmaßnahmen juristisch berechtigt als wichtiger einzustufen sein als die Sicherung der Vertraulichkeit. Dabei kann es logisch, gemäß des 3-Duale-Modells, für ein Verfahren nur ein dominantes Schutzziel pro Dual geben, die sich wiederum ihrerseits in eine Gesamtrangfolge sämtlicher Schutzziele bringen lassen können.

4.2 Selbstbezügliche Anordnung von Schutzzielen

Bei der Entwicklung des Maßnahmenkatalogs des SDM zeigte sich, dass durch den Selbstbezug von Schutzzielen bzw. den entsprechenden Schutzmaßnahmen eine Regel gefunden wurde, um Schutzmaßnahmen auch für einen hohen Schutzbedarf ausweisen zu können. Getroffene Schutzmaßnahmen müssen hiernach ihrerseits dem vollständigen Set der Schutzziele genügen. Was ist damit gemeint? Bei einem Grundrechtseingriff geringer Intensität bzw. bei normalem Schutzbedarf eines Verfahrens müssen bspw. zur Umsetzung des Schutzziels „Transparenz" Prozesse und Systeme protokolliert werden. Bei hohem Schutzbedarf müssen Protokolldaten zusätzlich integritätsgesichert signiert und vertraulichkeitsgesichert verschlüsselt werden, es muss ein Rollen- & Berechtigungskonzept für den Zugriff auf die Protokolldaten vorliegen usw.

Bei der Diskussion der 36 möglichen Zuordnungen zeigte sich, dass es möglich wird, den Katalog an Schutzmaßnahmen auf Vollständigkeit zu analysieren. So wird bspw. deutlich, dass eine integritätsgesicherte Maßnahme zur Sicherung von Transparenz von einer transparenzgesicherten Maßnahme zur Sicherung der Integrität eines Verfahrens zu unterscheiden ist. Auch die zunächst etwas seltsam anmutende Beziehbarkeit eines Schutzziels unmittelbar auf sich selbst – bspw. „Transparenz sichernde Transparenz" – ist sinnvoll. Sie verweist darauf, dass Transparenz hergestellt werden muss und keinesfalls als eine passiv immer schon gegebene Systemeigenschaft gelten kann. Es gilt die Methodik zur Herstellung von Transparenz transparent zu machen. Transparenz für einen Empfänger herzustellen verlangt vom Sender, über ein Modell des Empfängerhorizonts und dessen Methoden des spezifischen Beobachtens zu verfügen. Konkret: Transparenz für eine betroffene Person herzustellen (Datenschutzerklärung) be-

8 Siehe zur Diskussion weiterer Aspekte der Anordbarkeit der elementaren Schutzziele die Beiträge von Robrahn/Bock, Jensen und Pohle in diesem Heft.

9 Der Begriff Dual stammt von Pfitzmann. Er soll bezeichnen, dass zwei Schutzziele im gleichen Maße gelten, aber in einem Widerspruch zueinander stehen.

darf anderer Maßnahmen als solche, die Transparenz für die eigene Organisation oder für eine kooperierende Organisation, etwa im Kontext der Auftragsverarbeitung, oder für Aufsichtsbehörden herstellen sollen. Datenschutzbeauftragte interessiert bspw., welche Prozesse und Systeme in welcher Form wo protokolliert werden, um die Wirksamkeit der getroffenen Schutzmaßnahmen beurteilen zu können.

Aus der These von der relativen Vollständigkeit der Schutzziele folgt, dass durch Selbstbezug der elementaren Schutzziele weitere spezifische Schutzziele formulierbar sein müssen. So lässt sich bspw. das etwas überraschend geforderte Schutzziel „Belastbarkeit" (Art. 32 DSGVO) mit den Bordmitteln der vorhandenen Schutzziele als „integritätsgesicherte Verfügbarkeit" konzipieren, mit den entsprechend zu wählenden Schutzmaßnahmen. Umgekehrt ist es sinnvoll, durch Selbstbezug geschöpfte Schutzziel-Konstellationen eigens als ein spezifisches Schutzziel zu bezeichnen. So lässt sich bspw. eine gesichert vertrauliche Vertraulichkeit als Unbeobachtbarkeit bezeichnen, und dann mit speziell steganographischen Schutzmaßnahmen umsetzen. Sollte sich zeigen, dass die These der relativen Vollständigkeit der sechs elementaren Schutzziele nicht zu halten ist, legte das wiederum den Rückschluss nahe, dass man damit vielleicht nicht gleich ein neues Grundrecht, wohl aber eine neue wesentliche Facette gefunden bzw. konstruiert haben könnte.[10]

Mit der Regel der Selbstbezüglichkeit wird es außerdem möglich, die Vollständigkeit und Konsistenz eines Datenschutz-Schutzziele- und Maßnahmenkatalogs zu beurteilen und aufrechtzuerhalten. So lässt sich prüfen, ob ein als „neu" an den Schutzzielekatalog herangetragenes Schutzziel nicht durch selbstbezügliche Konstellationen rekonstruierbar oder unter vorhandene Schutzziele subsumierbar ist. Vorschläge für neue Schutzmaßnahmen oder für Veränderungen von Maßnahmen in einem Maßnahmenkatalog können ebenfalls anhand dieser Prüfung akzeptiert oder abgewiesen werden. Eine solche Qualitätssicherung vorzunehmen ist zudem eine notwendige Bedingung, um Maßnahmen in einer konsistenten Granularität und nach Schutzbedarf unterschieden ausweisen zu können.[11]

4.3 Hierarchische Anordnung von Schutzzielen

Schutzziele lassen sich hierarchisch anordnen. Nachfolgend wird die These plausibilisiert, dass grundsätzlich in jedem Falle die Sicherung der Integrität Vorrang hat, wobei das Verständnis von Integrität allerdings von der jeweiligen arbeitsteilig organisierten „Fachlogik" abhängt.[12]

Hiernach ließe sich von einer technisch-funktionalen Integrität eines Verfahrens sprechen, wenn ein Verfahren der funktionalen Spezifikation möglichst nahe kommt, die gewünschten Eigenschaften aufweist und wirksam funktioniert. Der Wirkungsgrad, die Nebenwirkungen und Seiteneffekte sind bedacht und unter Kontrolle gehalten. Immer gleiche Inputs führen zu immer gleichen Outputs, Kausalität ist das Kontrollideal.[13] In einem Bafög-Verfahren wird die Zahlungshöhe automatisch berechnet, das Ergebnis muss korrekt sein. Davon zu unterscheiden wäre eine rechtliche Integrität. Diese ist dann gewährleistet, wenn ein Verfahren den rechtlichen Anforderungen genügt. In Bezug auf ein Bafög-Verfahren hieße das, dass es mit allen seinen Komponenten allein und ausschließlich der Berechnung von Auszahlungshöhen und der Verwaltung von berechtigten Empfängern durch berechtigte Sachbearbeiter dient, unter Berücksichtigung sämtlicher einschlägiger Gesetze. Von einer auch betriebswirtschaftlichen Integrität ließe sich sprechen, wenn sich das Verfahren mindestens so kostengünstig betreiben lässt, wie die Bafög-Verfahren anderer Organisationen.

Wenn die fachspezifische Integrität eine Schutzziele-Hierarchie in einer arbeitsteiligen Organisation jeweils dominiert, muss das zweite Schutzziel in einem sehr engen Verhältnis dazu stehen, weil es die spezifisch fachliche Logik im Unterschied zu anderen operativ berücksichtigen muss.

Technisch betrachtet steht als zweites Schutzziel die gesichert funktionale Verfügbarkeit eines Verfahrens im Vordergrund, zu der insbesondere die Verfügbarkeit von Reparatur- und Backupprozessen zählen. Speziell sicherheitstechnisch ist dagegen die Sicherung der Vertraulichkeit der Datenverarbeitung das maßgeblich zu lösende Problem. Technisch müssen Maßnahmen zum Vertraulichkeitsschutz redundant bereitstehen. Der technische Vertraulichkeitsschutz sichert einer Organisation ihr Fortbestehen: Daten, die bspw. Teil des Geschäfts- und Verfahrensgeheimnis sind, dürfen dann nur noch unter klar kontrollierten Bedingungen abfließen können. Wenn die Datenverarbeitung von Organisationen voll durchdigitalisiert ist, gilt: Nur die Kontrolle über Datenflüsse kann den Bestand einer Organisation sichern. Anders ist die datenschutzrechtliche Perspektive: Hiernach wird die speziell datenschutzrechtliche Integrität in Form der Zwecksetzung, Zweckbestimmung, Zwecktrennung und Zweckbindung eines Verfahrens mit Hilfe von verfügbaren technischen Maßnahmen der Nichtverkettung durchgesetzt. Es soll ein Verfahren betrieben werden, in dem das Maß an Fremdbestimmung auf das unbedingt erforderliche Maß reduziert ist. Betriebswirtschaftlich und politisch dürfte das zweite Schutzziel ebenfalls der Bestärkung des Schutzziels der Sicherung der Verfügbarkeit dienen. Es soll das Verfahren geben, entweder zwecks optimaler Kapitalverzinsung oder um bestehende Machtverhältnisse sicherzustellen.

An dritter Stelle einer Zielehierarchie stünde dann, wieder für alle an einem Verfahren beteiligten Fachlogiken gemeinsam, die Transparenz. Die Funktion der Transparenz liegt darin, prüfbar zu machen, ob die fachliche Integrität wirksam gesichert ist.

Welches Schutzziel an vierter Stelle folgt, hängt wieder von der Fachlogik ab, mit welcher Dringlichkeit Fehlerkorrekturen durchzuführen sind. Steht die Sicherung der Verfügbarkeit ganz oben, muss die Intervenierbarkeit gesichert werden. Die Intervenierbarkeit riskiert zugleich grundsätzlich die Integrität, weil Veränderungen zwar nur organisationsintern gesteuert durchgeführt werden sollen, doch zugleich bieten die entsprechenden Maßnahmen komfortable Eingriffsmöglichkeiten auch für Externe.[14] Man kann insofern plausibel machen, dass eine unverzügli-

10 Zum „Finden" neuer Grundrechte vgl. Hornung 2014.

11 Bisherige Schutzzielekataloge würfeln Prinzipien, Grundsätze, Normen, Ziele, Prozesse und Regeln durcheinander und stellen auch Maßnahmen beliebig zusammen. Sie weisen keinen Maßstab für den Bezug zu gesetzlichen Anforderungen, zur Vollständigkeit oder der angestrebten Qualität aus. Diese Kritik gilt bspw. für die ISO 29101:2013 genauso wie für den Maßnahmenkatalog der CNIL (vgl. CNIL 2012).

12 Ein weiterer Vorschlag zur Anordnung findet sich bei Rost 2017.

13 An dieser Stelle kann die Frage vernachlässigt werden, ob diese Charakterisierungen auch für neuronale Netze oder für Verfahren mit künstlicher Intelligenz gilt.

14 Als Beispiel sei an den Staatstrojaner gedacht, den zu nutzen zwar Sicherheitsbehörden vorbehalten bleiben soll, bei dem aber zu vermuten ist, dass er

che Korrektur relevanter Abweichungen technisch hohe Priorität hat, während rechtlich eine Korrektur normativer Abweichungen in der Regel mehr Zeit zur Heilung beanspruchen darf, wobei ökonomisch eine gebotene Korrektur auch als aktuell zu teuer eingestuft werden kann.

Eine Diskussion einer hierarchischen Anordnung von Schutzzielen steht ersichtlich noch am Anfang. Eine Ausarbeitung sollte die ausgewiesenen spezifischen Widersprüchlichkeiten der Dualpaar-Anordnungen berücksichtigen. Das bedeutete z.B., dass der Ausweis eines führenden Leit-Schutzziels dazu führen muss, dass sich das entsprechende Dual-Schutzziel am Ende der Hierarchie befindet. Dann folgen die anderen beiden Dualpaare, die ihrerseits ebenso diametral angeordnet werden müssen.

Und warum das Ganze? Die These lautet, dass für jeden Organisationstyp[15] – Verwaltung, Unternehmen, wissenschaftliches Institut, freiwillige Vereinigung, totale Institutionen mit ihren starken Kontrollen über Personen (Gefängnisse, Armee, Schulen, Krankenhäuser) – eine Hierarchie an Schutzzielen ausweisbar ist, mit einer spezifischen Anordnung wiederum der Dualpaare innerhalb der Hierarchie. Für den Datenschutz würde das bedeuten, dass für jeden Typ von Organisation spezifische Hinweis zur Abwägung sowie vor allem ein Standardkatalog aufeinander abgestimmter Maßnahmen ausweisbar wäre.

5 Fazit

Die Schutzziele des Datenschutzes koppeln und entkoppeln, als organisationsnahe Kommunikationsmedien, die verschiedenen Fachlogiken, die an der Entwicklung und der Aufrechterhaltung eines kontrollierten Betriebs eines personenbezogenen Verfahrens in Organisationen beteiligt sind. Diese Eigenschaft ist für den Betrieb moderner personenbezogener Verfahren, die nicht gegen Grundrechte verstoßen und effektiv funktionieren sollen, in einer modernen „funktional-differenzierten Gesellschaft" (Luhmann) unabdingbar. Die Geltung von Schutzzielen im Datenschutz, und teilweise in der IT-Sicherheit, ist inzwischen gesetzlich legitimiert. Für das bislang ausgewiesene Set von sechs elementaren Schutzzielen darf man eine historisch relativierte Vollständigkeit annehmen. Dieses Set an Schutzzielen ist semantisch inzwischen so aufgeladen und ausdifferenziert, dass selbstbezügliche Bezugnahmen in der Praxis dafür genutzt werden können, einen Maßstab für die Qualität von Schutzmaßnahmen auszubilden. Der Versuch des Ausweises einer Steuerungshierarchie der Datenschutz-Schutzziele zeigt, dass diese für jeden Organisationstyp anders ausfällt.

Literatur

Apelt, Maja / Tacke, Veronika (Hrsg.): Handbuch Organisationstypen, Wiesbaden, VS Verlag für Sozialwissenschaften

BverfG, 2008: Urteil vom 27. Februar 2008 zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", Az. 1 BvR 595/07, 1 BvR 370/07, https://openjur.de/u/59199.html

CNIL, 2012: Measures for the privacy risk treatment, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf

Hornung, Gerrit, 2014: Grundrechtsinnovationen, Tübingen, Mohr Siebeck

Kloepfer, Michael 2015: Seminar „Neue Grundrechte – Analyse und Vorschläge", http://kloepfer.rewi.hu-berlin.de/doc/Themen_VEROEFF.pdf

Luhmann, Niklas 2000: Organisation und Entscheidung, Opladen/ Wiesbaden, Westdeutscher Verlag

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

Rost, Martin, 2012: Standardisierte Datenschutzmodellierung; in: DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438

Rost, Martin, 2013: Zur Soziologie des Datenschutzes; in: DuD – Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 85-91

Rost, Martin, 2017: Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten, in: Sowa, Aleksandra, 2017: IT-Prüfung, Sicherheitsaudit und Datenschutzmodell: Neue Ansätze für die IT-Revision, 1. Auflage, Springer Vieweg, S. 23-56

zumindest von Programmcodeherstellern und Hackern gekapert werden kann.

15 Siehe eine Auflistung von Organisationstypen moderner Gesellschaften bei Apelt / Tacke 2012.