# Eine kurze Geschichte des Prüfens

**Martin Rost**[1]

Viele Jahre profitierten Informationssicherheit und technisch-organisatorischer Datenschutz voneinander. Seit den 90er Jahren konnten die an IT-Sicherheit Interessierten ihre Forderungen mit den im Datenschutzrecht verankerten Bestimmungen zur Sicherung personenbezogener Daten begründen, während Technik-affine Datenschutzbeauftragte die überzeugenden Prüfkonzepte und Tools der IT-Sicherheit nach und nach übernahmen. Unter der Hand schlich sich dadurch, selbst bei Datenschutzaufsichtsbehörden, in den letzten Jahren eine Praxis ein, bei der die Konformität mit IT-Grundschutz mit der Konformität der technisch-organisatorischen Datenschutz-Anforderungen weitgehend gleichgesetzt wurde. Eine pauschale Gleichsetzung von Informationssicherheit und Datenschutz verkennt jedoch die unterschiedlichen Schutzobjekte beider, Geschäftsprozesse hier und Betroffene dort. Gegenwärtig zeichnet sich ab, dass die Maßnahmen der Informationssicherheit zunehmend ihre eigenen Rechtsgrundlagen bekommen und der technisch-organisatorische Datenschutz zunehmend die guten Methoden der Informationssicherheit für Prüfungen nutzt. Diese Entwicklung lässt sich anhand einer grob in drei Phasen umrissenen Geschichte des Prüfens der Datenverarbeitung von Organisationen nachvollziehen.

Stichworte: Datenschutz, Datensicherheit, Grundschutz, Informationssicherheit, IT-Sicherheit, Methodik, Prüfung, Rechtsgrundlagen der Informationssicherheit, Schutzziele, Standard-Datenschutzmodell (SDM).

## *1.* Einleitung

Die Angreifermodelle von Informationssicherheit und Datenschutz lassen sich gut konturiert einander gegenüber stellen: Die Informationssicherheit stellt insbesondere auf die Sicherung der IT von Organisationen vor Angriffen durch Personen ab, seien dies Hacker oder MitarbeiterInnen. Dagegen stellen die Aktivitäten des Datenschutzes insbesondere auf die Sicherung der Souveränität von Personen vor Angriffen von Organisationen ab. Im ersten Fall müssen sich deshalb Personen gegenüber Organisationen, im zweiten Falle müssen sich Organisationen gegenüber Personen als vertrauenswürdig erweisen.

Während heutzutage auf der Leitungsebene von Organisationen in der Regel keine Zweifel mehr daran geäußert werden, dass die Informationssicherheit unmittelbar im Interesse der Organisationen liegt, weil Geschäftsprozesse grundsätzlich zu schützen sind, trifft die technisch-organisatorische Durchsetzung des Datenschutzes vielfach auf Ignoranz oder Widerstand der Leitungsebene. Denn Datenschutz formuliert im Wesentlichen die Interessen von Betroffenen gegen die Geschäftsinteressen von Organisationen. Es besteht insofern ein struktureller Konflikt zwischen dem Schutzbedarf von Organisationen und dem Schutzbedarf von Personen, der deshalb rechtlich geregelt ist.

Dieser Unterschied in Perspektive und Motivation der Informationssicherheit und des Datenschutzes wurde bei der Umsetzung von Schutzmaßnahmen und Prüfungen in den vergangenen Jahren aus dem Auge verloren und nur noch selten thematisiert, mit negativen Folgen vor allem auf der Seite des Datenschutzes. Aufgrund aktueller Entwicklungen ist zu vermuten, dass sich dieses bislang auf Harmonie bedachte

1 Unabhängiges Landeszentrum für Datenschutz (ULD), Schleswig-Holstein, 24103 Kiel, Holstenstraße 98. E-Mail: martin.rost@datenschutzzentrum.de

Verhältnis von Informationssicherheit und technisch-organisatorischem Datenschutz neu justieren wird.

## *2.* Zum Verhältnis von Informationssicherheit und Datenschutz

Mit den Maßnahmen der Informationssicherheit können die operativen Einschränkungen und Kontrollen gegenüber Personen überwiegend technisch-organisatorisch gut durchgesetzt werden. Die Maßnahmen sind dabei, mit Ausnahme der von Bundesbehörden veranlassten, rechtlich bislang nicht eigenständig fundiert. Dagegen können Datenschutzmaßnahmen, die betriebliche Abläufe einschränken und zur Implementation von Sicherheitsmaßnahmen sowie deren Kontrolle führen, zwar rechtlich begründet werden, aber der Datenschutz verfügt bislang über keine ähnlich überzeugende Prüfmethodik wie die Informationssicherheit. Die Folge ist, dass technisch-organisatorische Sicherheitsmaßnahmen speziell für den Datenschutz von Personen zumeist nur punktuell wirksam durchsetzbar sind.

Diese beiden „über Kreuz liegenden" Schwächen zeigen sich in einer nicht hinreichend gegenseitig konturierten Praxis von Prüfungen und der Umsetzung von spezifischen Maßnahmen der Informationssicherheit und des Datenschutzes. So half der Bezug auf das Datenschutzrecht bislang dem IT-Sicherheitsbeauftragten Begründungen dafür zu finden, dass die Leitungsebene die Gelder für die Umsetzung von Schutzmaßnahmen bereitstellen muss. Folgerichtig wurden und werden immer noch Sicherheitsmaßnahmen zur Verbesserung der Informationssicherheit nicht aber spezifische Maßnahmen des Datenschutzes umgesetzt. Die methodisch überzeugenden und inzwischen weitgehend bekannten Prüf-Aktivitäten der Informationssicherheit, mit Methoden und Komponenten nach IT-Grundschutz, strahlen ihrerseits auf Datenschutz-Methodiken aus und helfen so im Gegenzug den Datenschutzbeauftragten, einige Anforderungen auch des technisch-organisatorischen Datenschutzes umzusetzen. Was dabei allerdings an spezifischen Datenschutzmaßnahmen tatsächlich in den letzten Jahren umgesetzt wurde oder immer noch umgesetzt wird, ist nicht klar absehbar. Man denke hier bspw. an die aus Datenschutzsicht in der Regel formulierte Anforderung nach gesteigerter Prüffähigkeit von Organisationen durch Dokumentation und Protokollierung oder die Forderungen nach Pseudonymisierung und Anonymisierung oder nach Verschlüsselung ausschließlich unter der Kontrolle des Nutzers. Diese Schutzmaßnahmen für Betroffene wurden im Rahmen des Identitätenmanagements von der EU gefördert und in den vergangenen zehn Jahren systematisch entwickelt, sie werden aber vom IT-Grundschutzkatalog nicht erfasst.[2]

Die Informationssicherheit bekommt nun nach und nach, auch in den Ländern und Kommunen, eine eigene gesetzliche Fundierung. Neben dem seit 2009 bestehenden, spezifisch auf die Belange des Bundes abgestimmten, BSI-Gesetz sowie den spezialgesetzlichen Regelungen im Rahmen des Neuen Personalausweises oder des

2 Hansen, Marit, 2008: Marrying Transparency Tools with User-Controlled Identity Management; in: Fischer-Hübner et. al., 2008: The Future of Identity in the Information Society, Springer US: 199-220.

DE-Mail-Gesetzes stehen in den Ländern E-Government-Gesetze vor der Tür bzw. liegen vor. Flankiert werden diese gesetzlichen Bemühungen von einer Informationssicherheitsleitlinie, die sich in wesentlichen Teilen an IT-Grundschutz orientiert und die der IT-Planungsrat für die gesamte deutsche Verwaltung verbindlich vorschreiben wird.[3] Und auch für den Privatbereich ist davon die Rede, dass die Bundesregierung bzw. das Innenministerium ein IT-Sicherheitsgesetz plant, das Mindeststandards für Betreiber kritischer Infrastrukturen vorschreibt.[4] Der Datenschutz auf der anderen Seite orientiert sich zunehmend an der Methodik von IT-Grundschutz, weist dabei allerdings über Grundschutz hinausgehend weitere spezifisch auf die Datenschutzperspektive zugeschnittene Schutzziele und Definitionen aus, die vornehmlich aus der Betroffenenperspektive formuliert sind und strukturell der Operationalisierung der datenschutzrechtlich zentral stehenden Anforderungen der Zweckbindung/ Zwecktrennung dienen.[5] Und auch das Datenschutzmanagement sucht Halt an Bewährtem, wenn es sich an die Prozesse der ISO 27001 anlehnt, die speziell an die Anforderungen des Datenschutzes angepasst sind.[6]

Durch diese gegenseitige Emanzipation von Informationssicherheit und Datenschutz in normativer und methodisch-operativer Hinsicht lassen sich deren Prüfperspektiven distanzieren und gegenseitig konturieren. Sicherheitsmaßnahmen der Informationssicherheit werden dadurch besser als bislang rechtlich gestützt und Schutzmaßnahmen des Datenschutzes können methodisch überzeugender als bislang systematisch geplant und geprüft werden.

Beide Disziplinen wirken gemeinsam darauf hin, dass Organisationen ihren Betrieb wirksam beherrschen und dieses auch gegenüber sich selber, den Betroffenen sowie den Aufsichtsbehörden, die stellvertretend das allgemein-gesellschaftliche Interesse formulieren, nachweisen können. Die Orientierung an Beherrschbarkeit und Gesetzeskonformität sind Voraussetzungen dafür, dass Organisationen und Personen einander vertrauen können. Ein solches „Systemvertrauen“ macht eine Gesellschaft effektiv.

Damit Personen Organisationen vertrauen können, darf aus Datenschutzsicht die notwendig personenbezogene Datenverarbeitung von Organisationen nur innerhalb eng gezogener Grenzen stattfinden können. Gerade weil Organisationen in der Regel die Mächtigeren sind und ein Interesse daran haben und vor allem in der Lage sind, Personendaten für sich selbst besonders vorteilhaft automatisiert zu verarbeiten, wenn sie sich nicht an die rechtlich gebotene Zweckbindung der Verarbeitung

3 Referententwurf E-Government-Gesetz des Bundes, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_EGov.pdf?__blob=publicationFile. Als Beispiel für ein bereits verabschiedetes E-Government-Gesetz: „Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (E-Government-Gesetz - EGovG)“, vom 8. Juli 2009.

4 So die Pressemitteilung vom 8.11.2012 in den Heise-News: http://www.heise.de/newsticker/meldung/Innenministerium-plant-IT-Sicherheitsgesetz-1746002.html

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

6 Siehe Fußnote 16.

personenbezogener Daten halten. Dabei geht es im Kern nicht darum zu regeln, wem die Daten „eigentlich“ gehören oder welche rechtliche Grundlage besteht. Entscheidend ist, dass der Zugang zu persönlichen Daten grundsätzlich das Risiko beinhaltet, dass Personen bis zum Verlust der Würde fremdbestimmt werden. Der Verlust an Würde kann sich aus einer grundrechtlichen Sicht bereits dadurch einstellen, weil ein Rechner automatisiert darüber entscheidet, ob bspw. ein Kredit bewilligt oder die Tür eines Raumes im Altersheim automatisiert verschlossen wird, weil dessen Bewohner einem intelligenten Überwachungsautomaten ungewöhnlich unruhig erscheint. Dass die Datenverarbeitung in solchen Anwendungsfällen sicher im Sinne der IT-Sicherheit zu gestalten ist, ist notwendig, damit keine zusätzliche Risikosteigerung durch technische Fehler oder unberechtigte Nutzung entsteht. Aber selbst beste IT-Sicherheit ändert nichts am Fortbestehen der Machtasymmetrie zugunsten einer Organisation.

Datenschutz kann es ohne Techniken der IT-Sicherheit nicht geben. Kryptomaßnahmen sind für beide Perspektiven funktional einsetzbar, auch wenn sie historisch zunächst für Anforderungen der IT-Sicherheit entwickelt und dann systematisch zunächst einseitig der IT-Sicherheit, die der Sicherung von Verfahren bzw. Geschäftsprozessen dient, zugeschlagen wurden. Insofern stellte sich hier schon frühzeitig die Frage: „IT-Sicherheit - für wen“?[7] Die grundrechtliche Beurteilung der Funktion von Kryptomaßnahmen hängt davon ab, welche Instanz die Kontrolle über die Herstellung und den Einsatz von Sicherheitsmaßnahmen hat und welche Schutzinteressen bei der Interaktion von Organisationen und Personen damit mehr oder weniger transparent letztlich durchgesetzt werden: Die der Organisationen, also der Behörden, Unternehmen oder Forschungsinstitute? Oder die der Personen, also der BürgerInnen und KundInnen, der PatientInnen und Individuen, der organisationsinternen Mitglieder bzw. MitarbeiterInnen?

## 3. Drei verschiedene Phasen der Prüfkultur

Nachfolgend werden drei Phasen im Verhältnis von Informationssicherheit[8] und technisch-operativem Datenschutz unterschieden. Die erste Phase beginnt Mitte der

7 So lautete der Titel eines Vortrags von Helmut Bäumler auf dem BSI-Kongress 1997, siehe: https://www.datenschutzzentrum.de/material/themen/divers/itsichfw.htm. Die Betrachtungsweise der „mehrseitigen Sicherheit“ (vgl. Müller, Günter; Pfitzmann, Andreas (Hrsg.), 1997: Mehrseitige Sicherheit in der Kommunikationstechnik, Band 1: Verfahren, Komponenten, Integration; Addison Wesley.) berücksichtigt die Sicherheitsinteressen aller beteiligten Parteien und vermutet potentielle Angreifer nicht nur „von außen“, sondern prinzipiell unter allen Beteiligten. Pauschal gewährtes oder abgefordertes Vertrauen wäre ein naiver Modus, der den Stärkeren begünstigt. Sicherheitsmaßnahmen, die unter dem Paradigma der mehrseitigen IT-Sicherheit entwickelt werden, müssen geeignet sein, Schutzziele auch gegenüber Verfahrensbeteiligten wirksam durchzusetzen. Da fängt dann Datenschutz im engeren Sinne an. Das Konzept der mehrseitigen Sicherheit setzt insofern auf den mündigen Bürger, der aufgeklärt seine Geschicke im Bereich seiner Sicherheitsbedürfnisse bzw. seines Privatssphärenschutz selbst in die Hand nehmen kann. Dies ist wiederum das Paradigma des „durch den Nutzer kontrollierten Identitätenmanagements“ (vgl. Hansen 2008 (siehe Fußnote 2)).

8 Informationssicherheit ist der aktuelle im Rahmen von IT-Grundschutz und ISO 27001 genutzte Begriff. Historisch wurden zunächst Begriffe wie Datensicherheit oder IT-Sicherheit verwendet. In einigen Ausführungen zur Informationssicherheit wird der technisch-operative Datenschutz der Informationssicherheit als eine Komponente untergeordnet. Wir präferieren die Markierung des Unterschieds.

60er Jahre, in denen Fachexperten von Organisationen anfingen, wesentliche Funktionen der Datenverarbeitung ohne IT-Kenntnisse zu nutzen. Sie reicht bis etwa zum Jahr 1995, als wiederum Laien vernetzte Rechner massenhaft nutzen konnten. Bis zu diesem Zeitpunkt war das Thema Sicherheit akademisch schon weit getrieben. Die Umsetzung realer Sicherheitsmaßnahmen und operativer Datenschutz geschah jedoch noch punktuell und mit Einzelmaßnahmen. Die zweite Phase dauerte etwa von 1995 bis 2010. In dieser Phase sind Informationssicherheit und Datenschutz in einer Art Notgemeinschaft darauf bedacht, die Probleme der Sicherheit der per Internet vernetzten Organisationen zu erkennen und das Schutzniveau insbesondere gegenüber organisationsexternen Angreifern zu steigern. Diese Phase ist insofern für den Datenschutz besonders bedeutsam, weil wesentliche Technologien der Privacy-Enhancing-Technologies (PET) entwickelt wurden, die spezifische Datenschutzanforderungen - wie bspw. die Wahrungen der Nutzerkontrolle bei Kryptoverfahren, Pseudonymität, Anonymität - technisch und organisatorisch umsetzen. Die dritte Phase ab etwa 2010 ist dadurch gekennzeichnet, dass sich die Aktivitäten im Sinne der Informationssicherheit und des technisch-organisatorischen Datenschutzes auf ihre spezifischen Schutzinteressen und deren Durchsetzung konzentrieren. Für Datenschutz geht es seitdem darum, bei Prüfungen nicht wie bislang primär und unmittelbar auf die Aspekte der Datensicherheit zu achten, sondern darüber hinaus auch die entwickelten Prototypen und Techniken zur Verbesserung des operativen Datenschutzes, man denke bspw. an nutzerkontrolliertes Identitätenmanagement, zur Anwendung in der Praxis zu bringen.[9]

### 3.1 Phase 1: Prüfen bis ca. 1995

Der Kontext: Die Bearbeitung der Themen der IT-Sicherheit von Organisationen ist nicht gesetzlich geregelt. Das Verständnis für die Relevanz von IT- und Datensicherheit entwickelt sich auf der Ebene der Organisationsleitungen zumeist langsam. Insbesondere Prozesse zur fortgesetzten Sicherstellung der Datensicherheit gelten vielfach als fragwürdige Kostenfaktoren. Zumeist agiert das Management unsicher, unentschieden, abwartend. Gefestigte Routinen gibt es für die Verfügbarkeitssicherung durch Backup und Restore sowie konventionelle physikalische Sicherheitsmaßnahmen zur Gebäude- und Objektsicherung, mit Zutrittskontrollen und Videoüberwachung. Faktisch zuständig kümmern sich die IT-Administration sowie technikaffine Datenschutzbeauftragte punktuell um die Fragen und Bearbeitung speziell der Sicherheit der IT-Infrastrukturen. Bei den Prüfmethoden der IT-Sicherheit nimmt der Einfluss durch Projektmanagement-Methoden zu, mit Orientierung an ersten Standards der NIST, der ISO und des DIN.

9 Beim Neuen Personalausweis müssen sich Organisation und Person vor dem Zugriff auf die Personendaten aufgrund eines Berechtigungszertifikates gegenseitig authentisieren. Und eine Organisation erhält erst dann ein solches Berechtigungszertifikat, nachdem es die Zweck gemäße Nutzung dieser Daten gegenüber einer Genehmigungsbehörde (Bundesverwaltungsamt) belegt hat. Das ist ein noch viel zu wenig beachtetes Beispiel dafür, wie Ansätze des PET in der Realität angekommen sind (siehe: Möller, Jan, 2012: Informationelle Selbstbestimmung mit dem elektronischen Identitätsnachweis; in: Peters, F./ Kersten, H./ Wolfenstetter, K.-D. (Hrsg.), 2012: Innovativer Datenschutz; 1. Auflage, Berlin, Duncker & Humblot).

Die Datenschutzbeauftragten sind formal zuständig, die Verfahren mit Personenbezug und die dafür genutzte IT zu kontrollieren. Die Organisationsleitungen agieren auf Anforderungen der Datenschützer typisch abwartend, reaktiv, uneingedacht, häufig bagatellisierend und abweisend. Die Datenschutzbeauftragten in den Betrieben oder der Länder und des Bundes gelten überwiegend als Technik-unkundige Modernisierungsverhinderer. Datenschützer prüfen vorwiegend die juristischen Inhalte der Verfahren, also die Rechtsgrundlagen (Gesetze, Verträge, Verantwortlichkeiten), die Zweckbestimmung und Zweckbindung/ Zwecktrennung, Erforderlichkeit, Löschfristen, das Vorhandensein geforderter IT-Dokumente. Auf der operativen Ebene werden punktuelle Einzelmaßnahmen getroffen wie bspw. die Abschottung von Räumlichkeiten und Regelung von Zugängen, Begrenzung der Zugriffe auf Systeme und Datenbestände, Trennung von IT-Systemen, Regelungen zur Passwortkomplexität, Möglichkeiten zur Nutzung von Verschlüsselung von E-Mails und Festplatten, Hashwertgenerierung/Hashwertvergleiche oder Zertifikatehandling. Auch liegen bereits umfangreiche Erfahrungen mit Virenscannern und Firewalls vor. Die Prüfung der IT geschieht anhand von IT-Dokumentationen und Protokollen, insbesondere bei Auftragsdatenverarbeitung und Fernwartung. Die Prüfmethodik hängt von zufällig vorhandenen Kompetenzen eines Datenschutzprüfers ab, etwa wenn dieser aus der Steuer- oder Finanzprüfung oder Revisionsabteilung stammt oder über spezifische IT-Kenntnisse etwa zu Betriebssystemen, Datenbanken oder Großverfahren wie bspw. SAP verfügt. Gearbeitet wird zumeist mit hauseigenen Checklisten, deren Aufbau sich häufig an der Abfolge von Phasen des Anhangs zu §9 BDSG orientiert.

Was sind die Folgen? Die Aktivitäten der Informationssicherheit und des technisch-organisatorischen Datenschutzes werden sowohl durch die Datenschutzbeauftragten als auch durch die Systemadministratoren erbracht, deren Interessen als weitgehend deckungsgleich gesetzt werden im Sinne von: Hauptsache es geschieht endlich etwas in Richtung Verbesserung der IT-Sicherheit. Es musste etwas gegen das externe Hackrisiko aus dem Internet und für die Verschlüsselung von E-Mails geschehen. Zugleich wird seitens der Datenschutzbeauftragten das strukturelle Risiko der IT-Sicherheit durch die Allmacht der Systemadministration nachdrücklich problematisiert. Auch werden erste datenschutzrechtliche Einschätzungen von Firewalls und Virenscanner formuliert, weil hier mit sicherheitstechnischer Begründung Zugriffe auf Kommunikationsinhalte und Verbindungsdaten geschehen. Dass IT-Sicherheit und technisch-organisatorischer Datenschutz nicht in einem schlichten Deckungszusammenhang stehen können, scheint punktuell immer wieder auf.

Fazit: Es bestand eine Kultur der normativ fundierten Betreuung der technischen Anforderungen der Informationssicherheit durch den Datenschutz.

### 3.2 Phase 2: Prüfen zwischen 1995 und 2010

Der Kontext: Die Relevanz von IT-Sicherheit haben die Organisationsleitungen zunehmend besser erkannt und fangen an, IT-Sicherheitsbeauftragte zu installieren. Der IT-Sicherheitsbeauftragte verdrängt bei der Analyse und Bearbeitung von

Sicherheitsanforderungen langsam den Technik-affinen Datenschutzbeauftragten. Dabei wird IT-Grundschutz auch außerhalb der Bundesbehörden zur faktischen Referenz für eine Praxis der Herstellung von Informationssicherheit in Deutschland, mit zunehmendem Einfluss bis in die EU. Die Festsetzung der zu treffenden Sicherheitsmaßnahmen wird methodisch getroffen, entsprechend der Feststellung des Schutzbedarfs bzw. anhand einer Gefährdungs- und Risikoanalyse. Die Herstellung der Sicherheit von IT-Systemen wird insofern zunehmend besser kontrolliert geplant, implementiert und betrieben. Es liegen um 2000 herum erste Erfahrungen mit Application-Level-Gateways und Intrusion-Detection-Systemen vor. Ab etwa 2007 machen zumindest Rechenzentren Erfahrungen mit standardisiertem Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001, das in den Demmingzyklus eingepasst ist und von systematischen Schutzzielebetrachtungen für Vertraulichkeit, Integrität und Verfügbarkeit geleitet wird. Maßnahmen und Prozesse der IT-Sicherheit werden in die standardisierten Prozesse bspw. von ITIL oder vereinzelt nach CoBIT eingepasst.[10] In den Grundschutzkatalog wird ein optionaler Datenschutzbaustein integriert, mit dem Datenschutz-Anforderungen gemäß „Anhang zu §9 BDSG“ abgearbeitet werden können.

Im Bereich des Datenschutzes kommt es zu einer Häufung von Datenschutzskandalen bspw. bei der Deutschen Bundesbahn oder bei LIDL sowie zu Datenlecks, die mit einer kurzen Renaissance des öffentlichen Interesses am Datenschutz, als einem gesellschaftlich relevanten Thema, einhergehen. Daraufhin wird im BDSG ohne Ambitionen ein wenig nachgeregelt. Weniger offensichtlich aber ebenso datenschutzrechtlich bedenklich sind die Big-Data-Aktivitäten dieser Jahre, wie bspw. die Entwicklung von Scoringverfahren bei Versicherungen, Banken und Auskunfteien. Im Februar 2008 verkündet das Bundesverfassungsgericht das Urteil zum Grundrecht auf Gewährleistung der Schutzziele Vertraulichkeit und Integrität informationstechnischer Systeme, weil das Grundrecht der Unverletzlichkeit der Wohnung im Bereich der IT einer objektspezifischen Präzisierung bedarf und den Anspruch von IT-Sicherheit auch für einzelne Personen grundrechtlich formuliert. Durch die globale Netzevernetzung treten weitere Themen hinzu, so internationaler Datenschutz etwa in Bezug auf die EU oder in Bezug zu den USA mit Selbstbindungskonzepten wie Safe Harbour. Nun bekommen auch Datenschutzbeauftragte, sofern sie initiativ werden, teilweise mehr Ressourcen zugestanden. Dadurch steigt der berechtigte Bedarf des Nachweises der Nachhaltigkeit von Datenschutzaktivitäten. Datenschützer agieren technikorientierter und insgesamt professioneller. Im Bereich der technisch-organisatorischen Maßnahmen werden zwischen 2000 und 2010 dezidierte Privacy-Enhancing-Techniken entwickelt, wie bspw. Anonymisierungstechniken, mehrstufige Pseudonymisierung oder anonyme Credentials, die dann im Konzept des „nutzerkontrollierten Identitätenmanagement“ zusammen geführt werden. Diese spezifischen Schutzmaßnahmen des Datenschutzes werden von der Praxis aber nicht aufgegriffen. Analog zum ISMS wird über

10 Die Nutzung eines standardisierten Projektmanagements zur organisationsweiten Umsetzung von Maßnahmen der IT-Sicherheit, etwa nach V-Modell oder nach PRINCE2, dürfte jedoch nach wie vor eine Ausnahmen sein.

Möglichkeiten der Umsetzbarkeit eines spezifischen Datenschutzmanagementsystems (DSMS) diskutiert. Als Prüfmethode wird die Anlehnung an Methoden der Informationssicherheit und des Risikomanagements gesucht, das Fehlen von entsprechenden Datenschutzprozessen kann jedoch mangels Soll-Vorgaben bei Prüfungen nicht beanstandet werden. Selbst Datenschützer sind aber nicht in der Lage, eine überzeugende Auskunft darüber zu geben, welche Eigenschaft ein Datenschutzmanagementsystem konkret aufweisen muss, das aus mehr als einem mit Checklisten ausgestattetem Datenschutzbeauftragten besteht. Es werden jedoch allgemeine Datenschutz-Policies wie „Privacy By Design“ übernommen sowie Auditierungsverfahren speziell für Datenschutz entwickelt. In den jungen Datenschutzgesetzen der neuen Bundesländer werden die technisch-organisatorischen Maßnahmen anhand von Schutzzielen organisiert, ohne dass diese etwa analog zum Vorbild von IT-Grundschutz methodisch genutzt werden.

Was sind die Folgen für das Verhältnis des technisch-organisatorischen Datenschutzes und der Informationssicherheit? Die Tätigkeitsprofile verschieben sich zueinander. Das Thema Informationssicherheit bekommt eigenes „Betreuungspersonal“, das methodisch Halt an den drei Schutzzielen der Sicherung der Verfügbarkeit, Integrität und Vertraulichkeit findet und mit Katalogen für entsprechende Schutzmaßnahmen versorgt ist. Datenschutz wird zu einem Thema einer empörten Öffentlichkeit, gerät methodisch jedoch zunehmend in die Defensive und muss bei Prüfungen der IT-vor-Ort faktisch vielfach die Konformität nach IT-Grundschutz auch als Konformität mit dem Datenschutzrecht akzeptieren. Der technisch-organisatorische Datenschutz bekommt mit PET zwar am Reißbrett entwickelte neue Schutzmaßnahmen spezifisch für Datenschutzanforderungen an die Hand, die aber praktisch irrelevant sind und, außerhalb eines relativ kleinen Auditbereichs, auch von keiner hinreichend kanonisierten Prüf- und Beratungsmethode begleitet werden. In methodisch überzeugender Weise sind Datenschutzanforderungen gem. Anhang §9 BDSG als lediglich optionaler Bestandteil in den IT-Grundschutzkatalog integriert. Ein Ansinnen, wonach Datenschutz normativ gestützt gerade auch die Maßnahmen der IT-Sicherheit bzw. der Informationssicherheit auf Grundrechtskonformität zu kontrollieren hat, ist angesichts dieser Situation unplausibel und wäre vor allem methodisch von Datenschutzaufsichtsinstanzen mehr als nur punktuell auch gar nicht einlösbar.

Fazit: Es wechselte die Führung in der Hoheit der Beurteilung und Gestaltung technisch-organisatorischer Maßnahmen: Die Datensicherheit betreut auch die Anforderungen des technisch-organisatorischen Datenschutzes, aufgrund methodisch überzeugender Konzepte in der Inkarnation insbesondere des IT-Grundschutzes des BSI.

### 3.3 Phase 3: Prüfen ab 2010

Der Kontext: Das Problem der Nutzung von Social Media wie Facebook und Google+ durch Mitarbeiter erreicht die Sicherheitsbehörden. Zu einem Teil sind diese Behörden Leidtragende der Entwicklung, etwa wenn Soldaten in Privatmitteilungen über Facebook militärtaktisch bedeutsame Anweisungen in Kriegsgebieten (indirekt)

verraten. Zu einem ungleich größeren Teil sind gerade Ermittlungsbehörden jedoch Nutznießer des Mangels an Datenschutz bei Social Media, weil sie sich Zugriff auf Vorratsdaten in einem historisch bislang ungeahnten Ausmaß verschaffen können. Im Privatbereich sind die Dämme der Zweckbindung der Datenverarbeitung durch Social-Media-Provider und deren Kunden faktisch vollends gebrochen. Datenschutz wird zu einem Thema erklärt, das Organisationen und Betroffen per Einwilligungen im Binnenverhältnis regeln können. Die Vorratsdatenspeicherung finanzieren die Unternehmen, der Zugriff durch die staatliche Exekutive ist jederzeit möglich.[11]

Die IT-Sicherheitsbeauftragten (IT-SiBen) sind in den Organisationen fest etabliert. Datenschutzbeauftragte sind sowohl Verbündete als auch Konfliktquellen, die IT-SiBen sind aber nicht mehr wie bisher auf die Kooperationsbereitschaft der Datenschutzbeauftragten angewiesen. Die IT-SiBen konsolidieren ihre Aktivitäten. Sie kommen wie die Datenschutzbeauftragten auch zunehmend in Kontakt auch mit den Inhalten von Verfahren, weil auch sie ein systematisches Interesse daran haben, dass Prozessverantwortlichkeiten fachlich korrekt festgelegt sind und differenzierte Schutzbedarfsprüfungen, die sich aus den Inhalten der Datenverarbeitung ergeben und finanzielle Auswirkungen haben, durchgeführt werden. Die Konsolidierung von IT-Sicherheitsmanagement und Grundschutz sowie die Integration in bestehende Prozessframeworks wird erfolgreich fortgesetzt. Organisationen verlangen nunmehr auch untereinander pauschal, dass sie den Mindestanforderungen an Informationssicherheit genügen und Compliance-Controlling-Prozesse aufgesetzt haben, wenn sie zusammenarbeiten (müssen). Der IT-Planungsrat nimmt seine Tätigkeit insbesondere zur Standardisierung der Kommunen und Länder übergreifenden Zusammenarbeit bei der elektronischen Datenverarbeitung auf und initiiert Prozesse zur bundesweiten Steigerung der Informationssicherheit in der öffentlichen Verwaltung, weitgehend ohne Bedarf an einem ernsthaften Kontakt zum Datenschutz.

In der Datenschutztheorie musste zunächst die Sicherung der Nicht-Verkettbarkeit als Operationalisierung der zentral stehenden datenschutzrechtlichen Anforderung der Zweckbindung/ Zwecktrennung herausgearbeitet und anschließend der Unterschied zur Sicherung des Schutzziels Vertraulichkeit geklärt sein.[12] Die Maßnahmen zur Umsetzung konditionierter Verkettungen von Datenverarbeitungsvorgängen wurden im Rahmen der Privacy-Enhancing-Technologies entwickelt. Seit 2012 enthält das Landesdatenschutzgesetz von Schleswig-Holstein als erstes den vollständigen Katalog der sechs Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit sowie Transparenz,

11 Dadurch entstehenden strukturelle Verwerfungen in den Märkten durch Kommunikationsmonopole, in der staatlichen Gewaltenteilung sowie in Bezug auf den monopolisierten Zugang zu sozialwissenschaftlichen Datensammlungen insbesondere von google und facebook (vgl. Rost, Martin, 2013: Zur Soziologie des Datenschutzes; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2, Februar 2013 (im Erscheinen)).

12 Frühzeitig formuliert in: Rost, Martin 2004: Nicht-Verkettbarkeit als Grundbegriff des Datenschutzes? Identitätsmanagement soziologisch beobachtet; in: Bizer, Johann; von Mutius, Albert; Petri, Thomas; Weichert, Thilo (Hrsg.), 2004: Innovativer Datenschutz 1992-2004, Wünsche Wege Wirklichkeit, Für Helmut Bäumler: 315-334.

Intervenierbarkeit und Nichtverkettbarkeit.[13] Diese Schutzziele gestatten die Entwicklung eines systematisch gewonnenen Katalog von technisch-organisatorischen Referenzmaßnahmen speziell für Datenschutzanforderungen, der Soll-Maßnahmen enthält, die mit den bei einer Prüfung festgestellten Ist-Maßnahmen verglichen und beurteilt werden können.[14] Diese Komponenten wurden im Standard-Datenschutzmodell (SDM) zusammengeführt. Das SDM ermöglicht eine systematische Planung, Implementation und einen Betrieb und dessen Prüfung von IT-gestützten Verfahren auf einem methodisch vergleichbaren Niveau zu IT-Grundschutz.[15] Ebenso nahe liegend ist die Implementation eines Datenschutzmanagementsystems analog zum Informationssicherheitsmanagementsystem nach ISO 27001 auf der Grundlage des SDM.[16]

Was sind die Folgen? Es kommt zu einer Separierung der Prüfinhalte und Prüftätigkeiten der Datenschutzbeauftragten und der IT-Sicherheitsbeauftragten. Gleichzeitig wächst das gegenseitige Verständnis für Methodikfragen und normative Argumentationen. Auf beiden Seiten zeichnet sich ab, dass man auf eine neue, qualitativ bessere Weise als bislang miteinander zusammenarbeiten muss. ISMS und DSMS müssen die Anbindung an ITIL- oder CoBIT-Prozesse sowie an das Qualitätsmanagement und die bewährten Formen des Controllings durch Key Performace Indicators, etwa im Rahmen einer Balanced Scorecard, oder die Nutzung von Key Risc Indicators, wie sie im CoBIT-Framework ausgebildet sind, suchen.

Die anstehende neue Justierung des Verhältnisses zwischen Informationssicherheit und technisch-organisatorischem Datenschutz ließe sich auf der methodischen Ebene dadurch erforschen, indem die Schutzziele einander konturierend in Zweierkonstellationen aufeinander bezogen werden, um bspw. den Unterschied zwischen der Anforderung einer „integren Transparenz“ und einer „transparenten

13 Grundlegend und vornehmlich theoretisch ausgerichtet: Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele - revisited; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358. Anhand einer kritischen Diskussion von „Privacy By Design“ und „Global Privacy Standards“ das Schutzzielekonzept konsolidiert und praktisch gewendet: Rost, Martin; Bock, Kirsten, 2011: Privacy By Design und die Neuen Schutzziele - Grundsätze, Ziele und Anforderungen; in: DuD - Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-35. Zur Vereinbarkeit der Neuen Schutzziele mit BDSG, LDSG-SH und dem Entwurf der EU-Verordnung: Bock, Kirsten; Meissner, Sebastian; 2012: Datenschutz-Schutzziele im Recht - Zum normativen Gehalt der Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 425-431.

14 Ein erster Entwurf für einen Katalog mit generischen Referenz-Datenschutzmaßnahmen: Probst, Thomas, 2012: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444.

15 Siehe Fußnote 5.

16 Was genau ein DSMS von einem ISMS übernehmen kann und welche inhaltlichen Unterschiede herauszuarbeiten sind, befindet sich aktuell in der Diskussion (siehe Quiring-Kock, Gisela, 2012: Anforderungen an ein Datenschutzmanagementsystem - Aufbau und Zertifizierung; in: DuD 2012/11, 36. Jahrgang, Heft 12: 832-836.) Ein auf Datenschutzanforderungen sehr viel spezifischer abstellender Vorschlag, bei dem die gute Prozessstruktur und Methodik der ISO 27001 mit dem auf den „Neuen Schutzzielen“ basierenden „standardisierten Datenschutzmodell“ verbunden wird, findet sich bei: Rost, Martin, 2013: Organisiertes Datenschutzmanagement, in: DuD - Datenschutz und Datensicherheit 2013/05, 37. Jahrgang (im Erscheinen).

Integrität“ zu klären. Die Sicherung einer „integren Transparenz“ wäre vermutlich eher ein Thema des Datenschutzes, der somit die Führung zur Lösung des Konflikts übernähme, während die Sicherung einer „transparenten Integrität“ eher ein Thema für die Informationssicherheit wäre.

In der praktischen Umsetzung muss der technisch-organisatorische Datenschutz zunächst mit der Nutzung von Tools zur Modellierung bzw. systematischen Prüfung von IT-Verbünden mit denen der Informationssicherheit gleichziehen. Dazu zählen auf der inhaltlichen Ebene zum einen UML- und BPM-Modellierungen, die vornehmlich unter datenschutzrechtlichen Aspekten zu prüfen sind. Dazu zählt aber auch die Nutzung eines Datenschutzmodellierungstools analog zum GS-Tool.[17] Sollte ein derartiges Gleichziehen auf der Methodik-Ebene mit IT-Grundschutz gelingen, stellt sich im Anschluss die Frage, wie sich eine Grundschutzmodellierung mit einer Datenschutzmodellierung rechnergestützt in Beziehung setzen ließen. Sollten die Datenschützer nicht in der Lage sein, derart methodisch gleichzuziehen, bleibt die Grundschutzmodellierung jedoch das weiterhin faktisch führende Risikobearbeitungsparadigma der Technik auch für Grundrechtsanforderungen. Aus grundrechtlichen Erwägungen heraus wäre die Datenschutzmodellierung vermutlich das führende Bewertungssystem.

Fazit: Das Verhältnis von Informationssicherheit und technisch-organisatorischem Datenschutz wird sich in der nächsten Zeit, auf der Grundlage jeweils gefestigter normativer und methodischer Selbstgenügsamkeit, neu justieren müssen. Ein schlichter Rückfall in die vorigen Dominanzstrukturen, wonach zuerst Datenschutz und anschließend Informationssicherheit führte, ist dabei unwahrscheinlich.

## 4. Fazit

Informationssicherheit und technisch-organisatorischer Datenschutz haben viele Jahre mit gegenseitigem Gewinn kooperieren können. Während sich die Methoden der Informationssicherheit und des technisch-organisatorischen Datenschutzes dabei angeglichen haben, haben sich die Gesetzesgrundlagen und Inhalte der Definitionen differenziert. Entsprechend lassen sich die Aktivitäten der IT-Sicherheitsbeauftragten von denen der Datenschützer zunehmend deutlicher jeweils zuspitzen und dadurch unterscheiden. Datenschutz sieht sich methodisch zunehmend besser in der Lage, auch die Maßnahmen der Informationssicherheit kritisch zu beurteilen, wobei sich die Maßnahmen der Informationssicherheit wiederum zunehmend besser auch ohne Bezugnahme auf Datenschutzrecht normativ rechtfertigen lassen. Eine systematische Neujustierung des Verhältnisses beider könnte auf der Basis einer gegenseitigen Profilierung der sechs elementaren Schutzziele untereinander gelingen.

17 Dazu läuft derzeit ein Projekt unter Beteiligung des ULD.