Zusammenfassende Schlussfolgerungen

Mit dem *Recht auf informationellen Systemschutz* wird ein *neues Paradigma* zur Gestaltung des Datenschutzrechts der Zukunft vorgeschlagen. Seine Entwicklung ging aus einer kritischen Hinterfragung einiger Kernannahmen des aktuellen Datenschutzrechts hervor. Das Recht auf informationellen Systemschutz überwindet einen die Komplexität reduzierenden Dualismus sowie den Monismus aktueller Datenschutzgesetzgebung und zielt darauf ab, *angemessene Regelungen für Personendatenflüsse innerhalb und zwischen pluralen gesellschaftlichen Bereichen* zu definieren. 2032

Damit setzt das neu vorgeschlagene Lösungskonzept an *sämtlichen der drei in dieser Arbeit vorgestellten Strukturmerkmalen des DSG* an: 2033

Der *Dualismus* wird zu einem ausdifferenzierten, pluralistischen System weiterentwickelt. Für das DSG wird somit der entgegengesetzte Weg, als ihn die DSGVO vorsieht, vorgeschlagen. Es geht um die Anerkennung von Pluralismus. 2034

Das Datenschutzrecht soll nicht mehr in erster Linie mittels *Generalklauseln* regulieren. Vielmehr sollen Vorgaben an Personendatenverarbeitungen systemadäquat definiert werden. Dies erfolgt mit dem Ziel, Systeme wie Subjekte zu schützen. Gesetzgeberisch wird mit Szenarien zu arbeiten sein, die evaluieren, welche Auswirkungen verschiedene Gestaltungsweisen von Datenflüssen resp. Vorgaben auf die Integrität der jeweils involvierten Gesellschaftsbereiche haben. Angemessen ist eine datenschutzrechtliche Gesetzgebung, wenn hinreichend konkret definierte Verarbeitungsvorgaben vorliegen und damit die Gestaltung der Personendatenflüsse die Integrität der betroffenen sozialen Kontexte bestmöglich respektiert. Erreicht wird dies durch die Anerkennung der pluralen Hintergrundkontexte von Personendatenverarbeitungen und -flüssen sowie durch einen ausdifferenzierten Einsatz diverser Gestaltungsoptionen datenschutzrechtlicher Vorgaben. Alle bislang bekannten Instrumente werden hierbei selektiv eine Rolle spielen. Keines der Instrumente, auch nicht die informierte Einwilligung, wird alleiniger Lösungsansatz sein können. 2035

Der *Subjektschutz*, der im bisherigen Datenschutzrecht als *Persönlichkeitsschutz* figuriert, wird ergänzt, indem als Schutzzweck des Datenschutzrechts der *Systemschutz* anerkannt wird. Es sind weder nur das Datensubjekt und die Personendaten als Quasi-Objekte noch die konkrete, invasive und in räumlichem Denken verhaftete Verletzungshandlung, die kognitiv im Vordergrund stehen. Vielmehr liegt der Fokus auf Personendatenflüssen innerhalb und zwischen Gesellschaftsbereichen. Bereits die potentielle Möglichkeit, das *Risiko* bestimmter Verarbeitungshandlungen kann (datenschutz-)rechtlich problematisch sein. Das Datenschutzrecht ist damit weiter aus einem deliktsrechtlichen Denken heraus- 2036

zulösen und pointiert in die Richtung eines Risikorechts zu entwickeln. Das Systemschutzparadigma verdrängt das Subjektschutzparadigma nicht. Vielmehr inkludiert der Systemschutz den Subjektschutz, der zu einem kontextuellen und damit sachlich ausdifferenzierten Schutz wird.

2037 Ein Recht auf informationellen Systemschutz geht davon aus, dass ein in Zukunft tragfähiges und wirkungsvolles Datenschutzrecht seine Garantenstellung für die *Integrität und Funktionstüchtigkeit von etablierten Institutionen, Systemen oder Kontexten der Gesellschaft* wahrzunehmen hat. Um dieses neu resp. erweitert definierte Schutzziel zu erreichen, ist anzuerkennen, dass es im Datenschutzrecht um die *angemessene Regelung von Datenflüssen* geht. Die Überzeugungskraft der Gestaltung von Personendatenflüssen misst sich an den Auswirkungen der Datenflüsse auf die Robustheit der involvierten Gesellschaftsbereiche. *Datenschutzrecht ist systemrelatives resp. akzessorisches Recht.*

2038 Personendatenverarbeitungen und -praktiken spielen eine zentrale Rolle bei der Frage, ob gesellschaftlich etablierte Institutionen – der Gesundheitsbereich, die Demokratie, der Sozialstaat, das Privatleben – stabil und geschützt bleiben oder ob diese erodiert werden. Ein generalklauselartiges, auf Formalismen (wie privacy policies) zurückgreifendes, am Subjekt- und Handlungsunrecht anknüpfendes Datenschutzrecht ist nicht in der Lage, den Subjektschutz, geschweige denn den Systemschutz zu gewährleisten. Das Datenschutzrecht muss als Garant der tragenden gesellschaftlichen Säulen eine gänzlich neue Bedeutungsdimension erlangen. Es handelt sich beim Datenschutzrecht keineswegs um ein losgelöstes, isoliertes und eigenständiges Rechtsgebiet, das nur wenige Expertinnen und Experten interessiert, sondern um ein Rechtsgebiet, das in essentieller Weise die Funktionstüchtigkeit der für die Einzelnen und deren Wohl bedeutsamen Institutionen gewährleistet.

2039 In dieser Arbeit wird eine *Theorie* entwickelt, die sich am *Facettenreichtum gesellschaftlicher Kontexte* orientiert. Im Zentrum steht die Erkenntnis, dass es im Datenschutzrecht um die Regulierung von Datenflüssen geht, eingebettet in ihre jeweiligen Landschaften.

2040 Der hier präsentierte Vorschlag für ein Datenschutzrecht der Zukunft weist *nicht* in die Richtung der Reduktion von Komplexität, sondern macht sich die unzähligen Möglichkeiten, Datenflüsse zu gestalten, zunutze und plädiert vor dem Hintergrund pluraler Verarbeitungskontexte für ausdifferenzierte Lösungen.

2041 Das in dieser Schrift freigelegte *Systemschutzparadigma* ist *kein Deus ex machina*. Vielmehr zeigte die Untersuchung, dass systemische Schutzerwägungen schon immer, wenn auch eher subkutan, angelegt waren. Erhärtet wurde die Theorie mit einer Vielzahl von Beispielen, vom Facebook-Skandal über die Volkszählung und von der Yellow Press über das Adoptionsrecht bis hin zur geheimen privat-

detektivischen Versicherungsobservation. Für die Entwicklung der Thesen und die Ausarbeitung des neuen Paradigmas waren verschiedene, etappenweise gewonnene Erkenntnisse erforderlich. Sie werden nachfolgend in Bezug auf ihre Systemrelevanz kompiliert:

2042 Der **erste Teil** dieser Schrift stand unter dem Titel «Vergangene Zukunft». Ein Blick auf historische und literarische Quellen mochte zunächst als anachronistisch und paradox für eine juristische Studie zu einem Rechtsgebiet erscheinen, das von modernen Informationsverarbeitungstechnologien, der Digitalisierung und dem Vertrauen in Erkenntnisse künstlicher Intelligenz herausgefordert wird. Doch diese rückwärts und seitlich gerichtete Betrachtung ermöglichte richtungsweisende Erkenntnisse für die rechtswissenschaftliche Untersuchung und das Datenschutzrecht der Zukunft. Die Analyse von *historischen, geschichtswissenschaftlichen sowie literarischen Quellen* generierte die *These*, wonach es im Datenschutzrecht um die Gestaltung von Personendatenflüssen geht und wonach die Verarbeitung von Informationen und spezifisch von Personendaten nachhaltigen Einfluss auf die Etablierung, den Schutz oder eben die Erosion von Institutionen hat.

2043 Das *erste Kapitel* mit dem Titel «Der geheime Schlüssel» wies den traditionsreichen und sagenumwobenen Geheimworten und Geheimhaltungspflichten die Schlüsselrolle zu, um neue Erkenntnisräume für das Datenschutzrecht zu eröffnen. Anhand zweier Märchen wurde sichtbar gemacht, wie durch Geheimworte und deren Ermittlung diverse soziale Güter erlangt oder verteidigt werden konnten (im Fall von Ali Baba Geld, im Fall von Rumpelstilzchen ein Kind). Solche Geschichten über Geheimworte resp. ihren Bruch rückten das Bild des Informationsflusses innerhalb oder zwischen verschiedenen Welten in das Zentrum der Aufmerksamkeit. Geheimnisse und daraus entspringende Pflichten zeigten sich als Instrumente der Blockade von Informationsflüssen, was sich anhand der alten Geheimhaltungspflichten im Gesundheitsbereich (Hippokratischer Eid), aber auch im Kontext der Kirche (Beichtgeheimnis) bestätigte. In heutiger Terminologie lassen sich diese Geheimhaltungspflichten als die ältesten datenschutzrechtlichen Vorgaben beschreiben. Die untersuchten Beispiele liessen zudem deutlich werden, dass das Rechtsgebiet, das heute Datenschutzrecht genannt wird, nicht nur einzelne Menschen, stattdessen ebenso Institutionen schützt. Dass es um Informationsflüsse geht, wurde weiter anhand von Gestalten, die als Informationsmittler figurieren, namentlich dem Diener, sichtbar.

2044 Das *zweite Kapitel* beschrieb, inwiefern Informationsverarbeitungen als «Herrschaftstechnologien» zum Einsatz kamen. Hier wurde belegt, wie alt systematische und systematisierende Personendatenerfassungen sind – von den biblischen Volkszählungen über das mittelalterliche Buch des Lebens bis hin zur Etablierung absolutistischer Staatsherrschaften (Philipp II. ging mit dem Titel «Papier-

könig» in die Geschichte ein). Derartige Herrschaftstechnologien mit ihren Verarbeitungsprozessen stiessen oft auf Widerstand (eine Genferin wurde inhaftiert, weil sie die Kreidenummerierung an ihrem Haus, welche auch der Personenerfassung diente, entfernte).

2045 Es folgte im *dritten Kapitel* eine Annäherung an den Begriff des «Privaten» und dessen Schutz. Nach einem Blick auf die Bedeutung der Freiheitsrechte für die Entwicklung des *Privatheitsschutzes* und die Herausbildung eines privaten Lebensbereiches im Privatbereich, der stark räumlich konzipiert wurde («my home is my castle»), wendete sich die Studie der Entwicklung der ersten Datenschutzerlasse zu.

2046 Der **zweite Teil** befasste sich unter dem Titel «Die drei Strukturmerkmale des DSG» mit der *Funktionsweise* des schweizerischen Datenschutzgesetzes. Es wurde gefragt, wie das DSG konzeptionell aufgebaut ist. Insofern wurden *drei tragende Säulen* herausgearbeitet, an denen das DSG auch nach seiner Totalrevision festhält. Immerhin bringt die Totalrevision neue Ansätze, womit die drei traditionellen Strukturmerkmale neu kontextualisiert werden.

2047 Im *vierten Kapitel* wurde der «Dualismus» als erstes Strukturmerkmal vorgestellt. Prägend für das schweizerische Datenschutzgesetz ist, dass Personendatenverarbeitungen durch öffentliche Stellen des Bundes anders geregelt werden als Personendatenverarbeitungen durch Private. Hieran ändert weder die Systematik des Gesetzes, beiden Bereichen einen gemeinsamen Teil voranzustellen, in dem auch die allgemeinen Verarbeitungsgrundsätze verortet werden, noch die Bezeichnung des DSG als Einheitsgesetz etwas. Markant wird die Differenzierung der Regelung für die beiden Bereiche anhand der entgegengesetzten Ausgangspunkte implementiert: Für den öffentlichen Bereich gilt ein prinzipielles Verarbeitungsverbot mit Erlaubnisvorbehalt. Die gesetzliche Grundlage ist hier von herausragender Bedeutung. Für den privaten Bereich gilt die prinzipielle Verarbeitungsfreiheit mit Schranken, die in erster Linie durch die allgemeinen Verarbeitungsgrundsätze gesetzt werden. Der Entscheid für ein dualistisches Regime, das Personendatenverarbeitungen durch Privatpersonen anders regelt als Personendatenverarbeitungen durch öffentliche Stellen des Bundes, war Ergebnis der politischen Kräfte. Namentlich wirtschaftsfreundliche Positionen führten dazu, dass die datenschutzrechtlichen Vorgaben stark divergieren und das Schutzniveau für den sog. privaten Bereich geringer ist als für den öffentlichen Bereich. Dualistische Regime können als Grobversionen eines datenschutzrechtlichen Systemschutzes bezeichnet werden, da sie die Differenzierungswürdigkeit zwischen verschiedenen gesellschaftlichen Bereichen anerkennen. Die Schweiz weicht mit der Totalrevision, ungeachtet des Übergangs der DSGVO zu einem monistischen Modell, nicht von ihrem Dualismus ab. Die Vorstellung, wonach die Schweiz ein

Recht auf informationelle Selbstbestimmung verankert, wurde in diesem Teil für den privaten Bereich als unzutreffend beurteilt.

Das *fünfte Kapitel* widmete sich dem «generalklauselartigen Regelungsansatz» als zweitem Strukturmerkmal. Insofern wurden die allgemeinen Verarbeitungsgrundsätze in den Dualismus eingepasst. Die Ausführungen in diesem Kapitel zielten zudem darauf ab, praxisrelevante sowie dogmatische Erkenntnisse zu den tragenden Verarbeitungsgrundsätzen zu generieren. Damit ging es auch darum, den für das Datenschutzrecht elementaren generalklauselartigen Vorgaben eine konkretisierende Struktur zu geben. Die Analyse der einzelnen Verarbeitungsgrundsätze förderte zu Tage, inwiefern sich in ihnen systemrelative Ansätze finden. Als ergiebig stellten sich die Analyse des Zweckbindungsgrundsatzes und in diesem Zusammenhang die Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil heraus. Das Urteil gilt als Magna Carta des Datenschutzrechts. Rezipiert wurden in erster Linie dessen subjektivrechtliche Dimension und das Grundrecht auf informationellen Subjektschutz. Das Urteil führt indes unmissverständlich den Systemschutz durch das Datenschutzrecht vor Augen: Nur wenn die Bürgerinnen und Bürger auf das Statistikgeheimnis vertrauen dürfen und Personendaten, die zum Zweck der Volkszählung erfasst werden, nicht zur Erfüllung anderer Verwaltungsaufgaben genützt werden, könne die Integrität der Statistik gewährleistet werden. Wenn die Bürgerinnen und Bürger dagegen befürchten müssten, dass von ihnen zum Zweck der Volkszählung erteilte Informationen z. B. zu Konsequenzen im Steuer- oder Migrationsbereich führen, wäre nicht mit wahrheitsgemässen und vollständigen Informationen zu rechnen. Verwaltungssanktionen könnten dies nicht verhindern. Nur eine strenge Zweckbindung, das Statistikgeheimnis sowie organisatorische Massnahmen würden das Funktionieren der statistischen Erhebung sicherstellen. Die Analyse der weiteren Verarbeitungsgrundsätze bestätigte die Bedeutung des Systemschutzes. 2048

Im *sechsten Kapitel* verengte sich der Fokus auf die Normierung des Datenschutzgesetzes für den privaten Bereich. Titelgebend für das dritte Strukturmerkmal war der «Persönlichkeitsschutz». Schutzobjekt der Normen des DSG für den privaten Bereich ist die Persönlichkeit, anknüpfend an Art. 28 ff. ZGB. In diesem Kapitel wurden die konkretisierenden Normen des DSG, Art. 12 ff. DSG resp. 30 ff. nDSG vertiefend dargestellt. Gezeigt wurde, dass die prinzipielle Verarbeitungsfreiheit in erster Linie durch die generalklauselartigen Grundsätze limitiert wird. Der Wille des Datensubjektes wird als Widerspruch oder als Rechtfertigungsgrund integriert. Das Regime wurde als Missbrauchsgesetzgebung taxiert, eine Qualifikation als Recht auf informationelle Selbstbestimmung verworfen. Diese Beurteilung wurde durch einen Blick auf das Recht am eigenen Bild und dessen Funktionsweise sowie durch eine Untersuchung der Einwilligungskonstruktionen im Biomedizinrecht erhärtet. Das DSG dagegen lehnt sich eng an die 2049

Mechanik von Art. 28 ff. ZGB an. Folglich ist das DSG vom *Subjektschutz,* dem *Persönlichkeitsschutz* geprägt. Damit handelt es sich um eine deliktsrechtliche und abwehrrechtliche Konstruktion.

2050 Der **dritte Teil** dieser Arbeit stand unter dem Titel «Vom Recht auf informationellen Subjektschutz zum Recht auf informationellen Systemschutz».

2051 Das *siebte Kapitel* knüpfte unter der Überschrift «Datenschutz auf dem Prüfstand» an die im zweiten Teil beschriebenen Strukturmerkmale an und analysierte, wie funktionstüchtig die Normierung durch das DSG ist. Das Ergebnis lautete, dass auch für die Schweiz zunächst von einem eigentlichen *Vollzugsdefizit* ausgegangen werden muss. Mit anderen Worten blieb und bleibt das DSG weitgehend toter Buchstabe, die faktische Verwirklichung und Umsetzung ist ungenügend. Die schwache Einhaltung des Gesetzes wurde im privaten Bereich insb. mit dem geringen Risiko von Konsequenzen begründet. Interventionen vonseiten des EDÖB oder individualrechtliche Klagen vonseiten der Subjekte sind nicht ernsthaft zu befürchten. Es folgte eine Auseinandersetzung mit den – wenigen – Urteilen zum Datenschutzrecht. Problematisiert wurde die *inkonsequente Definierung des Schutzobjektes* in datenschutzrechtlichen Fällen durch die Schweizer Gerichte. Ein Gesetz, in dessen Zentrum Generalklauseln stehen, ist auf eine strukturierende und konkretisierende Rechtsprechung angewiesen. Diese vermisst man in der Schweiz. Immerhin haben in den letzten Jahren Interventionen des EDÖB aufgrund von sog. Systemfehlern dem Datenschutzrecht Nachdruck verliehen. Auch wenn dieses Instrument zur Rechtsdurchsetzung des Datenschutzrechts mit der Totalrevision des DSG fallengelassen wurde, zeigte sich in ihrer Analyse erneut die systemische Dimension des Datenschutzrechts. Mit ihr wird anerkannt, dass ein ausschliesslich individualrechtlicher Ansatz im Datenschutzrecht, auch was die Durchsetzung desselben bei Verstössen anbelangt, ungenügend ist. Zudem wurde festgestellt, dass mit den jüngsten Urteilen, die einer Intervention des EDÖB vorangingen, das Datenschutzrecht und die Rechtsprechung hierzu eine Aufwertung erfahren haben. Gleichwohl ist zu attestieren, dass die Wichtigkeit des Datenschutzrechts in der Praxis von den Unternehmen ungenügend beachtet wurde. Wie intensiv das Thema die Informationsgesellschaft beschäftigt, zeigte sich anhand eines Schlaglichts auf die *mediale Berichterstattung* und die *politischen Debatten*. Hier wurde deutlich, dass der Datenschutz und das Datenschutzrecht gerade auch spezifisch für bestimmte Gesellschaftsbereiche verhandelt werden. Den Abschluss des Kapitels bildete ein Blick auf die Ursachenforschung bezüglich der Defizite des aktuellen Datenschutzrechts. Genannt wurden die ungenügenden Sanktionsrisiken sowie die mangelnde strukturierende Wirkung eines generalklauselartigen Datenschutzrechts. Ein zentrales Begründungsmuster wurde, in Einklang mit dem subjektivrechtlichen Ansatz des zeitgenössischen Rechts, in der Achtlosigkeit der Da-

tensubjekte verortet, denen angelastet wird, für Rabatte und die Nutzung von vermeintlichen Gratisdiensten ihre Personendaten zu kommerzialisieren. Sodann wurde gezeigt, dass für Schwächen des Datenschutzrechts pauschal der rasante technologische Fortschritt verantwortlich gemacht wird. Eine Evaluation dieser *Erklärungsmuster* ist von hoher Bedeutung. Nur wenn die Defizite in zutreffender und hinreichend präziser Weise identifiziert werden, sind Fortschritte zu ihrer Beseitigung im und durch das Recht denkbar. Folglich wurden in diesem Kapitel zwei Herausforderungen, die faktischer Natur sind, präziser dargestellt: erstens die *neuen Informationstechnologien* und zweitens die *Kommerzialisierungstendenzen*. Die *neuen Technologien* wurden anhand dreier Potenzen beschrieben: Tracking und Monitoring, Aggregierung und Analyse sowie Verteilung und Veröffentlichung resp. umgekehrt: Aufgreifen und Zugreifen. Diese drei Potenzen werden regelmässig miteinander kombiniert. Mit diesen Ausführungen konnte ein besseres und genaueres Verständnis der Funktionsweisen und Gefährdungspotentiale neuer Informationsverarbeitungstechnologien gewonnen werden. Unübersehbar wurde, dass allein das Bild von Informationsflüssen in Netzwerkstrukturen Ausgangspunkt datenschutzrechtlicher Analysen sein kann. Es ist deutlich besser geeignet, datenschutzrechtliche Herausforderungen abzubilden, als eine Vorstellung, die einem Datensubjekt Personendaten als Quasi-Objekte gegenüberstellt. Ähnlich wie die Chiffre des rasanten technischen Fortschritts wurde diejenige von «Daten sind das Gold des 21. Jahrhunderts» dekodiert. Bewusst wurde darauf verzichtet, einen weiteren zivilrechtlichen Beitrag zur Kommerzialisierung des Persönlichkeitsrechts zu leisten. Stattdessen wurde anhand einer *Stufenfolge* herausgearbeitet, inwiefern im Zusammenhang mit Personendaten *expandierende wirtschaftliche Begehrlichkeiten* zur Erosion anderer gesellschaftlicher Bereiche führen. Die Praxis von Kreditauskunfteien bildete eines der Illustrationsbeispiele.

Es folgte im *achten Kapitel* eine Analyse der «jüngsten Lösungsstrategien». Im 2052
Vordergrund stand hier die Präsentation der *legislativen Neuerungen*, namentlich der DSGVO, zudem der Totalrevision des DSG. Nachgezeichnet wurden die wichtigsten Entwicklungstrends: der lange Arm der DSGVO, aber auch des DSG in territorialer Hinsicht, der Ansatz diversifizierter Schutzziele trotz des Übergangs zu einem Monismus, der Ansatz der Stärkung der Rechtsposition des Datensubjektes, der Ansatz der faktischen Verwirklichung des Datenschutzrechts, der Compliance-, Governance- und Accountability-Ansatz, der risikobasierte Ansatz sowie der Ansatz der starken Behördenhand. Im DSG bedeutet die Integration mehrerer neuer Ansätze durch die Totalrevision, dass die drei Strukturmerkmale des bisherigen DSG eine neue Einbettung und damit eine neue Bedeutung finden werden. Es folgte eine Auseinandersetzung mit den wichtigsten der in der *Lehre diskutierten Ansätze*. Wie sich zeigte, kommt vorrangige

Bedeutung den im Subjektschutz basierten *Einwilligungskonstruktionen* zu. Sie werden sowohl *persönlichkeitsrechtlich* wie *eigentumsrechtlich* diskutiert, wobei die Begründung eines eigentlichen Herrschaftsrechts der Datensubjekte im Vordergrund steht. In die Gegenrichtung weist der *Anonymisierungsansatz*, bei dem das Band zwischen Datensubjekt und Personendaten nicht gestärkt, stattdessen gekappt wird. Bezüglich beider Lösungsansätze wurden *Einwände* diskutiert, denen zufolge beide Ansätze sowohl konzeptionell wie faktisch an ihre Grenzen stossen. Basierend auch auf diesen kritischen Einwänden wurde die Entwicklung eines neuen Paradigmas möglich.

2053 Das *neunte Kapitel* widmete sich der Theoriebildung für ein «Recht auf informationellen Systemschutz». Ausgangspunkt war eine Fallkonstellation zur geheimen Observation im (öffentlich-rechtlichen) Versicherungskontext. Die Analyse des Sachverhaltes, des Bundesgerichtsurteils sowie des anschliessenden Urteils des EMGR, EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, zeigte, dass sich die rechtliche Konfliktlage nicht in einem bipolaren und individualrechtlichen Konflikt erschöpft. Rechtlich problematisch ist nicht erst eine konkret durchgeführte Observation des Privatlebens einer IV-Beziehenden, getragen von wirtschaftlichen Motiven der IV-Versicherung. Vielmehr erodiert die Praxis – ungeachtet der Frage, ob sie gesetzlich vorgesehen ist oder nicht – bereits aufgrund der potentiellen Möglichkeit die Integrität des Privatlebens des Kollektivs der IV-Beziehenden, zudem die Integrität des Sozialversicherungskontextes und, im Zusammenhang mit der IV, die Integrität des Gesundheitsbereichs. Wenn Versicherungen aus wirtschaftlichen Motiven selbst bei nicht erhärtetem Betrugsverdacht die Expertisen des medizinisch zuständigen Personals systematisch in Frage stellen und medizinisch nicht geschulte Personen – in diesem Fall Detektive – mittels geheimer Observation eine Invalidität beurteilen sollen, wird nicht nur der Gesellschaftsbereich des Privatlebens erodiert. Die Praxis unterminiert zugleich die Integrität des Gesundheits- und Sozialversicherungsbereichs, indem sie die dort geltenden Ziele, Logiken und Rationalitäten durchkreuzt. Anhand des konkreten Falles wurde die *kollektive Dimension des Rechtskonfliktes* herausgearbeitet, wobei sich die Untersuchung systemtheoretische Ansätze zunutze machte.

2054 Das *Recht auf informationellen Systemschutz* ist ein *neues Paradigma* zur Gestaltung des Datenschutzes und des Datenschutzrechts der Zukunft. Seine Aufgabe wird sein, Flüsse von Personendaten ausdifferenziert so zu gestalten, dass die Robustheit von etablierten Teilsystemen unserer Gesellschaft garantiert wird. Das Datenschutzrecht der Zukunft kann nur ein systemadäquates Recht sein. Die systemische Dimension des Datenschutzrechts war zwar seit jeher in diesem angelegt; ihre Bedeutung wurde bisher aber nicht erkannt und folglich auch nicht anerkannt. Mit dem Recht auf informationellen Systemschutz wird das Da-

tenschutzrecht zum Garanten für die Integrität stabilisierter und stabilisierender gesellschaftlicher Bereiche. Es leistet einen Beitrag zum Schutz der Demokratie, des privaten und freiheitlichen Lebens, der Gesundheit, der Wissenschaft und Forschung, des Sozialstaats, des Arbeitskontextes usf. Indem das künftige Datenschutzrecht auf den Schutz gesellschaftlicher Systeme abzielt, wird es auch seinen Schutzauftrag gegenüber dem einzelnen Subjekt wahrnehmen können. Denn das *Recht auf informationellen Systemschutz inkludiert den informationellen Subjektschutz*. Erst damit wird das Datenschutzrecht all seinen Bedeutungsdimensionen gerecht. Erst damit wird das Datenschutzrecht seinen Schutzzielen – dem Schutz des Subjektes, aber auch dem Schutz etablierter Institutionen – wirksam Nachachtung verschaffen.