erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Martin Rost

Bob, es ist Bob!

Seit bestimmt zwanzig Jahren zählt es unter FIfFlern zum selbstgewiss-aufklärerischen Gestus, Nicht-Technikern mehr Interesse an der notorischen Unsicherheit von IT und dem ungenügenden Datenschutz abzuverlangen. Allerdings rechtfertigen viele Artikel in der FIfF-Kommunikation diesen selbstgewissen Gestus nicht, weil es den Autoren vielfach an analytisch bedeutenden Kenntnissen zum Datenschutz – im Unterschied beispielsweise zu Themen der IT-Sicherheit – mangelt. Was genau meint denn „Datenschutz"?

Die vielfach festzustellende Inkompetenz in Bezug auf Datenschutz ist insbesondere deshalb ein ernsthaftes Problem, weil das FIfF als „kritischer Berufsverband der Informatiker" (Wikipedia) im deutschsprachigen Raum in meinen Augen die politische Avantgarde unter den Informatiker.innen repräsentiert. Zwar werden in vielen Artikeln verlässlich Grundrechtsverstöße aufgelistet und beleuchtet, aber ein zweifellos notwendiges Skandalisieren allein ersetzt keine ernsthafte theoretische Befassung – wobei eine ernsthafte Beschäftigung sich wiederum auch nicht darin erschöpft, über eine detaillierte Orientierung im komplizierten Datenschutzrecht zu verfügen. Es drängt sich mir seit langem schon der Verdacht auf, dass ein, allerdings die gesamte Datenschutzszene durchziehender, Empörungsaktivismus den Mangel an ernsthaften analytischen oder theoretischen Diskussionen über Datenschutz verdeckt. Ich möchte nachfolgend ebenfalls einmal diesen selbstgewiss-aufklärerischen Gestus simulieren, den Spieß umdrehen und Ihnen mehr ernsthaftes Interesse für Datenschutz abverlangen.

Ich bitte Sie, dass Sie sich vor dem Weiterlesen selbst zwei Fragen beantworten:

1. Welcher zentrale Konflikt soll durch „Datenschutzrecht" geregelt werden?

2. Was unterscheidet Schutzmaßnahmen des Datenschutzes von denen der IT-Sicherheit? Notieren Sie sich doch bitte Ihre Antworten, vielleicht mit nur wenigen groben Stichworten. Dann können Sie sich selber davon überzeugen, wie schlüssig Ihr Wissen zum Datenschutz ist.

These 1: Datenschutz nimmt nicht den Schutz von Privatheit zum Ausgangspunkt der Bestimmung, ebenso wenig wie den Schutz von Freiheit, Autonomie und Selbstbestimmung einer Person. Auch nicht der Schutz der Rechte von Betroffenen und noch viel weniger irgendwelche Vorstellungen von Privacy, die mal so oder mal so und mal auch ganz anders oder gar nicht ausfallen können, bilden den Ursprung des Datenschutzes. Und auch die Differenz „öffentlich/privat" erzeugt nicht den wesentlichen Datenschutzkonflikt. Datenschutz nimmt vielmehr die Risiken erzeugende Machtasymmetrie zwischen Organisationen und Personen zum Ausgangspunkt. Das Datenschutzrecht und die technischen und organisatorischen Datenschutzaktivitäten sind bereits Formen des Unterbedingungstellens (Konditionierung) dieses strukturellen Machtkonflikts in modernen Gesellschaften. Welche Rolle dabei Recht und Technik für diese im Rechtsstaat notwendige Konditionierung der Machtasymmetrie spielen, möchte ich nachfolgend erläutern.

Auf der einen Seite stehen die mächtigen Organisationen als Risikogeber – hier denke man paradigmatisch als erstes natürlich an den Staat, aber nicht nur. Auf der anderen Seite befinden sich die von Organisationen abhängigen Personen, denen durch die Organisationen die Rolle als Risikonehmer aufgebürdet wird. Risiko meint hier: Organisationen erzeugen durch die von ihnen betriebenen personenbezogenen Verfahren Risiken, die es ohne diese Verfahren für die Personen nicht gäbe. Dieser Konflikt ist der Ursprung der regulativen Idee des Datenschutzrechts. In den 70er-Jahren hatten Datenschützer.innen vornehmlich den Staat vor Augen, heute sind es vor allem die global agierenden Unternehmen, die von keinem Leviathan gebremst werden. Von Technik ist hier noch überhaupt keine Rede. War Ihnen dieser kristallklare Gedanke der Konditionierung von Machtasymmetrie zwischen Organisationen und Personen als Gegenstand des Datenschutzrechts als Antwort in den Sinn geschossen oder haben Sie ihn vielleicht sogar notiert? Nein? Sehen Sie! Ja? Dann heiße ich Sie willkommen in Level 2, das sogleich folgt.

Was heißt jetzt „Konditionierung der Machtasymmetrie"? Das verfasste Rechtsstaatsversprechen, das im Datenschutzrecht

zum Ausdruck kommt, besteht darin, dass die Relation zwischen einer jeden Organisation und den mit ihr verbundenen Personen unter Bedingungen steht oder gestellt werden kann. Diese Beziehung soll jedenfalls nicht „naturwüchsig", sondern rechtlich und operativ vernünftig geformt zugänglich sein. Für eine vernünftige Form der Beziehung zwischen Organisationen und Personen müssen Organisationen die Kriterien natürlich kennen, anhand derer sie ihre Verfahren auszugestalten haben. Diese Kriterien sind Gesetze und letztlich die Grundrechte. Wenn Personen den ihre Daten erhebenden und verarbeitenden Organisationen dagegen ausgeliefert sind, wie es bspw. bei Usern gegenüber Facebook, Google, Apple, Microsoft, Cisco, IBM, Akamai, Telekom, Vodafone … der Fall ist – und ebenso bei Bürger.innen gegenüber der öffentlichen Verwaltung und den Sicherheitsbehörden oder bei Patient.innen gegenüber dem Krankenhaus – dann ist das eine soziale Konstruktion, die immer auch anders, sowohl rechtlich als auch prozessual oder technisch, gestaltet sein könnte. Datenschutz prüft solche Konstruktionen der Organisationen gegenüber Personen anhand der Anforderungen der Verfassung. Datenschutz bezeichnet insofern all diejenigen Vorkehrungen, die auf Seiten der Organisationen zu treffen sind, um die Machtasymmetrie zwischen Organisationen und Personen so zu formen, dass Personen vor der Willkür der Organisationen geschützt sind oder sich schützen können.

Dass Personen ihre Daten und Identitäten ohne Anker in Organisationsprozessen selbst kontrollieren können, ist in diesem Sinne bspw. keine Datenschutzmaßnahme. Vorstellungen zu „Selbstdatenschutz" werden in der Datenschutzszene im Kontext der „Privacy-Enhancing-Technologies" seit Ende der 90er-Jahre diskutiert. Selbst-Datenschutz in Bezug auf IT ist allerdings eine reine Fiktion, weil ein Nutzer immer auf die Nutzung schon funktionierender Techniken, die letztlich von Organisationen her- oder bereitgestellt werden, angewiesen ist. Ein tatsächlich über alle Layer hinweg wirksamer privater Selbstschutz vor übergriffig agierenden Organisationen ist unmöglich. Der Sicherheitsanker liegt insofern in den gesellschaftlichen Strukturen, nicht in den Personen. Datenschutz muss deshalb, mit gesellschaftlicher Strukturperspektive ausgestattet, primär auf Schutzvorkehrungen für Personen auf Seiten der Organisationen hinwirken.

Im Schatten eines starken Staates, der Grund- und Bürgerrechte gewährt, kann im Prinzip zwischen allen adressierbaren Einheiten eines Staates Augenhöhe hergestellt werden. Ein starker Staat ist dabei sowohl der einzige Garant für die wirksame Durchsetzung von Grundrechten als zugleich der stärkste Angreifer auf genau diese Grundrechte, die er gewährt. Ist Ihnen diese Dialektik einer solchen Gleichzeitigkeit von Garant- und Angreifer-Rolle geläufig? Denken Sie dabei an das Arzt-Patient-Verhältnis: Niemand kann Sie, wenn Sie bspw. schwer verletzt sind, so legal töten wie Ärzt.innen, die jedoch zugleich die einzigen sind, die Sie überleben lassen werden.

Privatheit und informationelle Selbstbestimmung, die im Datenschutz natürlich eine wesentliche konzeptionelle Rolle spielen, sind Eigenschaften sozialer Beziehungen, die aber erst dann entstehen können, wenn Organisationen nicht zuvor schon in Bezug auf Personen übergriffig agiert haben. Dass wenige Organisationen das Leben der Menschen unmittelbar „durchformen", ist dabei soziologisch der zentrale Indikator einer vormodernen Gesellschaft. Die Organisationen einer Gesellschaft sind immer schon da, ganz gleich, welchen Bedarf nach Autonomie, Privatheit und Rebellion Personen innerlich spüren. Privatheit für jedermensch und Abfordern von Selbstbestimmung sind insofern Eigenschaften sozialer Strukturen, die nur unter voraussetzungsvollen Umständen historisch entstehen können. Sie kennzeichnen die allerjüngste Moderne, die konkret durch eine „funktionale Differenzierung" (Niklas Luhmann) charakterisiert ist. Diese funktionale Differenzierung sozialer Systeme, in der es keine logische Ordnung der Dinge aus einem Punkt heraus mehr gibt, erzwingt von Personen, dass diese im Modus der Selbstbestimmung mit dem „Zwang zur Individualisierung" (Norbert Meuter) agieren – ein Modus, den einzunehmen sich in modernen Gesellschaften niemand frei aussuchen kann. Was ist mit „Zwang zur Individualisierung" gemeint? Es gibt heute keine Kleiderordnung mehr, außer bei betont autoritären Organisationen. Man wählt als Bürger politische Programme oder Personen und heiratet nach eigenen Überzeugungen und Gefühlslagen, man sucht sich unter 3.000 verschiedenen Studiengängen einen passenden in Abu Dhabi aus; man kann versuchen, einfach und sinnlich zu sein oder seinen Körper zu betonen oder in die Ausbildung seines Witzes, seines Intellekts, seiner Spiritualität oder seines Geschmacks zu investieren. Wie Personen sich gestalten, ist insofern offen kontingent. Aber dass man in diesen und einer Großzahl weiterer Parameter zu Lösungen der Lebensgestaltung kommen muss, die dann eben zwangsläufig für jede Person zu einer einmaligen Konstellation führen, ist in der Moderne nicht freigestellt. Es besteht Wahlzwang. Wie dürfen Organisationen sich dann noch anmaßen, formend in die Lebensgestaltung einzugreifen? Aber genau das tun sie, wieder mehr denn je. Individualität zu beanspruchen ist damit so wenig eine Privatangelegenheit wie auch Datenschutz es nicht ist.

Ich möchte Ihnen eine Zwischenfrage stellen: Was sind eigentlich Grundrechte? Ja, genau, Grundrechte, also etwa im Unterschied zu Menschenrechten und Bürgerrechten? Also die, die typischerweise gleich im ersten Semester eines Jurastudiums behandelt werden. Und die, die den Maßstab für Datenschutz bilden. Notieren Sie sich doch wieder mal Ihre Antwort auf diese Frage! Was sind Grundrechte und wie unterscheiden sich diese von den anderen Rechten? Die Antwort zu finden gebe ich Ihnen als Hausaufgabe mit auf den Weg.

Und gleich noch eine weitere Zwischenfrage: Wie lautet DIE ohne jeden Zweifel zentrale Regelung im kontinental-europäischen Datenschutzrecht? Sie verstehen gar nicht, worauf die Frage hinausläuft? Ich behaupte, das kann man als Bürger.in durchaus wissen. Falls Ihnen die Antwort in den Sinn schießt, was ich sehr hoffe, dann sind Sie vielleicht auch noch in der Lage, den Artikel des BDSG oder der Datenschutz-Grundverordnung zu nennen, in dem diese zentrale Regel, die zweifellos so alternativlos und klar wie die Deny-All-Regel bei einer Firewall-Administration ist, notiert ist? Diesen Artikel könnte man doch mal so auswendig lernen wie den ersten Artikel der EU-Grundrechte-Charta. Kennen Sie den Wortlaut des ersten Artikels der EU-Grundrechte-Charta? Meine Erfahrungen aus einer Großzahl an Datenschutz-Schulungen der letzten Jahre zeigt, dass viele Expert.innen zu Fragen der IT-Sicherheit und auch des Datenschutzes diese einfachen Fragen zum Datenschutzrecht nicht beantworten können. Es stimmt selbstverständlich: Man muss Bürger.innen mehr Kenntnisse bzgl. IT-Sicherheit abverlan-

gen, man muss allerdings von politisch engagierten Informatiker.innen auch konkrete Kenntnisse bzgl. Grundrechte und deren wirksame Umsetzung verlangen können. Die Praxis besteht eben nicht nur aus Technik und Betriebswirtschaft.

Sie können nun wiederum an Ihren Aktivitäten ablesen, wie ernst es Ihnen in Bezug zum Datenschutz tatsächlich ist, wenn Sie nach den Ihnen fehlenden Antworten zu den obigen Fragen zu recherchieren beginnen (oder eben nicht). Wenn Sie bei dieser Gelegenheit an die EU-Grundrechte-Charta geraten, schauen Sie doch gleich auch noch mal in Artikel 7 und vor allem in Artikel 8.

Deshalb nun zurück zur eingangs angekündigten Frage nach dem Unterschied zwischen operativem Datenschutz und IT-Sicherheit. Wie wäre es wieder mit ein paar groben Notizen, in denen Sie den Unterschied zwischen operativem Datenschutz und IT-Sicherheit notieren?

These 2: Ausgangspunkt für den operativen Datenschutz ist nicht die notorische und sinnfällige Unsicherheit der IT, die bei der Verarbeitung personenbezogener Daten zum Einsatz kommen mag. Ausgangspunkt für operative Schutzmaßnahmen des Datenschutzes ist stattdessen die Eingriffsintensität der personenbezogenen Datenverarbeitung einer Organisation. Fragen der IT-Sicherheit oder zum systematischen Ausnutzen technischer Schwachstellen durch Organisationen stellen sich erst in zweiter Linie. Denn zuallererst gilt: Jede Verarbeitung personenbezogener Daten durch eine Organisation stellt für eine davon betroffene Person einen Grundrechtseingriff dar.

Über den vorigen Satz kann man leicht hinweglesen, so im Modus des „ja, ja, ist klar". Das sollten Sie jedoch nicht tun; lesen Sie ihn bitte noch einmal. Dieser Satz enthält das Paradigma des operativen Datenschutzes.

Um es mit anderen Worten noch einmal darzulegen: Allein der Umstand der Verarbeitung personenbezogener Daten erzeugt eine riskante Machtasymmetrie zu Ungunsten der davon betroffenen Person. Das ist der Konflikt, auf den ein ernstzunehmender Datenschutz zu reagieren hat. Der operative Datenschutz nimmt deshalb jene Schutzmaßnahmen zum Gegenstand, die die Eingriffsintensität – oder den Grad der Beeinträchtigung, wie es in der ab Mai 2018 geltenden Datenschutz-Grundverordnung heißt – einer Datenverarbeitung mindern sollen. Dazu zählen dann bspw. Techniken, mit deren Hilfe die Datenverarbeitung, insbesondere mit Blick auf die Wirksamkeit von Schutzmaßnahmen, (über)prüfbar wird. Wie wird Prüfbarkeit – also eine Bilanzierung von Soll-Vorgaben, die dem Gesetz zu entnehmen sind, und Ist-Feststellungen, die durch Beobachtung von Verfahrenseigenschaften entstehen – im Datenschutz hergestellt? Ein Verfahren, und die dabei genutzte Datenverarbeitung, muss im Hinblick auf die Herstellung von Prüfbarkeit spezifiziert werden (auf die Zukunft des Verfahrens gerichtet), muss mit allen Daten, IT-Komponenten und Prozessen dokumentiert werden (Ausweis der Methode zur Feststellung von Ist-Zuständen des Verfahrens mit Referenz auf die Soll-Werte) und das Verfahren muss protokolliert werden (auf die Vergangenheit gerichtet). Außerdem zählen hierzu Techniken, die vor allem funktional den Zweck der Datenverarbeitung durch das Einziehen von Grenzen einschränken, indem bspw. einzelne Verfahren, und jeweils deren Datenbestände, IT-Systeme oder Prozesse, unterschieden werden und nur eng am Zweck orientiert zum Einsatz kommen.

Die Transparenz bzw. die Prüfbarkeit eines Verfahrens ist kein Selbstzweck, denn Transparenz entfaltet allein noch keine Schutzwirkung für betroffene Personen. Prüfbarkeit stellt Transparenz her, um beurteilen zu können, ob die Maßnahmen zur Minderung der Eingriffsintensität angemessen wirksam sind. Ein Beispiel für eine solche Maßnahme zur Minderung einer Eingriffsintensität ist das Setzen von Grenzen für ein Verfahren bzw. dessen Datenverarbeitung. Was heißt „abgrenzen" oder „trennen"? Und wie durchlässig muss eine „Grenze" für ein Verfahren trotzdem sein?

Gesetzt sei der Fall, dass Sie die drei Gewalten – die drei Gewalten haben Sie drauf, da habe ich jetzt keine Zweifel – im gleichen Landesrechenzentrum rechnen lassen. Dass die verschiedenen Gewalten auf einer gemeinsamen IT-Infrastruktur rechnen lassen, ist heute vielfache Praxis, obwohl ein Landesrechenzentrum – man kann alternativ auch an irgendwelche Clouds denken – einen operativen Kurzschluss zwischen den Gewalten bildet. So kann bspw. in einer Clearingstelle oder einer anderen architektonisch zentralen Stelle für die zentrale Vermittlung von Datenpaketen der Enterprise-Service-Bus (ESB) von Microsoft zum Einsatz kommen. Aus Datenschutzsicht stellt sich angesichts einer solchen Vermittlungsarchitektur, die bei einem Verfahren zum Einsatz kommt, die Frage: Ist anhand der Spezifikation, Dokumentation und Protokollierung des ESB prüfbar, wie die Trennung der Gewalten sichergestellt ist? Oder verallgemeinert gefragt: Welche Systemgrenzen sind auf welchem Layer eines Verfahrens wirksam? Bei einem Landesrechenzentrum kann man immerhin solche Aspekte noch prüfen, bei typischen Cloudlösungen kann man jedoch diesbezüglich gar nichts mehr prüfen. Wieder zeigt sich: Ausgangspunkt des Datenschutzes ist die Konditionierung der Machtasymmetrie, die nicht auf der operativen Ebene unterlaufen werden darf und die erst einmal noch gar keine typischen Probleme der IT-Sicherheit betreffen.

So, und wie ist es nun um die IT-Sicherheit bestellt? Um potenziell angreifende Hacker kümmern sich inzwischen die Kolleg.innen aus dem IT-Sicherheitsmanagement. Das IT-Sicherheitsmanagement ist schon vor nunmehr gut zehn Jahren zu einer mächtigen Abteilung innerhalb vieler Organisationen aufgestiegen. Den wenigsten Organisationsleitungen muss man immer noch erklären, dass ihre Organisationen über Kronjuwelen

Martin Rost

Martin Rost ist stellvertretender Leiter des Technikreferats des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

verfügen, die sie absichern sollten. Und sie wissen inzwischen auch, wie unsicher das Betreiben von IT ist. Die Schutzmaßnahmen nehmen dann die Sicherheit von Geschäftsprozessen in den Blick, nicht die Sicherheit der Betroffenen vor den Aktivitäten der Organisation selber. Außerhalb der kritischen Infrastrukturen (Stichwort „KRITIS") sind Organisationen nicht gesetzlich verpflichtet, eine sichere IT zu betreiben, abgesehen aus Gründen des Datenschutzes! Wenn eine Organisationsleitung sich dann doch einmal sperrt und keine Gelder bereitstellen will, muss man sich als IT-Sicherheitsbeauftragte.r manchmal auf Datenschutzgesetze berufen. Mit der Folge, dass dann Sicherheitsmaßnahmen, die nicht dem Schutz der Betroffenen dienen, betrieben werden. Der Schutz der Betroffenen wird innerhalb der IT-Sicherheit allenfalls als Compliance-Risiko gelistet. Das heißt, Organisationen interessieren sich für Datenschutz nur insoweit, als dass sie kalkulieren, welche Kosten mit Datenschutzverstößen einhergingen (und wie groß das Risiko ist, dass diese Verstöße bspw. von einer Datenschutzaufsichtsbehörde festgestellt werden). Deshalb muss man als Datenschützer.in gerade den IT-Sicherheitsbeauftragten immer wieder darlegen, dass Schutz zuvorderst den Betroffenen zu gelten hat und somit auch die Maßnahmen der IT-Sicherheit den grundrechtlichen Anforderungen zur Minderung der Eingriffsintensität genügen müssen. Insofern gilt zweifellos: Grundrechtlich müssen Maßnahmen des Datenschutzes die Maßnahmen der IT-Sicherheit dominieren! Aber haben Sie schon einmal als Datenschützer.in versucht, über diesen Konflikt mit der Organisationsleitung oder einem IT-Sicherheitsbeauftragten zu sprechen?

Klar ist: Ein Datenschützer, der keine Konflikte hat, macht seinen Job nicht. Ganz gleich, ob im Betrieb oder als Landesdatenschützer. Denn die Organisation, für die man als Datenschützer.in arbeitet oder mit der man zu tun hat, ist … die Hauptangreiferin. Das bleibt eine Organisation selbstverständlich auch bei einem rechtskonformen Betrieb, bei dem ausnahmsweise auch mal die Einwilligungen von Betroffenen keine Farce sind und wo der IT-Betrieb zudem eine gute Informationssicherheit aufweisen mag. Viele betriebliche Datenschützer.innen dienen sich allerdings, allein weil ihnen ihre Aufgabenstellung gar nicht klar vor Augen steht, ihren Organisationen als (allerdings zumeist wenig kompetente) Sidekicks der Sicherheitsbeauftragten an.

Was folgt nun aus alldem theoretisch und politisch? Ich spreche nachfolgend drei typische Figuren an, die nicht nur in FIfF-Artikeln der letzten Monate angesprochen wurden.

Zum Beispiel folgt aus der Erkenntnis über die durch Organisationen erzeugten Machtasymmetrie, dass Algorithmen keine Schuld für irgendetwas haben können, wenn etwas schief oder falsch läuft. Es sind immer die Organisationen (nicht: die einzelnen Mitarbeiter.innen), die die Algorithmen erschaffen, von einfachen Artefakten bis zur vernetzt-komplexen Künstlichen Intelligenz (KI), und die so nicht zuletzt auch ihr personales Inventar mit Motiven aufladen und damit irgendein „Schuldverhältnis" überhaupt erst erzeugen. Technik hilft Organisationen, die Machtasymmetrie zu reproduzieren, zu festigen, auszubauen.

Üble Nebelschwaden entstehen auch durch poppiges Gerede über Algorithmen-Ethik oder Datenschutz-Ethik. Die Unterstellung, dass man aufgrund eines starken technischen Wandels ja einfach nicht wissen könne, wie neue Techniken einzuhegen sind, und die daraus folgende Empfehlung, sich deshalb lieber an wolkigen Ethik-Diskursen zu versuchen – anstatt bestens legitimiert geltendes Recht zu vollziehen –, bedient allein und ausschließlich die Interessen der starken Organisationen, denen Grundrechte und Datenschutz im Weg stehen. Eine Dauerüberwachung von Menschen durch Handys oder lauschende Assistenzsysteme in den Wohnungen ist mit der EU-Grundrechte-Charta nicht vereinbar, eine wirksame Datenschutzaufsicht würde das auch feststellen. Wenn der Grundrechtseingriff durch ein Verfahren nicht durch Schutzmaßnahmen auf ein grundrechtlich akzeptables Niveau minimiert werden kann, darf das Verfahren von der Organisation nicht eingesetzt werden. Wer Ethik zur normativen Regulation solcher Datenschutz-Konflikte empfiehlt, untergräbt das bestehende Datenschutzrecht, und das nützt den Organisationen. Die Motive der Organisationen, die solche invasiven Techniken entwickeln und nutzen, wandeln sich ja genau gar nicht, sondern werden durch die Nutzung von neuen Techniken im Gegenteil besser denn je zementiert. Und auf diese Aktivitäten richtet sich das Datenschutzrecht: Es geht den Organisationen nach wie vor und weiterhin um die Stabilisierung einer optimalen Kapitalverzinsung, auch durch Verfügungsgewalt über Personen. Es geht weiterhin um Machterhalt und Machtausbau in Bezug auf die Herstellung der öffentlichen Ordnung oder um Wahrheitskonstruktionen, denen sich niemand verschließen können soll. Das Datenschutzrecht zielt darauf ab, dass keine naturwüchsigen Herrschaftsformen en passant mit Hilfe von Technik durchgesetzt werden, die Demokratie, Rechtsstaat, Markt und freie Diskurse unterlaufen.

Und auch die irgendwie richtig erscheinende Forderung nach Datensouveränität mit der Vorstellung „meine Daten gehören mir" zeigt nur, dass sich nicht an Grundrechten orientiert wird, sondern dass wiederum Eigentum und Marktmechanismen den Referenzrahmen abgeben. Auch dieser Wandel in der Priorisierung von Waren gegenüber Normen spielt den dominanten Organisationen in die Hände, wieder zu Lasten von betroffenen Personen.

Was ist zu tun? Seit 2012 entwickelt rund ein Dutzend Kolleg.innen aus dem Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Standard-Datenschutzmodell (SDM). Das 54 Seiten umfassende Handbuch zum Modell ist seit November 2016 auf den Webseiten fast aller Datenschutz-Aufsichtsbehörden Deutschlands zu finden. Das SDM bietet zum einen eine Methodik zur Vermittlung von Rechtsnormen und technischen Funktionen und stellt zum zweiten einen Katalog mit spezifischen Standard-Datenschutz-Referenzmaßnahmen in Aussicht.

Für jeden ernsthaft an Datenschutz Interessierten kann insofern klar sein, aus welchen Gründen welche Maßnahmen für die Durchsetzung von Datenschutz zu treffen sind. Und wieder können Sie die Ernsthaftigkeit Ihres Interesses an einem wirksamen Datenschutz daran erkennen, ob Sie nun nach SDM recherchieren (oder nicht).

Letztendlich zeigt sich: Im Datenschutz müssen sich nicht nur Alice und Bob vor Carol schützen, das müssen sie auch, obendrein muss Alice aber auch noch vor Bob geschützt werden, wenn sie sich nicht allein wirksam vor Bob schützen kann, weil Bob von vornherein strukturell ungleich stärker ist.