Was meint eigentlich „Datenschutz“?

Seitdem nicht nur insbesondere Facebook und Google die Menschen weltweit vermessen, sondern seitdem als geklärt gilt, dass insbesondere die NSA und der GCHQ auf diese Daten zugreifen und diese zusätzlich mit ihren eigenen Daten noch aus ganz anderen Quellen verschneiden, wird in Teilen von Europa und den USA verstärkt über Datenschutz gesprochen. Der politische Skandal wird durch die Medien gut befeuert. Was jedoch aussteht, ist eine Analyse der Funktion des Datenschutzes als Ausgangspunkt zur Entwicklung einer aussichtsreichen Gegenstrategie. Als Ausgangspunkt sollten dabei nicht irgendwelche Imaginationen zu „Privatheit“ herangezogen werden, sondern die Aktivitäten von Organisationen, weil diese die Strukturen moderner Gesellschaften zerstören, die die informationelle Selbstbestimmung ermöglichen.

„Eine Gesellschaftsordnung ... und die sie ermöglichende Rechtsordnung, in der jemand nicht mehr weiß, wer wann was und bei welcher Gelegenheit über ihn weiß, ist mit unserer Verfassung nicht vereinbar.“

(Prof. Dr. Dr. Adalbert Podlech, 2008)

Dieses Statement von *Podlech* kann vermutlich als das Kondensat des deutschen Datenschutzrechts gelten. Das deutsche Datenschutzrecht wurde in den politisch und rechtsstaatlich schwierigen 1970er-Jahren zum ersten Mal formuliert. Damals sah sich der Gesetzgeber veranlasst, auf die zunehmende Nutzung datenverarbeitender Techniken – außerhalb von Fachzeitschriften wurden Computer zu der Zeit hin und wieder noch unsicher als „Robotergehirne“ bezeichnet – bei den Banken und Versicherungen sowie der Verwaltung, insbesondere bei den Sicherheitsbehörden, zu reagieren. Es bestand das strukturelle Risiko, dass sich die Gewaltenteilung zugunsten der Exekutive und zulasten von Legislative und Jurisdiktion auflösen würde. Den politisch Verantwortlichen stand durchaus bis in das konservative Lager hineinreichend das Risiko einer kollabierten Gewaltenteilung angesichts des nationalsozialistischen Terrors, einer sich „sozialistisch“ verstehenden Diktatur im Nachbarland sowie des aktuellen RAF-Terrors, klar vor Augen.

Die Datenschutzrechtler der ersten Generation thematisierten dieses strukturelle Risiko einer mangelhaften Gewaltenteilung als Risiko für die Handlungsfreiheit und Würde von Einzelpersonen. Entscheidend an dem Problemzuschnitt war, dass sie den Schutz der Privatsphäre an den Erhalt des

Von Martin Rost, Kiel

Rechtsstaates und der Demokratie koppelten. Das galt damals zweifelsfrei, heute ist das anders. Datenschutz wird vielfach als Privatproblem von Privatpersonen konzipiert, die von „Datenschützern“ aufgefordert werden, in ihren Facebook-Profilen auf wirksame „Datenschutzeinstellungen“ zu achten. Der Datenschutz entstand in den Siebzigern als ein staatlich institutionalisierter Zweifel des Staates vornehmlich an sich selber. Den ersten Datenschützern war vollkommen klar, dass nur ein auf die Gesellschaftsstruktur achtender Datenschutz in der Lage sein kann, die notorisch aus dem Ruder laufenden Geheimdienste sowie die mächtigen Banken und Sozialversicherungen sowie generell die zur Monopolisierung gedrängten Unternehmen einzufangen. Sie sahen auch den Zusammenhang von Organisationen und Technik. Die aktuelle wirtschaftsliberale Politik läuft diesem Ansatz jedoch seit gut 20 Jahren entgegen. Sie unterstellt dass die „Konsumenten-Demokratie“ der politischen Demokratie überlegen sei, weil sich in ihr die Präferenzen der Verbraucher mit jeder Kaufentscheidung manifestieren, während die Bürger ja nur alle vier Jahre an die Wahlurnen gingen. Die entmachtete Politik begreift Technik seitdem als ein Naturphänomen, das unwiderstehlich, politisch und rechtlich nicht einhegbar über die Menschen einbricht.

Allerdings gilt es auch festzustellen, dass dieses Statement von *Podlech*, wonach es für jeden Bürger möglich sein muss festzustellen, wer wann und was bei welcher Gelegenheit über ihn weiss, weltfremd anmutet, vermutlich nicht erst heutzutage. Prof. em. Dr. Dr. h.c. *Spiros Simitis*, ebenfalls ein sehr einflussreicher Datenschützer aus der ersten Datenschützer-Generation, legte den Schwerpunkt des Schutzobjekts des Datenschutzes in einem Interview 2009 anders.[1]

„Das Recht selbst darüber zu entscheiden, wer die Daten des Einzelnen, wann, unter welchen Bedingungen, wofür benutzt, dieses Recht (...) ist eine elementare Funktionsbedingung einer demokratischen Gesellschaft. Das ist nach meiner Überzeugung die Grundlage des Datenschutzes (...) nicht das Persönlichkeitsrecht! (...) Es steht die Struktur der Gesellschaft auf dem Spiel. Und diese Struktur der Gesellschaft definiert unsere Aufgabe. (...) Alles ist heute erhoben. Ich kann eine Politik entwickeln, die den Einzelnen als steuerbares Subjekt ansieht (...). Heute ist das eigentliche Stichwort für die Datenverarbeitung Prävention. Und in dem Maße wie ich bei der Prävention bin, steuere ich!“

(Prof. Dr. Dr. h.c. Spiros Simitis, 2009)

Es geht ums Ganze, um die Struktur der Gesellschaft, die die Aufgabe als Datenschützer definiert, es ist nicht erst das Persönlichkeitsrecht. Die Institutionalisierung des Datenschutzrechts und der Datenschutzaufsichtsinstitutionen ist bereits eine Reaktion auf strukturellen Konflikt in der modernen Gesellschaft, nämlich der Machtasymmetrie, die grundsätzlich zwischen Organisationen und deren „organisationsinternen“ Mitarbeitern und Mitgliedern sowie dem „organisationsexternen“ Klientel besteht. Es geht um die Konditionierung der Machtasymmetrie zwischen Verwaltungen und Bürger, zwischen Unternehmen und Kunden, zwischen Praxen und Klienten/ Patienten. Organisationen haben diese Machtasymmetrie in den vergangenen 30 Jahren zu ihren Gunsten ausgebaut und inzwischen durch die modernen Informations- und Kommunikationstechniken industriell verfestigt.

Bevor dieser Aspekt der Machtasymmetrie vertieft wird, sollte man noch einmal einen Schritt zurücktreten und fragen: Was versteht man unter „gesellschaftlicher Struktur“ oder „Gesellschaftsordnung“? Wie muss man sich Gesellschaft vorstellen, die als eine Art Ökosystem für Organisationen und Personen dient?

Politische und juristische Macht, Geld und wissenschaftliche Wahrheit lassen sich in der modernen Weltgesellschaft nicht mehr in eins setzen oder trivial ineinander umrechnen. Die Schwierigkeit dieser „Umrechnungen“ verschiedener Logiken ist das, was in der Soziologie seit mittlerweile mehr als 30 Jahren gut analysiert ist und z.B. als „funktionale Differenzierung“ bezeichnet wird.[2] In Bezug auf Einzelpersonen erzeugt die funktionale Differenzierung sowohl verschiedene soziale Funktionssysteme als auch Organisationen. Und mit diesen beiden zusammen entstehen dann Personenkonzepte oder konventionell ausgedrückt: Rollen. So ist es der Markt als eine gesellschaftliche Struktur, der das Konzept des „Kunden“ hervorbringt; es sind Rechtsstaat und Demokratie, die das Konzept des „Bürgers“[3] erzeugen; es ist die

---

1 Die hier besonders kenntlich gemachten Zitate maßgeblicher Datenschützer der ersten Generation sind Interviews entnommen, die von der Webseite www.maroki.de abrufbar sind.

2 Siehe *Niklas Luhmann*: Soziale Systeme, 1983, Frankfurt am Main.

3 Spätestens mit *Rousseau* lässt sich der politisch orientierte „Staatsbürger“ („citoyen“) vom politisch zwar interessierten, aber primär an seinen privaten Geschäften interessierten „Verwaltungsbürger“

wissenschaftliche Befassung mit Personen, die Konzepte wie „Mensch“, „Individuum“, „Patient“, „Klient“, „Subjekt“ oder eben auch das soziologische Konzept von „Person“ entstehen lässt. Diese Personenbegriffe stehen für verschiedene „allgemeine“ Rollenanforderungen, die sich in einer modernen Gesellschaft nicht verlässlich oder gar logisch zur Deckung bringen lassen, was aber gar nicht zu sozialen oder psychischen Verwerfungen führen muss. Im Gegenteil. Am Umgang mit einer Fülle an Konflikten und Unvereinbarkeiten entsteht dann die Fülle von Persönlichkeiten, die sich selber für einzigartig, für autonom oder für gegängelt oder für „originell“ halten können. Diese vielschichtigen Rollenkonzepte von Personen werden durch Funktionssysteme moderner Gesellschaften erzeugt und zugleich, das ist der Clou in diesem Zusammenhang, latent durch die Aktivitäten von Organisationen bedroht.[4]

Die Vielfältigkeit der funktional separierten Logiken ziehen Organisationen notwendig auf einen Punkt zusammen. Organisationen halten die Gesellschaft zusammen: Unternehmen beachten Recht, Politik und Wissenschaften, agieren aber letztlich unter dem Primat der Kapitalverzinsung, politische Organisationen agieren unter dem Primat des Machterhalts/Machtausbaus, Verwaltungen agieren unter dem Primat der Rechtskonformität. „Sicherheitsbehörden“ agieren unter dem Primat der Sicherung der öffentlichen Ordnung. Und wissenschaftliche Organisationen agieren unter dem Primat von Letztwahrheiten, und sei es die darauf zu bestehen, dass es keine gebe. Insofern ist festzustellen, dass Organisationen der gesellschaftlichen und eben auch der persönlichen Vielfalten einseitige Entscheidungen aufzwingen, die für Personen (und für die funktionale Differenzierung der Gesellschaft) Risiken bedeuten, die die strukturell mächtigen Organisationen auf die schwächeren Personen abwälzen. Diese unverzichtbare Syntheseleistung von Organisationen bringt zugleich große Risiken mit sich, insbesondere wenn Organisationen weltweit agieren, aber von keinem weltweit gültigen Recht in demokratisch kontrollierte Schranken verwiesen werden (können).

Organisationen, die nicht in Schranken verwiesen werden, erzeugen bekanntlich zwangsläufig gesellschaftliche Probleme: Es sind ja nicht nur die Unternehmen, die latent ein Monopol anzustreben gezwungen sind, Märkte austrocknen und die Natur ruinieren, sondern sie tendieren auch dazu, sich externe Kunden als interne Unternehmensmitglieder einzuverleiben, die nach den Regeln des Unternehmens agieren. Es sind ebenso die Sicherheitsbehörden, die sich permanent genötigt sehen, sich nicht an die Gesetze zu halten und vor allem die Gewaltenteilung zu unterlaufen. Sie gerieren sich grundsätzlich so, als sei ihre Aufgabe überhaupt nur noch erfüllbar, wenn sie permanent die Grundrechte eines jeden Bürgers einschränken und diese außer Kraft setzen. Und auch die wissenschaftlich orientierten Institutionen gilt es zu bedenken, die die um Wahrheit ringenden Diskurse mit ihrem seltsamen Zwang des besseren Arguments und die Anerkennung missliebiger Forschungsergebnisse durch dogmatisch wohl begründete Begriffs- und Methodenverbote entmutigen. Der Datenschutz thematisiert an den von den Organisationen provozierten Deformationen der Freiheit und Souveränität bzw. der Privatsphäre von Personen, ob als Bürger, Kunde oder Klient und Patient inkarniert, somit die Deformationen der modernen Gesellschaftsstruktur mit ihrer funktionalen Differenzierung. Diese Relationen zwischen Organisationen und Personen und deren konkrete Ausgestaltung zu beobachten, zu bewerten und auf der Basis von verfassten Grundrechten ggf. negativ zu sanktionieren, ist somit die Aufgabe des Datenschutzes.

„Die Schneckenhaus-Privacy war nur einmal kurz eine Realität, nämlich rückverbunden zu den vorindustriellen Lebensweisen. … Man wusste am Ende gar nicht mehr, welche gesellschaftliche Bedeutung der Datenschutz haben sollte.“

(Paul Müller, 2012)

Das Datenschutzproblem leitet sich nicht aus der Persönlichkeit von Menschen her und dessen irgendwie privatem Bedürfnis nach Privatheit. Vielmehr ist die schützenswerte Individualität und der Anspruch auf Freiheit des einzelnen Menschen selber ein Konstrukt einer bestimmten sozialen Struktur. Organisationen moderner Gesellschaften müssen die Chance auf Privatheit, Eigensinnigkeit, Autonomie der mit ihnen befassten Personen zulassen.

Das Datenschutzrecht war, zumindest von der Anlage und der Motivationslage der Gründergeneration her betrachtet, deshalb vor allem als eine Gefahrenabwehr gegenüber den Organisations-Egoismen datentechnisch bewaffneter Technokraten konzipiert, die insbesondere durch Prävention ihre systemischen Risiken bzgl. der Kapitalverzinsung, Macht, Sicherheit und Wahrheitsdefinition einseitig zu verringern trachten. Organisationen setzen ihr Risikoabwälzen heute technisch durch. Insofern stellt sich dringend die Frage nach dem Verhältnis von Technik und Recht.

„Ich bin davon überzeugt, dass Recht Technik gestalten kann. (...) Es gibt kein Privateigentum an Daten, sondern es gibt eine Ordnung wie man mit diesen Daten umgeht. Ich kann aber auch nicht jeden Umgang mit den Daten verbieten, weil, – ich lebe ja in einer sozialen Gemeinschaft, da muss man kommunizieren. Damit diese Kommunikation freiheitlich ist und die Selbstentwicklung des Individuums ermöglicht, deswegen brauche ich informationelle Selbstbestimmung.“

(Alexander Roßnagel, 2008)

Man muss das von *Rossnagel* angesprochene Problem begrifflich noch etwas präziser fassen, um den Zusammenhang von Recht und Technik und die Funktion des Datenschutzes in der modernen Gesellschaft genauer bestimmen zu können. Denn es geht nicht um Techniken für eine „soziale Gemeinschaft“ im engeren Sinne, sondern um „Gesellschaft“, soziologisch ist das ein großer Unterschied.

Eine Gemeinschaft könnte sich durchaus selbst weitgehend vernünftige, logisch-konsistente Regeln geben, die jedes Mitglied der Gemeinschaft verstünde und deshalb anerkennen könnte, weil sie für alle Mitglieder verallgemeinerbar das Beste sind. In einer Gemeinschaft macht die Rede von einem konsensualen „wir“ noch einen hinreichend präzisen Sinn. Gemeinschaft ist jedoch genau kein Ort der gesellschaftlich funktionalen Differenzierung. Und damit ist Gemeinschaft auch kein Kontext, in dem die spezifisch Schutzwirkung des Datenschutzes greift. Es geht stattdessen beim Datenschutz um das technisch gestützte Agieren von Organisationen in einer (Welt-) Gesellschaft in Bezug auf Personen und deren Umsetzung von Menschenrechten. In dieser Welt-Gesellschaft bestehen jede Menge an widersprüchlichen aber trotzdem verbindlichen Regelungen, bei denen es kein konsensuales „wir“ gibt.

Eine moderne Welt-Gesellschaft ist mehr denn je auf Vertrauen angewiesen gerade deshalb, weil es kein Welt-Recht und keine zentrale Regulationsinstanz gibt. In den modernen komplexen Handlungsverkettungen über technische Infrastrukturen müssen Organisationen und Nutzer einander über alles rechtlich Geordnete und alle bilateralen Einwilligungsvereinbarungen hinweg, vernünftig begründete, gegenseitige Vertrauensvorschüsse gewähren. Personen müssen dabei abstrakt in komplexe Systeme, in Organisationen und Maschinen, anstatt konkret in sinnfällig anständige Personen vertrauen können. Es geht um ein begründetes, begründbares, nicht blindes Systemvertrauen. Vertrauen zu gewähren und ebenso abzufordern, macht moderne Gesellschaften so besonders effektiv.

An dieser Stelle des Systemvertrauens kommt der Kommunikations- und Informationstechnik eine enorme Bedeutung zu. Technik muss so ausgelegt sein, dass sie die abstrakten Vertrauensanker der moder-

---

(„bourgeois“) und wiederum vom „Menschen im Staat“ („homme“), der sich nicht für die ihn umgebende politische Struktur interessiert, unterscheiden.

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

nen Weltgesellschaft nicht unterläuft, die darin bestehen, dass es Märkte gibt, die für eine vernünftige Ressourcenallokation sorgen und die private Diktatur von Monopolunternehmen behindern; dass Gewaltenteilung installiert ist, die die staatliche Willkür und Korruption bei Politik, Verwaltung und Justiz unwahrscheinlicher macht; dass freie spirituelle und insbesondere künstlerische und wissenschaftliche Diskurse stattfinden, die einer umsichtigen und verallgemeinerungsfähigen Vernünftigkeit selbst bei Unbestimmtheit eine Stimme verleihen. Die Infrastrukturtechniken, die die operative Basis für die oben genannten systemischen Vertrauensanker bilden, werden jedoch von wenigen global agierenden Privat-Organisationen beherrscht, die nur ihren eigenen Regeln nachgehen.

In Zeiten moderner Informations- und Kommunikationstechnik stellt sich bspw. die Frage, ob Markt oder Gewaltenteilung überhaupt realistische Vorstellungen sind. Am Beispiel veranschaulicht: Wie kann der operativ bestehende Kurzschluss, den ein Rechenzentrum für die Gewaltenteilung eines Landes bildet, wenn bspw. die IT des Landesparlaments, die IT des Landeskriminalamtes, der Staatsanwaltschaft sowie der verschiedenen Gerichtsinstanzen gemeinsam darin betreut werden, zum Schutz der Bürger verhindert werden? Genau hier für „Trennungen“ zu sorgen und „operative Kurzschlüsse der Gewalten“ zu verhindern, ist die Aufgabe eines modernen proaktivgestaltenden Datenschutzes. Nur wenn dies gelingt, ist „Privatheit“ trotz gesellschaftlicher Teilhabe von Menschen möglich.

„Die Aufgaben in Staat und Wirtschaft lösen Informationsströme aus, die zugeteilt werden müssen für die Aufgaben. Wenn man die hinreichend aufteilt ist das kein Problem. Die Aufteilung ist nicht das Problem, sondern es sind die Lobbys. Es geht nicht um Privatsphären. Sondern es geht darum, eine Technik sozial beherrschbar zu machen – das ist alles.“

(Wilhelm Steinmülle, 2009)

Das Datenschutzrecht setzt diese Anforderung nach Aufteilung von Informationsströmen mit zwei zentralen Regeln um:

1. Es ist verboten, personenbezogene Daten zu verarbeiten („Verbot mit Erlaubnisvorbehalt“, § 4 Abs. 1 BDSG).[5]
2. Wenn eine Datenverarbeitung ausnahmsweise gesetzlich erlaubt ist oder der Betroffene in einem privatrechtlichen Verhältnis explizit in die Verarbeitung seiner Daten eingewilligt hat, dann muss diese Datenverarbeitung nachweisbar eng zweckbestimmt erfolgen. Datenverarbeitung durch Organisationen ist kein Naturphänomen, sondern eine Aktivität von Organisationen.

Was ist zu tun? Organisationen müssen nachweisen, dass sie das generelle Verbot mit Erlaubnisvorbehalt zu Recht für den ausgewiesenen Zweck durchbrechen und sich dabei eng an den Zweck binden. Für den Fall einer berechtigten Verarbeitung müssen Organisationen sechs Typen an Anforderungen genügen. In der aktuellen Datenschutz-Diskussion werden diese Anforderungen unter dem Schlagwort der „Neuen Schutzziele“ gefasst. Schutzziele vermitteln gesetzliche Anforderungen mit technisch-organisatorischen Funktionen und Schutzmaßnahmen.

Schutzziele sind ein bekanntes Konzept. Im Datenschutz spielen die aus der IT-Sicherheit bekannten Schutzziele der Datensicherheit bzw. Informationssicherheit, nämlich *Verfügbarkeit, Integrität und Vertraulichkeit* eine Rolle. Wobei beim Datenschutz der Schutz der Integrität und Vertraulichkeit für Personen und nicht primär der Schutz von Geschäftsprozessen im Vordergrund stehen. Darüber hinaus sind drei weitere Schutzziele zu nennen. So ist *Transparenz* der Aktivitäten einer Organisation die wesentliche Voraussetzung für den Nachweis der Rechtmäßigkeit der Verarbeitung sowie für die Möglichkeit zur Steuerung und Regulation technisch-organisatorischer Prozesse. Das Schutzziel der *Nichtverkettbarkeit* operationalisiert die Erforderlichkeit und Zwecksetzung und die darauf hin abzustimmende Zweckbindung und Zwecktrennung einer Datenverarbeitung. Und das Schutzziel der *Intervenierbarkeit* operationalisiert insbesondere die Rechte von Betroffenen zur Korrektheit oder zur Löschung von Daten und fordert von den informationsverarbeitenden Stellen bzw. Betreibern von Systemen den Nachweis, dass sie ihre Systeme steuernd beherrschen. Das Mittel dazu wird im Rahmen moderner Organisationsframeworks wie ITIL oder CoBIT im weiteren Sinne als Changemanagement bezeichnet.

Drei Aspekte sind bei der Orientierung an Schutzzielen zu beachten:

1. Vollständigkeit der Beachtung

Die sechs Schutzziele sind vollständig umzusetzen.[6] Die Umsetzung bspw. allein der Transparenz-Anforderung ist datenschutzrechtlich bzw. telekommunikationsrechtlich unzureichend. So weist bspw. Facebook in seinen AGB oder in den Privacy-Bestimmungen darauf hin, dass Facebook die persönlichen Nachrichten zwischen Facebook-Nutzern mitliest. Diese Transparenz entfaltet keinerlei Schutzwirkung, sondern bestätigt allein, dass die Anforderungen von Vertraulichkeit und Nichtverkettbarkeit nicht umgesetzt werden.

2. Schutzziele aus der Sicht von Betroffenen umsetzen

Die Schutzziele der IT-Sicherheit und die Schutzziele des operativen, technisch-organisatorischen Datenschutzes stehen nicht zwingend in einem Deckungsverhältnis zueinander, eher im Gegenteil.[7] Die IT-Sicherheit muss bei jedem Anwender von IT-Technik einen potenziellen Angreifer vermuten. Der Datenschutz nimmt dagegen die schutzwürdigen Belange von Personen zum Ausgangspunkt und sieht in jeder Organisation und der von ihr verwendeten Technik einen Angreifer.

3. Die Schutzziele des Datenschutzes führen

Aus einer grundrechtlichen Perspektive müssen die Sicherheitsmaßnahmen der IT-Sicherheit den Anforderungen des operativen Datenschutzes genügen. Diese Forderung läuft in der Praxis jedoch ins Leere, weil die IT-Sicherheit bspw. mit IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) über eine erwiesenermaßen praxisgerechte Methode der Prüfung von Informationstechnik verfügt. Eine solche standardisierte Methode wird von den Datenschutzaufsichtsbehörden Deutschlands derzeit erarbeitet. □

Martin Rost, stellvertretender Leiter des Technikreferats, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel

[5] Einer solchen Regel folgt bspw. auch die Administration einer Firewall, bei der alle Kommunikations-Ports zunächst „dicht gemacht“ und anschließend die nur erforderlichen wieder geöffnet werden.

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

[7] Siehe *Martin Rost*: Eine kurze Geschichte des Prüfens; in: BSI 2013: Informationssicherheit stärken – Vertrauen in die Zukunft schaffen, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, S. 25-35.