Martin Rost

Risiken im Datenschutz

Der bisherige Kommentarliteratur zur Datenschutz-Grundverordnung (DSGVO) bezieht den Begriff des „Datenschutz-Risikos“ überwiegend auf die Vermeidung sichtbarer Schäden oder Kontrollverluste für Betroffene durch die Nutzung einer notorisch unsicheren IT. Eine solche Engführung des Verständnisses vom „*risk-based-approach*“ (RBA) verliert jedoch den Grundrechtseingriff und die Konditionierung der Machtasymmetrie zwischen Organisationen und Personen aus dem Blick. Martin Rost stellt in diesem Beitrag acht klar unterscheidbare Risikotypen vor.

Einleitung

Datenschutz wird mittlerweile häufig auf einen Schutz der Privatheit reduziert und missverstanden. Die Dringlichkeit oder Entbehrlichkeit des Datenschutzes wird dadurch zu einer Frage lediglich persönlicher Wertungen und Vorlieben. Datenschutz hat jedoch eine viel weiter reichende Funktion: Er wacht in modernen Gesellschaften darüber, dass Organisationen die bestehenden Autonomieerwartungen, die sich mit verschiedenen Rollen verknüpfen (bspw. als Bürger*in, Kund*in, Patient*in) nicht unterlaufen. Zu einem solchen Verständnis von Datenschutz gehören deshalb auch Elemente von Staatlichkeit, wie die Gewaltenteilung, die Rechtsstaatlichkeit und die Demokratie, die einerseits die Willkür von Organisationen brechen und andererseits „den modernen Bürger“ historisch überhaupt erst haben entstehen lassen. Der Umgang der Organisationen – z.B. Behörden, Unternehmen, Hochschulinstitute, Vereine, Arztpraxen und Notare – mit ihrem internen und externen Personal in einer modernen Gesellschaft einer der deutlichsten Indikatoren für Beschädigungen strukturell notwendiger Trennungen und Gewaltenteilungen zum Schutz vor Organisationswillkür. Organisationswillkür zielt darauf ab, aus würdevollen Subjekten willfährige Objekte zu machen. Die Willkür findet ihre Grenzen da, wo Grundrechte anerkannt sind und durch Aufsicht und wirksame Sanktionen durchgesetzt werden, nicht aber dort, wo nur ein Markt durchgesetzt ist. Wer gehört zu einer Organisation und muss mit einer weitgehend ungefragten Auswertung und Verarbeitung seiner personenbezogenen Daten rechnen? Wer kommt mit einer Organisation nur punktuell, etwa als Kundin oder Bürger, in Berührung und darf mit einem gewissen Schutz seiner personenbezogenen Daten rechnen? Diese Fragen zu entscheiden und die Beziehungen zu ge-

stalten fallen heute wieder zunehmend ausschließlich in das Belieben der Organisationen. Dass der wirksame Schutz vor Organisations-Willkür, gleichgültig ob durch staatliche oder private Stellen, die zentrale Funktion von Datenschutz ist, kann man seit den 1970er Jahren wissen. Dieses Wissen erodierte allerdings in den letzten Jahrzehnten (vgl. Pohle 2018). Es zeigt sich aktuell wieder sehr deutlich: Ein operativ wirksamer Datenschutz erfordert klare staatliche und zivilrechtliche Sanktionen.[1]

Risikodiskussionsfelder im Kontext von Datenschutz

Die DSGVO legt hinsichtlich ihrer Auswahl und Dimensionierung technisch-organisatorischer Schutzmaßnahmen eine Orientierung an Risiken nahe. Es wäre aber falsch, deshalb gleich von einem „*risk-based-approach*" der Grundverordnung zu sprechen, wie er bspw. in der IT-Sicherheit verfolgt wird. Dieser aus der Finanz- und Versicherungswirtschaft stammende Begriff findet sich in der DSGVO jedenfalls nicht.

Die Orientierung an Risiken soll es ermöglichen, die in Artikel 5 DSGVO abstrakt formulierten Grundsätze der Datenverarbeitung sowie die auf deren Umsetzung, Wirksamkeit und Nachweisbarkeit abzielenden Vorschriften (bes. Artikel 24, 25, 32 und 35) in konkrete Verarbeitungs- und Schutzfunktionen zu transformieren. Die Risiko-Orientierung folgt der durchaus einleuchtenden Idee, dass ein Betroffener am Eintreten oder Ausbleiben von Schäden handfest und unmittelbar spüren kann, ob die operative Behandlung von Risiken, die durch eine personenbezogene Verarbeitungstätigkeit entstehen, gelungen ist oder nicht. In Erwägungsgrund (EG) 75 wird zudem die betriebswirtschaftlich bewährte Risikoformel zur Anwendung empfohlen, wonach ein unmittelbares Risiko für Personen nach der Formel „Schadenshöhe mal Eintrittswahrscheinlichkeit" bestimmbar sei. Die Anwendung dieser Formel im Datenschutz erscheint plausibel, zumal sie z. B. Teil der bewährten IT-Grundschutz-Methodik des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist, mit der die Auswahl und die Intensität der Wirksamkeit von Schutzmaßnahmen der IT-Sicherheit festgesetzt wird. Allerdings schränkt das BSI den Nutzen dieser Risikoformel ein: „*Solche umfangreichen Erfahrungswerte fehlen in den meisten Fällen im sehr dynamischen Umfeld der Informationssicherheit. Daher ist es in den meisten Fällen praktikabler, sowohl für die Eintrittshäufigkeit als auch für die potenzielle Schadenshöhe mit qualitativen Kategorien zu arbeiten.*" (BSI 2017: 26) Mit anderen Worten: Die Risikoformel ist im Kontext der IT-Sicherheit nur als Heuristik geeignet.

Im Datenschutz beschäftigt man sich mit Risiken, seit die Sicherheit von Informationstechnologien – zunächst im professionellen Umfeld, später dann auch im privaten Nutzungsbereich und in Computernetzen – zu einem relevanten Problem wurde. Mittlerweile haben die anhaltende „Computerisierung", „Digitalisierung" und „Vernetzung" insbesondere bei technischen Datenschützern dazu geführt, Risiken des Datenschutzes mit Risiken der IT weitgehend gleichzusetzen (vgl. Rost 2013). Aus Sicht der IT-Sicherheit sind personenbezogene Daten lediglich „*besonders schützenswerte Daten*", die es sicherheitstechnisch vor unbefugtem Zugriff (von Außen wie von Innen) zu schützen gilt. Vielfach vertreten selbst professionelle Datenschützer*innen die Ansicht: Wenn die IT nur hinreichend sicher betrieben wird und eine Rechtsgrundlage

für eine Datenverarbeitung vorliegt, ist auch grundrechtlich alles Notwendige getan. Eine solche Auffassung greift aus Datenschutzsicht nicht nur zu kurz, sie ist falsch. IT-Sicherheit herzustellen ist selbstverständlich auch für den operativen Datenschutz unverzichtbar. Aber dies kann erst der zweite Schritt sein, davor besteht die anders gelagerte Aufgabe, die Grundrechtseingriffe operativ auf ein unabweisbares Mindestmaß zu reduzieren. Dazu gleich mehr.

Die technisch verengte, die Interessen Dritter und der Allgemeinheit vernachlässigende, Vorstellung vom Datenschutz wird zusätzlich durch eine ökonomische Sichtweise verstärkt. Danach besteht das zu lösende Problem der Betroffenen bzw. Kund*innen vornehmlich darin, ihre personenbezogenen Daten möglichst teuer an die sich dafür interessierenden Firmen zu verkaufen: „*Meine Daten gehören mir (und ich bestimme ihren Preis)!*“ In dieser Wahrnehmung besteht das Risiko der Betroffenen darin, dass sie ihre Daten zu billig verkaufen. Wenn diese Schnäppchen-Mentalität nicht in ein grundrechtliches Verständnis von Sinn und Zweck des Datenschutzes übergeht (was eine trivialisierende Ökonomisierung von Daten ausschließt), ist nichts an einer Souveränität für Betroffene gewonnen.

Eine weitere Trivialisierung des Datenschutzes besteht darin, den Schutz vor Werbematerialien für dessen Kardinalproblem zu halten. Hier gilt es zu verstehen, dass es im Kontext von „Werbung“ inzwischen viel weiter greifend um die Vorhersage von Verhalten und um die gezielte Steuerung von Personen auf Basis der Auswertung entsprechender gesammelter Daten geht. Das muss ebenfalls berücksichtigt werden, wenn ein Unwohlsein vor US-amerikanischen Kommunikationsunternehmen und Geheimdiensten formuliert wird, nur weil deren Aktivitäten nicht hinreichend transparent sind. Es geht um mehr als Transparenz, es geht inzwischen auch um subtiles Fälschen und Manipulieren von Kommunikationen. Ebenso wird das Hacker-Risiko als großes Problem in den Blick gestellt, wonach Bürger*innen damit rechnen müssen, dass Kriminelle beliebigen Zugriff auf PCs nehmen können. Mit jedem dieser Narrative gerät der Datenschutz mehr aus dem Blick oder wird kleingeredet. Zudem legen sie den Gedanken nahe, dass der einzelne Betroffene Datenschutz nur bei sich und für sich selbst lösen könne. Insofern erscheint dann „Selbstschutz“ sogar als aussichtsreichste Risikobewältigungsstrategie, die (wenn überhaupt) nur jenen IT-Expert*innen vorbehalten bleibt, die *Privacy-Enhancing-Technologies* beherrschen. Nein, nicht die Menschen sind Schuld, wenn Organisationen sich nicht an Datenschutzrecht halten.

Nach derartigen falschen Vereinfachungen zum Datenschutzproblem ist es an der Zeit, die Dimensionen des Risiko-Begriffs im Kontext eines grundrechtsorientierten Datenschutzes neu zu bestimmen. Diese Bestimmung muss ansetzen an einer wirksamen Umsetzung der „*Rechte und Freiheiten von Personen*“, wie die französische Formel das nennt, was im Deutschen „Grundrechte“ heißt.

Risiken im Kontext der DSGVO

Im EG 75 ist hinsichtlich der Risiken mangelhaften Datenschutzes von einem „*physischen, materiellen oder immateriellen Schaden*“, von „*Diskriminierung, Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem*

Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen“ die Rede. Weiterhin wird auf Fälle verwiesen, bei denen Personen „*... daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden ...*“

In einem der ersten, vom Bundesministerium des Innern herausgegebenen Kommentare zur DSGVO interpretiert Winfried Veil den EG 75 unter der problematischen Überschrift „*risikobasierter Ansatz*“. Ihn überzeugt die „*holzschnittartige Auflistung*“ nicht, u. a. weil die DSGVO an keiner Stelle die Schutzgüter definiere, gegen die das Risiko bzw. die Schäden für Rechte und Freiheiten abgeschätzt werden können (vgl. Veil 2018: 721). Er übersieht jedoch, dass gerade durch die Auflistung möglicher Schäden der Grundrechtsbezug verloren geht. Anstatt diesem Problem zu begegnen, weitet Veil die EG-75-Liste aus und ergänzt sie um weitere Risiken, die er dadurch zu rechtfertigen versucht, dass sie nunmehr „*wissenschaftlich fundiert*“ seien. Als weitere Risiken nennt Veil: „*Erhöhung individueller Verletzlichkeit durch Straftaten*", „*Schamgefühl und Publizitätsschäden*", „*Selektivitätsschäden*“ (unerwünschte Informationsverwendung in Auswahlprozessen), „*Informationspermanenz*“ (Schäden aus unbegrenzter Speicherbarkeit von Daten), „*Entkontextualisierung*", „*Informationsemergenz*", „*Informationsfehlerhaftigkeit*", „*Behandlung des Menschen als Objekt*", „*Fremdbestimmung*" und die „*Enttäuschung von Vertraulichkeitserwartungen*“ (Veil 2018: 724). Die Auflistung möglicher Datenschutz-Risiken in dieser Konkretion ist durchaus verdienstvoll. Aber Veil teilt offenbar nicht die Auffassung, dass die von ihm genannten Risiken bereits vollständig durch die Grundsätze in Artikel 5 DSGVO erfasst werden! Das Schutzgut der DSGVO ist, anders als Veil behauptet, ganz klar ausgewiesen: Es betrifft zum einen die aus Artikel 5 DSGVO ableitbaren Rechte, die auf Artikel 8 der EU-Grundrechte-Charta (GrCh) zurückgehen. Und es sind zum anderen die daraus resultierenden tatsächlichen Freiheitsgarantien für Personen, die aus einer wirksamen Umsetzung dieser und weiterer Grundsätze der DSGVO gegen die strukturelle Übermacht der Organisationen resultieren.

Diese Interpretation des Artikels 5 verlangt die Bereitschaft, die Grundsätze im Sinne von Gewährleistungs- und Schutzzielen auszulegen, die in IT-Systemen methodisch umzusetzen sind. Veil weist darauf hin, dass der Normengeber in Artikel 5 explizit nicht von Schutzzielen spreche (Veil 2018: 722). Diese Lesart kann nicht überzeugen. Schutzziele sind ein inzwischen methodisch etabliertes Instrument, um Beeinträchtigungen, also Grundrechtseingriffe und Schutzmaßnahmen, zu identifizieren. Schutzziele sind insofern eine Antwort auf die rechtsphilosophische Einsicht David Humes, wonach aus dem Sein kein Sollen folge, und auch aus einem Sollen kein unmittelbar erzeugbares Sein. Genau dafür, für die Vermittlung zwischen Sein und Sollen, bedarf

es vermittelnder Modelle. Schutzziele machen in einer gegenseitig schonenden Weise beide Seiten – Technik und Recht – füreinander relevant und aufeinander beziehbar. Zumindest das Bundesverfassungsgericht findet dieses Konzept der Schutzziele überzeugend, wie sich im 2008 ergangenen Urteil über die Vertraulichkeit und Integrität von IT-Systemen zeigt (vgl. BVerfG 2008).

Für jeden der Grundsätze aus Artikel 5 sowie die „*Optimierungsgebote der Schutzziele*" (Bock/Robrahn 2018) steht ein Katalog mit Umsetzungsmaßnahmen bereit, deren Wirkintensität durch die Höhe des Risikos bzw. die Höhe des Schutzbedarfs bestimmbar ist (vgl. SDM 2016). Die Risiken für Betroffene bestehen im engen Sinne darin, dass Organisationen die in Artikel 5 DSGVO bzw. in Artikel 8 GrCh formulierten Grundsätze nicht beachten. Diese Grundsätze und deren Umsetzung sind es, gegen die jede Verarbeitungstätigkeit – bspw. im Kontext der Datenschutz-Folgenabschätzung gemäß Artikel 35 oder des *Data-Protection-By-Design* gemäß Artikel 25 – zu planen, zu betreiben und nicht zuletzt auch zu prüfen ist. Die Liste konkret erwartbarer Schäden in EG 75 gibt dafür zusätzlichen Halt, sie ist aber bei Weitem nicht hinreichend, um alle wesentlichen Datenschutz-Risiken zu identifizieren und mit Blick auf die betroffenen Personen zu analysieren, zu bewerten und angemessen zu bearbeiten.

Felix Bieker hat einen ungleich überzeugenderen Ansatz vorgestellt, wie die Datenschutz-Risiken auf den Schutz der Rechte und Freiheiten zu fokussieren sind. Bieker macht zunächst die vergleichsweise kurze Passage des EG 75 stark, in der ausdrücklich auch von den „*immateriellen Schäden*" und der „*Verletzung der Rechte und Freiheiten der Personen*" die Rede ist. Zusätzlich zieht er EG 94 hinzu, der noch einmal ausdrücklich besagt, „*... dass ein Risiko nicht nur einen möglichen Schaden, sondern bereits die Beeinträchtigung eines Grundrechts umfasst. Für das Grundrecht auf Datenschutz nach Art. 8 GrCh bedeutet dieses Risiko, dass die – bereits durch jegliche Verarbeitung bestehende – Beeinträchtigung nicht in dem Maße verringert wird, wie es der Schutz der natürlichen Person erfordert.*" (Bieker 2018: 29)

Bezogen auf die technisch-organisatorischen Maßnahmen heißt das: Für eine personenbezogene Verarbeitung sind Vorkehrungen zu treffen, die die Beeinträchtigungen und Risiken für die Rechte und Freiheiten, die bereits durch die bloße Verarbeitungstätigkeit immer und notwendig entstehen, auf das geringst mögliche Maß verringern. Es gilt, nicht erst einen möglicherweise eintretenden materiellen (finanziellen) oder immateriellen (Rufschädigung) Schaden abzuwarten, um einen manifesten Datenschutzkonflikt identifiziert zu haben.

Acht Risikotypen

Viele Kommentatoren, und vor allem viele Datenschutz-Praktiker beziehen sich in einer Risikoanalyse ausschließlich auf die in EG 75 konkret gelisteten Risiken (typisch: Schmitz 2018). Mit den sich daraus ergebenden wenigen Schutzmaßnahmen zur Erhöhung der IT-Sicherheit können Organisationen sehr gut leben. So beruhigt bspw. Veil die Verantwortlichen damit, dass zwar zu berücksichtigen sei, „*... in welchem Ausmaß Risiken durch die konkrete Art der Datenverarbeitung entstehen, aber auch, wie sie bspw. durch technisch-organisatorische Maßnahmen, Transparenzmaßnahmen oder die Möglichkeit*

zur Geltendmachung von Betroffenenrechten wieder begrenzt werden (...). Aus Sicht eines Verantwortlichen können zusätzliche risikobegrenzende Maßnahmen also ein Weg sein, eine Interessensabwägung zu ‚gewinnen'." (Veil 2018: 238, Rn. 143)

Diese Kommentatoren verkennen die Funktion des Rechts bei der Bearbeitung spezifischer Konflikte: Recht macht Konflikte sichtbar, indem es diesen eine kommunizierbare Form gibt.[2] Allerdings löst die rechtliche Bearbeitung eines Datenschutzkonflikts den Konflikt nicht auf; das muss man auch vielen Datenschutz-Jurist*innen immer wieder ins Gedächtnis rufen. Um bspw. Umweltschutz durch ein angemessenes Umweltschutzrecht zu befördern, müssen Sachexpert*innen auch zu den biologischen, chemischen, physikalischen Eigenschaften der Umwelt herangezogen werden, die dem Konflikt zwischen Ökologie und Ökonomie eine kommunikativ zugängliche Form geben können, die sich dann politisch, rechtlich, wissenschaftlich bearbeiten lässt. Für die Umsetzung von Datenschutz müssen analog dazu Expert*innen für Organisationen, Sozialstrukturen und technische Systeme zu Rate gezogen werden. Das war in der ersten Phase der Entwicklung des Datenschutzrechts in den 1970er Jahren auch noch der Fall (vgl. Podlech et al. 1976). Seit der Machtübernahme der Jurist*innen in den Datenschutzaufsichtsbehörden werden materielle Analysen zentraler Datenschutzkonflikte offenbar für entbehrlich gehalten; Datenschutz wird spätestens seit dem Volkszählungsurteil auf Datenschutzrecht reduziert. Ohne die verschiedenen Dimensionen struktureller Datenschutzkonflikte zu berücksichtigen ist es jedoch unmöglich, einen Maßstab für die Beurteilung der Qualität und Wirkung datenschützerischer Aktivitäten zu gewinnen (vgl. Pohle 2018). Der durch Datenschutz zu bearbeitende Konflikt besteht eben gerade nicht im unmittelbaren Abwenden von Schäden für einzelne Personen oder im „*Bewahren einer Schneckenhaus-Privatheit*" (Paul Müller), die es so auch nie gab, sondern in der strukturellen Machtasymmetrie zwischen Organisationen als notorischen Risikogebern und Personen als unterlegenen Risikonehmern. Diese Asymmetrie wird durch die Nutzung der Informations- und Kommunikationstechnik auf Seiten der Organisationen seit den 1980er Jahren beständig verstärkt und hat sich gegenwärtig dermaßen verfestigt, dass es den Anschein hat, als ließe sie sich mit den aktuellen rechtsstaatlichen Normen und kontrollierenden Aktivitäten nicht mehr ausreichend bearbeiten. Mehr noch: Gewaltenteilung, Rechtsstaatlichkeit, Märkte und freie Diskurse als moderne Quellen der personalen Souveränität und Autonomie sind nicht mehr nur bedroht, sondern sie sind dabei, sich aufzulösen.

Es gibt ungleich mehr und andere Risiken für Personen, die der operative Datenschutz deshalb thematisieren und die die Datenschutzaufsichtsbehörden sowohl im Hinblick auf den unmittelbaren Schutz für Betroffene als auch zum Schutz der gesellschaftlichen Strukturen moderner Gesellschaften bearbeiten müssen. Wenn aber niemand den professionellen Datenschützer*innen die Prüfung der real wirksamen Bearbeitung *aller* Risiken tatsächlich abverlangt, dann wird das auch nicht geschehen.[3]

1. Legitimitätsrisiko: Es ist heute durchaus möglich, als Organisation innerhalb der EU eine personenbezogene Verarbeitungstätigkeit zu betreiben, die nicht legitim ist, d. h. genauer: die sich gar nicht grundrechtskonform betreiben lässt, weil schon ihre Zwecksetzung unzulässig ist und die Subjektqualität der betroffenen Personen nicht beachtet. Diese Objektivierung macht den Kern einer jeden „automatisierten Ent-

scheidung“ aus, wenn Maschinen intelligent erscheinend auf Aktivitäten von Menschen reagieren. Automatisierte Einzelfallentscheidungen sind insofern betrieblicher Alltag, selbstverständlich auch bei Organisationen, die ihren Firmensitz innerhalb der EU haben und insofern von der DSGVO erreichbar sind. Diese Formen der Datenverarbeitung sind aber insbesondere bei den durchindustrialisierten Verarbeitungstätigkeiten amerikanischer Kommunikationsfirmen anzutreffen. Wenn offensichtlich illegitime Verarbeitungstätigkeiten, in denen personenbezogene Daten wie Erbsen betrachtet werden, massenhaft betrieben werden können, untergräbt das das Vertrauen von Bürger*innen in die Rechtsordnung. Zugleich ist offensichtlich: Die staatliche Exekutive, insbesondere die Sicherheitsbehörden inklusive ihrer Geheimdienste profitieren vom ungezügelten Agieren der Unternehmen, auf deren Datenbestände gern zurückgegriffen wird.[4] Warum sollte ein Staat diese Win-Win-Situation beenden wollen?

2. Legalitätsrisiko: Selbst wenn eine Organisation mit einer Verarbeitungstätigkeit grundsätzlich legitime Zwecke verfolgt, kann die Rechtsgrundlage, die das Verbot mit Erlaubnisvorbehalt aus Artikel 6 DSGVO (bzw. Artikel 8 der EU-Grundrechtecharta) für den gesondert auszuweisenden Zweck aufheben würde, fehlen oder unzureichend sein. Fehlt eine Rechtsgrundlage, geht das zunächst einmal zu Lasten der Organisation, denn gerade das Fehlen lässt sich leicht feststellen und sanktionieren. Ungleich schwieriger kann es seitens der Datenschutzaufsichtsbehörden oder Gerichte sein zu beurteilen, ob eine vom Verantwortlichen vorgelegte Rechtsgrundlage zur Rechtfertigung einer Verarbeitungstätigkeit ausreicht. Für den Betroffenen bedeutet eine vorhandene, belastbare Rechtsgrundlage vor allem: der/die Verantwortliche hat sich mit der Datenverarbeitung befasst. Das verbessert zumindest die Chancen, dass eine Datenverarbeitung von anderen Verarbeitungen getrennt betrieben wird und auch Maßnahmen der IT-Sicherheit getroffen wurden. Ist der Zweck einer Datenverarbeitung hinreichend eng ausgewiesen, können insbesondere die Erforderlichkeit der Datenerhebung und mögliche „Zweckdehnungen“ im Betrieb vor Gericht nachgewiesen werden. Allerdings spricht die DSGVO bspw. in Art. 24 von Verarbeitungszwecken im Plural und erleichtert rechtlich begründbare Zweckänderung gegenüber den bisher gültigen deutschen Datenschutzregelungen.

3. Modellierungsrisiko: Selbst bei einer datenschutzrechtlich konformen Datenverarbeitung besteht das Risiko, dass in der praktischen Umsetzung des Verarbeitungszwecks die Intensität des Grundrechtseingriffs durch Datenschutzmaßnahmen nicht auf das unbedingt erforderliche Maß verringert wird. Das ist eine häufig anzutreffende Konstellation: Die Datenverarbeitung sieht auf der konzeptionellen Ebene rechtskonform aus, der Betrieb ist es jedoch nicht, allein weil die Intensität des Grundrechtseingriffs nicht auf der Grundlage eines relevanten Angreifermodells bestimmt oder die Intensität unterschätzt wurde. Bei der Modellierung sind deshalb zwei Aspekte zu beachten: a) Es ist ein Angreifermodell zu explizieren: Wer ist Angreifer mit welchen Motiven und Ressourcen? b) Was sind die spezifischen operativen Risiken für den Betroffenen?

zu a) Der Hauptangreifer auf Personen bzw. personenbezogene Daten ist aus Datenschutzsicht immer die datenverarbeitende Organisation selbst, nicht aber bspw. „*der Hacker*“. Dass die Organisation, die die Datenverarbeitung betreibt, als Hauptangreifer zu modellieren ist, bildet den Kern jeder grundrechtlich orientierten Risikobestimmung und Datenschutzanalyse. Hiervon ausgehend gilt es, weitere strukturelle Angreifer-Organisationen zu identifizieren und deren Zugriffsmotive und -ressourcen auf eine Verarbeitungstätigkeit abzuschätzen. Konkret sind dabei die Sicherheitsbehörden, die Leistungsverwaltung, die Bereitsteller von IT-(Infrastruktur)Diensten und kritischen Infrastrukturen (wie Energieversorger), Versicherungen und Banken, die Finanzämter, die Forschungsinstitute (insbesondere psychologischer und sozialwissenschaftlicher Art), Krankenhäuser, Ärzte, Rechtsanwälte, aggressive Start-ups und Werbeagenturen in Betracht zu ziehen. Am Ende bilden dann natürlich auch Hacker bzw. Cracker ebenso wie bspw. untätige Datenschutzbeauftragte oder Datenschutz-Aufsichtsbehörden ein zu beachtendes Risiko für Betroffene.

zu b) Die spezifischen operativen Risiken, die durch Schutzmaßnahmen zu bearbeiten sind, sind den Anforderungen der DSGVO zu entnehmen. Einen konkretisierenden ersten Ausgangspunkt bilden die Grundsätze aus Artikel 5 DSGVO. Artikel 5 enthält, teilweise unnötig verklausuliert, sieben Schutzziele. Negiert man diese Grundsätze - eine Datenverarbeitung wird nicht sicher verfügbar, nicht integer, nicht vertrauenswürdig, nicht transparent, nicht eng zweckbestimmt, nicht änderbar und nur mit den unbedingt nötigen Datenvolumen betrieben - dann lassen sich aus diesem Ansatz heraus konkrete Schutzmaßnahmen gewinnen. So muss eine Verarbeitung personenbezogener Daten redundant ausgelegt sein, es müssen Datenbestände und Kommunikationen verschlüsselt erfolgen, alles muss spezifiziert, dokumentiert und protokolliert sein, es muss wirkungsvoll geändert und gelöscht werden können usw.. Das alles immer mit dem Blick darauf, dass die betroffenen Personen zu schützen sind, nicht die Organisationen. Die deutschen Datenschutz-Aufsichtsbehörden empfehlen, ebenso wie das Bundesamt für Sicherheit in der Informationstechnik (BSI), zur Bestimmung angemessener Schutzmaßnahmen die Anwendung des Standard-Datenschutzmodells (SDM).[5]

Eine Risikoanalyse derart methodisch entlang eines Angreifermodells zu entwickeln, das die Organisation als Angreifer begreift und die betroffenen Personen als zu schützen in den Mittelpunkt stellt, und die sich dabei auch nicht auf Risiken und Sicherheitsmängel der IT beschränkt, ist natürlich heikel. Es fehlt in vielen Organisationen, aber auch bei vielen Datenschutzaufsichtsbehörden, an der Bereitschaft und der Erfahrung, den Datenschutzkonflikt derart klar herauszuarbeiten. Wenn die nunmehr verlangte Datenschutz-Folgenabschätzung in Artikel 35 DSGVO ernsthaft durchgeführt wird und sich die Datenschutz-Aufsichtsbehörden nicht mit schlechten Simulationen davon abspeisen lassen, wird es für Organisationen schwieriger als bislang werden, diesen Konflikt ins Unkenntliche zu verschmieren (vgl. Forum Privatheit 2017).

4. Transparenzrisiko: Selbst wenn eine Organisation eine legitime Verarbeitungstätigkeit rechtskonform betreibt und den Grundrechtseingriff auf das nach dem Stand der Technik minimale Maß reduziert, so ist diese Tätigkeit vielfach in den realen Aus-

wirkungen nicht transparent im Sinne von beobachtbar oder sogar messbar. Viele Eigenschaften von IT-Systemen (Hardware/Software) und Prozessabläufen können in der Praxis nicht geprüft werden, weder durch Betroffene noch durch die Datenschutzaufsichtsbehörden, noch durch die verantwortliche Organisation (bzw. deren interne Datenschutzbeauftragte). Meist scheitert dies allein an der mangelnden Prüfkompetenz, da die Komplexität insbesondere der Informationstechnik sehr groß geworden ist. Die Transparenz einer Datenverarbeitung herzustellen ist dabei kein Selbstzweck (vgl. Engeler 2018), Transparenz hat allein eine dienende Funktion: Sie ist wesentliche Voraussetzung für die Kontrollierbarkeit (für das Zusammenstellen aller für die Verarbeitungstätigkeit relevanten Komponenten), die Prüfbarkeit (Soll-Ist-Abgleich der Aktivitäten der Komponenten) und die Beurteilbarkeit (der Prüfergebnisse durch Jurist*innen) von Verarbeitungstätigkeiten im Hinblick darauf, ob Verantwortliche die Grundsätze insbesondere des Artikels 5 sowie weiterer Anforderungen der DSGVO beachtet und wirksam umgesetzt haben. Eine Organisation die beabsichtigt, Datenschutz-Anforderungen nachzukommen, und die Schutzmaßnahmen und Prüftools installiert, muss allerdings damit rechnen, dass sogar von diesen Maßnahmen neue Risiken ausgehen, die nicht zu erkennen und zu bewältigen sind.

5. Zweckbindungsrisiko: Selbst wenn eine Organisation ordnungsgemäß rechtskonform und transparent bzw. prüfbar personenbezogene Daten verarbeiten sollte, so ist im laufenden Betrieb permanent damit zu rechnen, dass die Organisation den mit der Rechtsgrundlage ausgewiesenen Zweck unterläuft, ausdehnt oder erweitert. Dies kann vorsätzlich, etwa durch den Einsatz von Big-Data-Technologien, oder spontan angeregt durch besondere sich ergebende Gewinnmitnahmechancen, durch „leichte Unfairness“ oder durch die schleichende Ausbildung einer leichtsinnigen Kultur des weitgehend zweckbefreiten Datenumgangs passieren. Typisch werden in sicherheitskritischen Ausnahmesituationen Regeln missachtet und Schutzmaßnahmen umgangen. Das schleichende Unterlaufen des ursprünglichen Verarbeitungszwecks geschieht oft durch neue IT-Optionen und Schutzmaßnahmen, die zur Überwachung von Mitarbeiter*innen genutzt werden, deren Nutzung aber nicht durch den Zweck gedeckt ist. Viele der in der zweiten Hälfte von EG 75 aufgezählten Schäden unterfallen dem hier angesprochenen Risikotypus.

6. IT-Sicherheitsrisiko: Natürlich ist es ein Risiko für Betroffene, wenn eine Organisation keine angemessene Auswahl und Dimensionierung an Schutzmaßnahmen für ihren operativen Datenschutz und ihre IT-Sicherheit getroffen hat. Diese Risiken sind es, die der EG 75 besonders klar und gut in den Blick stellt und die durch Grundschutzmaßnahmen des BSI bearbeitbar sind. Ein weiteres, häufig unbeachtetes Risiko im Kontext der IT-Sicherheit ist allerdings die Notwendigkeit, dass die IT-Schutzmaßnahmen ihrerseits nach Maßgabe des Datenschutzrechts bzw. des operativen Datenschutzes zu konfigurieren sind. Denn auch die Maßnahmen der IT-Sicherheit müssen grundrechtskonform betrieben werden. Nicht datenschutzkonform betriebene IT-Sicherheitsmaßnahmen intensivieren in aller Regel den Grundrechtseingriff.

7. Datenschutzdurchsetzungsrisiko: Unterlassene oder mangelhafte Datenschutzkontrollen stellen ein in der Praxis sehr hohes Datenschutz-Risiko dar. Dieses Risiko resultiert nicht primär aus der skandalös geringen personellen Ausstattung der Datenschutz-Aufsichtsbehörden (vgl. Schulzki-Haddouti 2015), sondern mehr noch aus deren mangelhafter Prüfqualität.

Selbst wenn personenbezogene Verarbeitungstätigkeiten von Aufsichtsbehörden geprüft werden, dann ist in der Regel unklar, was genau und wie Datenverarbeitungen geprüft wurden. Die Transparenz und Integrität der meisten Datenschutzprüfungen durch die Aufsichtsbehörden ist massiv infrage zu stellen, wenn keine Auskünfte über den Prüfstandard und die Prüfmethode gegeben und keine Prüfkonzepte, Prüfdokumente und Prüfprotokolle vorgelegt werden können, die über das Niveau kurzer Rechenschaftsberichte für das Parlament hinausgehen.

Den Anforderungen, die Datenschutzaufsichtsbehörden an die Verarbeitungstätigkeiten anderer Organisationen stellen, müssen die Kontrollbehörden gegenüber ihren Verfahren – nämlich Verarbeitungstätigkeiten anderer Organisationen zu überwachen und die Anforderungen der DSGVO durchzusetzen (vgl. Art. 57, Abs. 1 lit. a DSGVO) – selbst genügen. Selbst wenn Datenschutzprüfungen im Sinne des Art. 5 DSGVO hinreichend transparent, integer, zweckorientiert usw. durchgeführt werden, bspw. mit Rückgriff auf das bereits erwähnte Standard-Datenschutzmodel, so bleiben negative Prüfergebnisse seitens der Aufsichtsaufsichtsbehörden vielfach ohne Konsequenzen für den verantwortlichen Datenverarbeiter. Negative Prüfergebnisse führen darüber hinaus auch nicht zwingend zur Verbesserung von Verarbeitungstätigkeiten, selbst wenn Sanktionen erfolgten. Bei mehrfachen Beanstandungen im Tätigkeitsbericht eines Landesbeauftragten verliert sich, wenn keine weiteren Konsequenzen hinzutreten, schnell der ohnehin mäßige Sanktionscharakter.

Aber selbst wenn eine Datenschutz-Aufsichtsbehörde einen Datenschutzkonflikt mit den Verantwortlichen vor Gericht bringt, entscheiden Gerichte vielfach nicht in der Sache, sondern retten sich mit der Beanstandung von Formfehlern. Und selbst wenn ein Gericht bereit ist, in der Sache zu entscheiden, dann erweisen sich die gesetzlichen Regelungen oft als unzureichend – was wiederum auf das anhaltend mangelnde Interesse des Gesetzgebers am Datenschutz schließen lässt.

8. Politikrisiko: Gegenwärtig ist in Deutschland keine Partei auszumachen, die den vom Datenschutz zu bearbeiten Konflikt und die daraus resultierenden Grundrechtsrisiken analytisch auf den Grund zu gehen vermag, von Einzelpersonen insbesondere bei den Grünen abgesehen. Das gleiche gilt für NGOs oder Interessensvertretungen, denen über sinnfällige Skandalisierungen hinaus schnell die Luft ausgeht (vgl. Rost 2017). Betroffene haben aktuell keinen mächtigen Anwalt ihrer Interessen; die Schutzfunktion der Datenschutz-Aufsichtsbehörden ist nicht mehr nennenswert. Das vorherrschende *Framing* (vgl. Wehling 2016) der politischen Diskurse zum Datenschutz verzwergt und trivialisiert die wirksame Umsetzung von Grundrechten entweder, wie oben gezeigt, zur Privatangelegenheit oder zu einem Risiko der IT-Sicherheit und nimmt den Datenschutzgesetzen ihre Schärfe, wenn anstatt auf deren Durchsetzung zu dringen wohlfeile Ethik-Diskurse geführt werden, wie das der europäische Datenschutzbeauftragte Butarrelli gern praktiziert. Das alles nützt einzig den ohnehin

übermächtigen Organisationen, die die gesellschaftlichen Kommunikationen weiter ausformen und beherrschen. Wenn Datenschutz parteipolitisch nicht mehr auf Resonanz stößt – das war mal anders –, dann könnte dies ein Indikator dafür sein, dass die Gesellschaft sozialstrukturell in die Vormoderne zurückzufallen droht – also in eine Zeit, als wenige Organisationen und einzelne Personen noch strikt hierarchisch das Leben von Menschen bestimmten. Zugespitzt formuliert lautet die These: Gegenwärtig können wir dabei zusehen, wie eine moderne, und das heißt soziologisch fundiert formuliert, funktional-differenzierte Gesellschaft entweder zu einer stratifizierten Gesellschaft regrediert (so Rost 2012) oder alt wird (so Lehmann 2015). An der wirksamen Umsetzung von Grundrechten zeigt sich, ob Modernisierungschancen der funktionalen Differenzierung genutzt werden.

Fazit

Die Zuspitzung der Interpretation von Risiken der DSGVO auf einen *risk-based-approch* wird selbst zum Risiko für einen an der wirksamen Umsetzung von Grundrechten interessierten Datenschutz, wenn sich der Fokus auf die in Erwägungsgrund 75 DSGVO aufgelisteten konkreten Schäden und Kontrollverluste reduziert. Es geraten zumindest die grundrechtlich wesentlichen Risiken für Personen dann in den Blick, wenn der für den Datenschutz konstitutive Konflikt der asymmetrischen Machtbeziehung zwischen den Risiken erzeugenden Organisationen und Personen zum Ausgangspunkt von Risikoanalysen wird. Die DSGVO gibt, insbesondere mit den Grundsätzen der Datenverarbeitung in Artikel 5 sowie den auf die wirksame Umsetzung abzielenden Artikeln 24, 25, 32 und 35, einen guten Rahmen für die Bestimmung und Dimensionierung technisch-organisatorischer Maßnahmen zur Verringerung einer Vielzahl von Datenschutz-Risiken. Ohne eine politisch gewollte massive Stärkung der Datenschutz-Aufsichtsaktivitäten, die auch zu wirksamen Sanktionen führen, ist allerdings, gerade wegen des Einsatzes besonders wirksamer moderner Überwachungstechniken, der gesellschaftliche Rückfall wieder in die Vormoderne wahrscheinlich.

MARTIN ROST Martin Rost arbeitet als stellvertretender Leiter des Technikreferats des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Er leitet die Unterarbeitsgruppe „Standard-Datenschutzmodell“ des „Arbeitskreis Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Deutschlands.

Literatur

Bieker, Felix, 2018: Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, in: Datenschutz und Datensicherheit (DuD), 2018, Nr. 1: 27-31.

BSI 2017: Standard-200-3, Risikoanalyse auf der Basis von IT-Grundschutz, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html (abgerufen: 20.01.2018).

BVerfG 2008: Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 (=BVerfGE 120, 274 - 350), „Grundrecht auf Gewährleistung der *Vertraulichkeit* und Integrität informationstechnischer Systeme“.

Engeler, Malte, 2018: Das überschätzte Kopplungsverbot. Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen; in: Zeitschrift für Datenschutz (ZD), Nr. 2: 55ff.

Forum Privatheit, 2017: Whitepaper Datenschutz-Folgenabschätzung, 3. überarbeitete Auflage, https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (abgerufen: 20.01.2018).

Lehmann, Maren, 2015: Das »Altwerden funktionaler Differenzierung« und die »nächste Gesellschaft«, in: Soziale Systeme (Special Issue), Jg. 20, Nr. 2: 308-336.

Podlech, Adalbert; Dierstein, Rüdiger; Fiedler, Herbert; Schulz, Arno (Hg.), 1976: Gesellschaftstheoretische Grundlage des Datenschutzes, Datenschutz und Datensicherung, Bachem-Verlag: 311-327.

Pohle, Jörg, 2018: Datenschutz und Technikgestaltung (Dissertation, im Erscheinen).

Robrahn, Rasmus; Bock, Kirsten, 2018: Schutzziele als Optimierungsgebote; in: Datenschutz und Datensicherheit (DuD), 2018, Nr. 1: 7-12.

Rost, Martin, 2012: Zur Soziologie des Datenschutzes; in: Datenschutz und Datensicherheit (DuD), Nr. 37: 85-91.

Rost, Martin, 2013: Eine kurze Geschichte des Prüfens, in: BSI (ed.), Informationssicherheit stärken – Vertrauen in die Zukunft schaffen, Secumedia-Verlag: 25-35.

Rost, Martin, 2017: Bob, es ist Bob!, in: FifF-Kommunikation, Jg. 34, Nr. 4: 63-66.

Schmitz, Barbara, 2018: Der Abschied vom Personenbezug. Warum der Personenbezug nach der DS-GVO nicht mehr zeitgemäß ist; in: Zeitschrift für Datenschutz (ZD), Nr. 2: 5-8.

Schulzki-Haddouti, Christiane, 2015: Zu kurz gekommen. Deutsche Datenschutzbehörden leider unter Personalknappheit; in: c‘t 2015, Nr. 17: 76-78.

SDM 2016: Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V 1.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.0.pdf (auch in englischer Version verfügbar; abgerufen: 20.01.2018).

Veil, Winfried, 2018: Risikobasierter Ansatz; in: Gierschmann, S.; Schlender, K.; Stentzel, R.; Veil, W., 2018: Kommentar Datenschutz-Grundverordnung, 1. Aufl., Köln, Bundesanzeiger-Verlag: 712ff.

Wehling, Elisabeth, 2016: Politisches Framing. Wie eine Nation sich ihr Denken einredet – und daraus Politik macht; edition Medienpraxis 14.

Anmerkungen:

1 Versicherbare Risiken können in Preise hinein verrechnet werden. Nicht-bezifferbare und deshalb auch nicht versicherbare Risiken lassen sich jedoch nicht verrechnen. Als Beispiel für eine zivilrechtliche Behandlung ließe sich an ein Sammelklagesystem mit dem Ziel eines nicht prognostizierbaren und deshalb nicht versicherbaren Strafschadenersatzes etwa US-amerikanischer Prägung denken.

2 Der gesellschaftliche Bezug, den die DSGVO in den EG 4 und 6 herstellt, ist auffallend schwach ausgebildet und offenbar von dem Motiv getrieben, dass Datenschützer Verständnis für die besonderen Nöte der Datenverarbeiter aufbringen sollen. Man muss grundrechtlich nicht zwingend die Vorstellung teilen, dass durch die „Globalisierung Datenschutz vor neuen Herausforderungen steht“ (EG 6). Das leitet schon analytisch fehl, weil es nicht „die Globalisierung“ sein kann, sondern es international agierende Organisationen sind, die sich nicht an Grundrechte halten, u. a. weil ihre Aktivitäten keiner wirksamen Datenschutzkontrolle unterliegen.

3 Eine intrinsische Motivation gilt unter Verwaltungsmitarbeiter*innen als unprofessionell. Dabei sind die Mitarbeiter*innen einer oder eines Beauftragten für den Datenschutz keine neutralen Verwaltungsmitarbeiter*innen und auch keine Richter*innen, die alle beteiligten Interessen abzuwägen haben: Sie sollen entschieden Partei für Betroffene ergreifen.

4 Das ist natürlich auch dem Bundesverfassungsgericht längst aufgefallen. Prof. Voßkuhle, der aktuelle Präsident des Bundesverfassungsgerichts, deutete bereits im November 2011 an, dass sich das BVerfG mit Facebook beschäftigen werde. „*Verfassungsgerichtspräsident warnt vor Facebook (…) Er deutete an, dass das Bundesverfassungsgericht gezwungen sein könnte zu prüfen, ob sich das Facebook-Angebot mit dem Recht auf informationelle Selbstbestimmung verträgt. ‚Da will ich dem für solche Fragen zuständigen Ersten Senat nicht vorgreifen. Es spricht jedenfalls einiges dafür, dass das Bundesverfassungsgericht in den nächsten Jahren gefordert sein wird, die Bedeutung und Reichweite der Grundrechte in einer Welt der digitalen Vernetzung neu zu bestimmen.‘*“ (RP-Online v. 6.11.2011, http://www.rp-online.de/digitales/internet/verfassungsgerichtspraesident-warnt-vor-facebook-aid-1.2542329, abgerufen: 21.01.2018).

5 Bislang ist Anwendung des SDM in einigen Aufsichtsbehörden allerdings noch keine gängige Prüf- und Beratungspraxis (vgl. SDM 2016).