6 Fortentwicklung des Datenschutzrechts

Für viele Regelungen der Datenschutz-Grundverordnung musste festgestellt werden, dass sie den gegenwärtigen Herausforderungen des Datenschutzes nicht gerecht werden, dass diese Defizite aber nicht durch kleine Wortlautänderungen behoben werden können. Vielmehr erfordern diese Defizite grundsätzliche Diskussionen der hinter ihnen stehenden Regelungskonzepte. Daher werden in diesem Kapitel wichtige Fragen dieser Regelungsaspekte aus Sicht des Verbraucherschutzes diskutiert. Im ersten Schritt werden wichtige Herausforderungen des Datenschutzes heute und morgen angesprochen, denen das Datenschutzrecht gerecht werden muss. Im zweiten Schritt werden konzeptionelle Mängel der Datenschutz-Grundverordnung angesprochen, die verhindern, dass sie den Herausforderungen gerecht werden kann, und diskutiert, welche konzeptionellen Ansätze stattdessen verfolgt werden sollten. Im darauffolgenden Kapitel wird dann erörtert, auf welchen Wegen die notwendige Modernisierung des Datenschutzrechts in der Europäischen Union und in der Bundesrepublik Deutschland erreicht werden könnte.[482]

6.1 Datenschutz in der Welt von heute

Die gegenwärtige Datenschutz-Governance zeichnet sich durch eine Ko-Regulierung durch die Europäische Union und die Mitgliedstaaten aus, die aus den zahlreichen Öffnungsklauseln und Regelungsaufträgen der Datenschutz-Grundverordnung folgt. Darüber hinaus finden sich in der Datenschutz-Grundverordnung weite Erlaubnistatbestände mit hoher Selbstbestimmung der Verantwortlichen. Zahlreiche Defizite gibt es bei der Information der Verbraucher sowie bei der Einwilligung und den anderen Erlaubnistatbeständen.[483] Auch die Reichweite der Betroffenenrechte ist vielfach unklar, zumal diese stark einschränkbar sind. Die technikneutralen Regelungen der Datenschutz-Grundverordnung schlagen in eine Risikoneutralität um, die den Risiken und der Komplexität moderner Datenverarbeitung in allen Wirtschafts-, Gesellschafts- und Verwaltungsberei-

482 S. Kap. 7.
483 S. Kap. 3.4 bis 3.9.

chen nicht gerecht wird.[484] Die Aufsichtsbehörden wurden indes zwar mit neuen Aufgaben versehen,[485] gleichzeitig sind sie in ihrer Aufgabenwahrnehmung aber durch unzureichende finanzielle wie personelle Ausstattungen behindert. Die aufwandsreichen Abstimmungsverfahren unter den Aufsichtsbehörden, die die Verordnung vorsieht, dürften zwar mittel- und langfristig zu einer größeren Harmonisierung führen, sind aber zunächst eine zusätzliche Belastung für die Aufsichtsbehörden.[486] Der Erfolg zahlreicher Innovationen der Datenschutz-Grundverordnung ist an hohe Anforderungen an ihre Umsetzung gekoppelt, die weder in der Datenschutz-Grundverordnung geregelt noch in der politischen Umsetzung gesichert sind.[487]

Gerade besonders populäre Dienstleistungen des digitalen Zeitalters werden heute ohne monetäre Gegenleistung angeboten und stattdessen durch die Preisgabe personenbezogener Daten durch die Nutzer entlohnt.[488] Diese Daten stellen das eigentliche Produkt dar; die Finanzierung der Dienstleistung erfolgt durch Leistungen Dritter, die beispielsweise personalisierte Werbung schalten lassen. Die Verarbeitung dieser Daten verspricht mitunter enorme Gewinne und löst so Begehrlichkeiten aus. Diese Verarbeitung kann Grundlage sein, um umfassende Profile zu erstellen, und ermöglicht so eine personalisierte Ansprache des Verbrauchers. Diese ist zwar insofern zu dessen Vorteil, als sie auf dessen (vermeintliche) Bedürfnisse zugeschnitten ist, wirkt aber verhaltensbestimmend und schränkt durch ihre algorithmenbasierte Vorauswahl die autonome Willensbildung des Verbrauchers ein. Sie kann sich sogar unmittelbar ins Negative kehren, wenn der Verantwortliche etwa bestimmte Eigenschaften des Verbrauchers zu dessen Manipulation ausnutzt.

Die Datenschutz-Grundverordnung war mit dem Ziel angetreten, eine umfassende Modernisierung und Harmonisierung des europäischen Datenschutzes zu bewirken, gleichzeitig aber auch positive ökonomische Effekte im europäischen Binnenmarkt mit einem verbesserten Grundrechtsschutz natürlicher Personen zu verbinden.[489] Der Modernisierungsbedarf des Datenschutzrechts ergab sich aus zahlreichen technischen Entwicklungen, die letztlich zur Entstehung neuer Datenquellen sowie neuer Mög-

484 S. näher Kap. 6.3.1.
485 S. hierzu näher Roßnagel, Datenschutzaufsicht, 2017.
486 S. Datenschutzkonferenz, Erfahrungsbericht, 2019, 21 ff.
487 S. die Beiträge in DuD 8/2019.
488 Kugelmann, DuD 2016, 566.
489 So die Erwägungsgründe 1, 2, 4, 5, 6, 7, 10 und 13 DSGVO.

lichkeiten der Vernetzung dieser Datenquellen und damit zu einer sowohl quantitativen wie auch qualitativen Zunahme der Verarbeitung personenbezogener Daten führte. Die so gewonnenen Daten können bei immer weiter steigender Rechenleistung und ständig verbesserten Analyseverfahren trotz immenser Datenmassen auch immer besser und schneller zusammengeführt und ausgewertet werden.[490] Diese Entwicklung ist dabei keineswegs abgeschlossen, sondern stellt das Datenschutzrecht vor weiterhin ungelöste Herausforderungen. Als Schlagworte seien hier Smart Car,[491] Smart Health,[492] Smart Home,[493] Smarte Assistenten[494] und Robotik[495] sowie als Oberbegriffe Ubiquitous Computing, Internet of Things, Artificial Intelligence und Big Data genannt. Die Techniken bereiten den Weg für einen immer stärker informatisierten Alltag,[496] in dem Erkenntnisse über die betroffene Person nicht nur aus den von dieser direkt eingegebenen Informationen (etwa in einem Social Network) abgeleitet werden, sondern gerade auch aus einer immer weiter verbreiteten Beobachtung des Verhaltens der Person im alltäglichen Leben – auch in privaten Räumen. Diese Erkenntnisse können dann in Form von Profilen und algorithmenbasierten Einordnungsverfahren für die Bewertung von Verbrauchern sowie etwa in Form von Microtargeting für die Verhaltensbeeinflussung zum Zweck der Werbung für Dienstleistungen und Produkte, der Wahlinformation und vieler anderer Zwecke genutzt werden.

Sind bereits mit Blick auf aktuelle Datenverarbeitungen zahlreiche datenschutzrechtliche Probleme ungelöst, so kündigen sich durch die dargestellte technische Entwicklung der Verarbeitung personenbezogener Daten und die diese ausnutzenden Geschäftsmodelle bereits neue Problemfelder an. Besondere Herausforderungen für das Recht stellen „intelligente" Systeme dar, die auf Basis einer umfänglichen Sensorik algorithmenbasierter Verfahren perspektivisch eine umfassende Unterstützung des Verbrauchers in allen Lebenslagen in Aussicht stellen. Das System kann dann als Erweiterung des menschlichen Gedächtnisses fungieren und einfache Aufgaben

490 S. zu den Herausforderungen von Big Data für das Recht z.B. Hoffmann-Riem, 2018.
491 S. hierzu umfassend Roßnagel/Hornung, 2019.
492 S. z.B. Jandt, DuD 2016, 571; Dochow, 2017.
493 S. z.B. Skistims, 2016; Geminn, DuD 2016, 575.
494 S. z.B. Thies/Knote u.a., in: Roßnagel/Friedewald/Hansen, 2018, 175; Knote u.a., Informatik Spektrum, 2020, 118 ff.; Thies/Knote/Jandt/Söllner, DuD 2020, Heft 9, i.E.; Steidle, 2005.
495 S. z.B. Keßler, MMR 2017, 589.
496 S. Roßnagel, 2007.

des Alltags ganz übernehmen, gleichzeitig aber auch bei komplexen Tätigkeiten Hilfestellung geben. Gegenüber den immensen Vorteilen solcher Systeme treten die Nachteile durch die zugrundeliegende Verarbeitung personenbezogener Daten in der Wahrnehmung des Verbrauchers in den Hintergrund.

6.2 Datenschutzherausforderungen in der Welt von morgen

Die Entwicklung von Techniken, die für die Verarbeitung und Nutzung von Verbraucherdaten genutzt werden können, und die Entwicklung von Geschäftsideen, diese Techniken für die Erfassung und Beeinflussung von Verbraucherverhalten einzusetzen, werden viele weitere und derzeit noch unbekannte Herausforderungen für den Verbraucherdatenschutz hervorrufen. Diese sind sehr schwer vorherzusehen. Wichtig ist daher, dass das Datenschutzrecht so konzipiert ist, praktiziert wird und angepasst werden kann, dass es mit all diesen Herausforderungen konstruktiv umgehen kann. Dies wird im Folgenden bei der Konzipierung von Entwicklungsideen zum Datenschutzrecht berücksichtigt.

Eine Entwicklung ist aber im Kontext von Big Data und Künstlicher Intelligenz bereits heute schon gut absehbar: Die immer stärkere Auswertung der explodierenden Mengen an personenbezogenen Daten der Verbraucher in Form ihrer Quantifizierung und Verwendung in Maßnahmen der Verhaltensbeeinflussung und menschlichen oder automatisierten algorithmenbasierten Entscheidungsverfahren.

Der Verbraucher der Zukunft wird jederzeit von digitalen Infrastrukturen umgeben sein und durch alle seine Handlungen in diesen Strukturen Datenspuren hinterlassen, die zur Ausbeutung durch Anbieter und Dritte zur Verfügung stehen. Diese legen auf der Basis algorithmenbasierter Datenverarbeitungssysteme von ihren Nutzern Profile an, schließen aus den erfassten Merkmalen auf Eigenschaften dieser Personen und übertragen diese statistisch erwiesenen Eigenschaften auf alle, die diese Merkmale aufweisen. Daher sind alle in der Statistik gefangen – auch wenn sie sich ihr entziehen wollen.[497] Sie sind unentrinnbar Teil einer anonymen Vergemeinschaftung[498] durch algorithmenbasierte Systeme. Beispielsweise verhindert dann in einer digitalisierten Verkehrsinfrastruktur auch die Nutzung eines unvernetzten Fahrzeugs nicht die Erfassung durch diese smarte

497 S. hierzu Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 365 ff.
498 S. zu dieser z.B. Hubig, in: Roßnagel/Sommerlatte/Winand, 2008, 165 ff.

Infrastruktur und die Erfassung aller anderen, vernetzten Verkehrsteilnehmer. Auch durch bewusste Technikaskese kann der einzelne es nicht vermeiden, etwa von automatisierter Entscheidungsfindung betroffen zu sein. Dies schließt ein, Ziel von Prognosen, Verhaltensbeeinflussungen und algorithmenbasierten Entscheidungen zu sein, die auf diesen Statistiken beruhen.[499] Das Konzept von Einwilligung und individueller Selbstbestimmung wird dadurch grundsätzlich infrage gestellt. Der Einzelne verliert die Kontrolle darüber, „wer was wann und bei welcher Gelegenheit" über ihn weiß.[500] Die Statistik wirkt auch gegenüber dem, der nicht an ihrem Zustandekommen durch Datenpreisgabe mitgewirkt hat.

Statistiken, wie sie zur Mustererkennung bei Big Data-Analysen oder beim Lernen von algorithmenbasierten Systemen eingesetzt werden, wirken normbildend und verhaltensbestimmend. Sie korrelieren Verhaltensmerkmale und beschreiben „normales" und „abweichendes" Verhalten. Wenn an diese Muster oder Modelle positive und negative menschliche oder automatisierte Entscheidungen anknüpfen, werden sich die Menschen diesen Mustern und Modellen anpassen, um in den Genuss der positiven Wirkungen zu gelangen und negative zu vermeiden. Durch sie unterliegt jeder der „Normativität der Normalität".[501] Wer nicht auffallen oder bestimmte algorithmenbasiert getroffene Entscheidungen beeinflussen will, akzeptiert die erwartete Normalität als Verhaltensnorm. Verhaltensmuster und -modelle können durch diese Normbildung indirekt, aber wirkungsvoll die Wahrnehmung von Grundrechten beeinflussen. Die anonymen Muster wirken auf diese Weise genauso negativ auf die Persönlichkeitsentfaltung des Einzelnen und die freie Kommunikation und Willensbildung in der Gesellschaft insgesamt ein, wie dies das Bundesverfassungsgericht bereits im Volkszählungsurteil als Auswirkungen personenbezogener Überwachung festgestellt hat.[502]

6.3 Vorschläge zur Fortentwicklung des Datenschutzes

Im Folgenden werden Ansätze zur Weiterentwicklung des Datenschutzes angesprochen, die sich nicht auf einzelne Regelungen der Datenschutz-

499 S. Roßnagel, ZD 2013, 562 (566); Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 365 ff.
500 BVerfGE 65, 1 (43).
501 Weichert, ZD 2013, 251 (258); Roßnagel, ZD 2013, 562 (566).
502 BVerfGE 65, 1 (43).

Grundverordnung, sondern auf Regelungskonzepte beziehen, die ihr zu Grunde liegen oder die sie verfolgen sollte, um den absehbaren Herausforderungen in der Zukunft gerecht werden zu können. Hierzu werden aus Verbrauchersicht die Möglichkeiten einer risikoadäquaten Weiterentwicklung des geltenden Datenschutzrechts sowohl auf Ebene der Europäischen Union als auch auf Ebene der Mitgliedstaaten beleuchtet und konzeptionelle Beiträge unterbreitet, um die notwendige Diskussion zu einer risikoorientierten Modernisierung des Datenschutzrechts anzuregen (6.3.1). Weiterhin wird geprüft, wie konzeptionell die Stellung der Verbraucher gestärkt (6.3.2) und ihre Überforderung verhindert werden kann (6.3.3). Da durch moderne Datenverarbeitungssysteme auch dritte Verbraucher, die nicht selbst betroffene Personen sind, beeinträchtigt sein können, erstreckt sich die Prüfung auch auf die Frage, wie sich diese Beeinträchtigungen bewerten und steuern lassen (6.3.4). Schließlich folgen konzeptionelle Überlegungen, wie das Recht die Datenschutzprinzipien stärken kann (6.3.5).

6.3.1 Risikoadäquate Weiterentwicklung oder Ergänzung des Datenschutzrechts

Ein wesentlicher Schwachpunkt der Datenschutz-Grundverordnung ist ihre zu weitgehende Risikoneutralität. Sie beachtet zwar Risiken der Datenverarbeitung, um die Belastungen der Verantwortlichen zu reduzieren.[503] Risikobetrachtungen finden jedoch nicht statt, wenn es um den Schutz von Grundrechten und Freiheiten der betroffenen Person geht. Der Datenschutz-Grundverordnung fehlen risikoadäquate Differenzierungen der Datenschutzgrundsätze, der Zulässigkeit der Datenverarbeitung und der Betroffenenrechte. Auch wo die Datenverarbeitung sehr unterschiedliche Grundrechtsrisiken verursacht, finden die gleichen abstrakten Regelungen Anwendung – etwa für die wenig riskante Kundenliste eines Handwerkers ebenso wie für die um Potenzen risikoreicheren Datenverarbeitungsformen des Internet der Dinge, von Big Data, Cloud Computing und

503 Vor allem in ihrem Kapitel IV stellt die DSGVO die Pflichten der Verantwortlichen unter Risikovorbehalt – s. z.B. Art. 24, 25, 30, 32, 33, 34, 35, 36 und 37 DSGVO – mit der Folge, dass in der Praxis diese Pflichten nur für einen Bruchteil der Verantwortlichen tatsächlich wirksam werden – s. hierzu auch Albrecht, CR 2016, 88 (94); Roßnagel, DuD 2016, 561 (565); Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 375 f.

datengetriebenen Geschäftsmodellen. Die Datenschutzpraxis berichtet: „Gerade kleinere Wirtschaftsakteure und insbesondere Vereine übten dahingehend Kritik, dass sie von den Anforderungen der Datenschutz-Grundverordnung in gleicher Weise berührt sind wie datenhungrige Großkonzerne und Soziale Netzwerke."[504] Gerade diese ungerechtfertigte Risikoneutralität ist es, die erhebliche Akzeptanzprobleme der Datenschutz-Grundverordnung auf Seiten der Bevölkerung in Europa – und damit Skepsis gegenüber Politik und Rechtsetzung der Europäischen Union insgesamt – hervorzurufen droht.

Der Grund für diese Risikoneutralität ist, dass die Datenschutz-Grundverordnung einer übertriebenen Ausprägung des Grundsatzes der Technikneutralität folgt. Dieser Grundsatz soll im Prinzip das Risiko einer Umgehung rechtlicher Vorschriften minimieren, indem die Datenschutzregelungen „nicht von den verwendeten Techniken abhängen".[505] Richtig verstanden ist eine technikneutrale Regelung dann sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische Weiterentwicklungen ausschließen. Sie ist daher so zu fassen, dass die rechtlichen Vorgaben auch auf weiterentwickelte Techniken anwendbar sind.[506] Dies schließt aus, Regelungen für einzelne *Ausprägungen* einer spezifischen Technikanwendung zu treffen. Dies darf aber nicht verhindern, Vorgaben für bestimmte technische *Funktionen* vorzusehen – insbesondere, wenn eine bestimmte Funktion – wie z.B. Tracking, Gesichtserkennung, Profilbildung oder Scoring – besondere Risiken für Grundrechte verursacht. Denn in einer technikgeprägten Welt kann Grundrechtsschutz nicht erfolgen, wenn nicht auch Risiken durch Technik aufgegriffen und durch die Regulierung technischer Funktionen gesteuert werden. Solche Funktionen können risikospezifisch und datenschutzgerecht reguliert werden, ohne dass im Regelfall die rechtliche Anforderung durch die Weiterentwicklung einer Technik überholt oder nicht anwendbar wird.[507]

Zwar benennt die Datenschutz-Grundverordnung in den Erwägungsgründen 6 und 101 abstrakt die in Kapitel 6.1 geschilderten Herausforderungen, die technischer Fortschritt und Globalisierung für das Datenschutzrecht bedeuten. Sie greift jedoch keine einzige Technikfunktion auf, deren Datenschutzrisiken – wie etwa bei Big Data, Cloud Computing, Internet der Dinge und künstlicher Intelligenz – bereits heute intensiv ge-

504 S. Unabhängiges Datenschutzzentrum Saarland, 2019, 15.
505 S. Erwägungsgrund 15 Satz 1 DSGVO.
506 S. grundsätzlich Roßnagel, in: Eifert/Hoffmann-Riem, 2009, 323 ff.
507 S. hierzu weiter unten in diesem Unterkapitel.

nutzt oder diskutiert werden und die auch noch bei veränderten technischen Merkmalen in vielen Jahren ein Problem für den Datenschutz darstellen.[508] Damit überspannt sie das Konzept der Technikneutralität und wird im Ergebnis risikoneutral.

Ziel der Europäischen Kommission war es, in ihrem Entwurf der Datenschutz-Grundverordnung einen besonders zukunftsoffenen Datenschutzrahmen zu schaffen.[509] Damit bleibt sie aber auch bei den Bedingungen für die Zulässigkeit der Verarbeitung personenbezogener Daten, der Voraussetzungen und Folgen der Betroffenenrechte und der Konkretisierung der Datenschutzprinzipien bei höchst abstrakten Vorgaben. Die Praxis zeigt, dass „der dem Vollharmonisierungsanspruch und der technikneutralen Ausgestaltung geschuldete hohe Abstraktionsgrad einzelner Regelungen der Verordnung… eine Bandbreite an Deutungsmöglichkeiten bietet und dem Anwender die Umsetzung der Vorgaben erschwert".[510] Datenverarbeitungen zu verhindern, die unzumutbare Risiken verursachen, ist nicht das Ziel der Verordnung. Sie knüpft an keiner Stelle die Zulässigkeit besonders riskanter Funktionen der Datenverarbeitung an das Fehlen bestimmter Grundrechtsrisiken oder macht sie von der Bewältigung dieser Risiken abhängig. Doch nur durch die Berücksichtigung typischer Risiken bestimmter Datenverarbeitungsformen im Verordnungstext kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden.

Die Konkretisierung der hochabstrakten Vorgaben für die unendliche Vielfalt von einzelnen Diensten und Anwendungen in allen Gesellschafts-, Wirtschafts- und Verwaltungsbereichen sollte – vom theoretischen Konzept her – den Gerichten, den mitgliedstaatlichen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss überlassen bleiben.[511] In der Praxis bleiben im ersten Zugriff diese Konkretisierungen jedoch den Verantwortlichen überlassen.[512] Sie nutzen die Abstraktheit der Vorgaben, um sie nach ihren Interessen zu praktizieren. So berichten Aufsichtsbehörden: „Ab dem ersten Geltungstag der Datenschutz-Grundverordnung taten eini-

508 Dies ist für Social Networks in Art. 20 DSGVO und für algorithmenbasierte Entscheidungsverfahren in Art. 22 DSGVO allenfalls in abstrakten Ansätzen der Fall. S. zur Kritik an diesen beiden Vorschriften Kap. 3.10 und 3.11.

509 „Es sollte … nicht versucht werden, jede Frage, die den Datenschutz in Europa in den nächsten 20 Jahren beschäftigen könnte, bereits heute im Detail regeln zu wollen", Reding, ZD 2012, 195 (198).

510 Unabhängiges Datenschutzzentrum Saarland, 2019, 16.

511 Reding, ZD 2012, 195 (198).

512 Hierauf besteht auch die Europäische Kommission, Commission Staff Working Document, 15 f.

ge große außereuropäische Anbieter so, als wäre nun der Datenschutz viel laxer zu handhaben. Gerichtliche Untersagungen gegen eine invasive Datenverarbeitung wurden nicht mehr als bindend angesehen, da das neue Datenschutzrecht die entsprechende Verarbeitung angeblich erlauben würde."[513] Die betroffenen Personen, die damit nicht einverstanden sind, müssen sich bei den Aufsichtsbehörden beschweren oder den Gerichtsweg beschreiten. Die Aufsichtsbehörden können im Einzelfall prüfen und notfalls – nach Abstimmung mit anderen Aufsichtsbehörden – eingreifen. Sie sind aber durch die vielen anderen Aufgaben, die ihnen Art. 57 und 70 DSGVO stellen, angesichts ihrer zu geringen Ressourcen überfordert.[514]

Endgültig verbindliche Aussagen zur Auslegung der Datenschutz-Grundverordnung kann jedoch nur der Europäische Gerichtshof treffen. Dieser ist wiederum auf die Vorlage bestimmter Fragen und Themen durch die mitgliedstaatlichen Gerichte angewiesen. Problematisch ist auch die Dauer von Verfahren, bis sie zum Europäischen Gerichtshof gelangen und bis sie von diesem entschieden sind. Wegen der dynamischen Entwicklung der Informationstechnik und ihrer Anwendungen sind die dem Streitgegenstand zugrundeliegenden Datenschutzprobleme oft nicht mehr aktuell, bis durch die Entscheidung des Europäischen Gerichtshofs eine gesicherte Rechtsprechung zu entstehen beginnt. Eine praktikable Lösung, um das Ziel zu erreichen, die vielen Vorgaben der Datenschutz-Grundverordnung zu konkretisieren und die zahlreichen offenen Fragen zu beantworten, die sie verursacht, ist dies nicht.[515] Bis zur abschließenden Klärung einzelner Fragen durch den Europäischen Gerichtshof lädt die Datenschutz-Grundverordnung zu interessengeleiteten Interpretationen und Meinungsstreitigkeiten geradezu ein. Die Machtasymmetrie zwischen großen datenverarbeitenden Unternehmen und Verbrauchern führt vor diesem Hintergrund zu einer Schlechterstellung der Verbraucher.[516]

Technikneutralität ist zur Regelung komplexer Sachverhalte ein unverzichtbares Instrument, sofern die Regelung einzelner technischer Ausprägungen vermieden wird.[517] Zum Problem wird sie dort, wo auch einzelne technische Funktionen nicht risikospezifisch adressiert werden.[518] Letzterem verweigert sich die Datenschutz-Grundverordnung aber, soweit es um

513 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2019, 9.
514 S. Kap. 3.15.
515 Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 376.
516 Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 376 f.
517 S. Roßnagel, in: Eifert/Hoffmann-Riem, 2009, 323 ff.
518 S. hierzu umfassend Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 374 ff.

den Schutz der betroffenen Person geht – zu Unrecht. Diese Form der Regulierung wird den eigenen Zielsetzungen der Verordnung nicht gerecht, die betroffenen Personen vor den Bedrohungen, die sich durch den Einsatz moderner Technik für ihre Grundrechte und Freiheiten manifestieren, zu schützen. Dies zeigt sich exemplarisch bei den neuen Anforderungen wie der Pflicht zum Datenschutz durch Systemgestaltung und durch Voreinstellungen. Diese Vorgaben sind in ihrer Abstraktheit nicht in der Lage, die Entwicklung und den Einsatz der Techniksysteme und Geschäftsmodelle datenschutzgerecht zu steuern.[519]

Dabei sind technik- und bereichsspezifische Regelungen zum Datenschutz in der Union möglich, die gerade nicht der in der Datenschutz-Grundverordnung verfolgten spezifischen Ausprägung von Technikneutralität folgen. Ein bereits existierendes Beispiel hierfür ist Art. 6 eCall-Verordnung (EU) 2015/758[520], der Datenschutzanforderungen beim automatisierten Notruf in Kraftfahrzeugen regelt. Auch die geplante ePrivacy-Verordnung fällt in die Kategorie bereichsspezifischer risikoadäquater Regulierung.[521]

Risikospezifische Regelungen, bei denen sich der Gesetzgeber mit den besonderen Risiken bestimmter Technikanwendungen und Geschäftsmodelle auseinandersetzt, sind im Datenschutzrecht zum Schutz der Grundrechte und Freiheiten der betroffenen Personen unabdingbar. Beispiele für solche risikoadäquaten, aber dennoch technikneutralen Regelungen, die überwiegend den Ansatz eines Datenschutzes durch Systemgestaltung verfolgen und als Konkretisierung von Art. 25 DSGVO angesehen werden können, könnten sein:[522]

- Riskante Datenverarbeitung darf nur zulässig sein, wenn geeignete Schutzvorkehrungen getroffen sind. Deren Eignung ist permanent nachzuweisen.
- Profile sind nur zulässig, wenn sie für den objektiven Zweck einer zulässigen datenvermeidenden Anwendung erforderlich sind.
- Vorsorgemaßnahmen müssen Risiken reduzieren und potenzielle Schäden begrenzen – auch bei anonymen Daten, die künftig noch einen Personenbezug erhalten können.

519 S. Kap. 3.13 und 3.14.
520 EU ABl. L 123 vom 19.5.2015, 77.
521 S. im Kommissionsentwurf die Art. 8, 10, 12 und 16; KOM(2017) 10 endg.
522 Beispiele überwiegend entnommen aus Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 361 (377 f.). Zu weiteren Beispielen für den Datenschutz in der öffentlichen Verwaltung und im Beschäftigtenkontext s. Roßnagel, DuD 2017, 290 (293 f.).

- Neben den Datenverarbeitern sind auch die Hersteller von Informationstechnik dafür in die Pflicht zu nehmen, dass sie diese datenschutzgerecht gestalten und voreinstellen.
- Anforderungen an die transparente, datenvermeidende und missbrauchsresistente Gestaltung des Systems (Vermeidung von Profilen) und deren datenärmste Konfigurierung werden bereichsspezifisch konkretisiert.
- Anforderungen an die Architektur der Datenverarbeitung müssen so gestaltet werden, dass die personenbezogenen Daten prinzipiell im Bereich der betroffenen Person selbst verbleiben und nur anonymisierte oder pseudonymisierte Daten in den zentralen Systemen verarbeitet werden.
- Die Datensicherheit ist an den Schutzzielen Datenvermeidung, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit auszurichten.[523]
- Um Maßnahmen, die technischen Selbstdatenschutz durch die betroffenen Personen ermöglichen, zur Durchsetzung zu verhelfen, sind Hersteller und Verantwortliche zu verpflichten, geeignete Schnittstellen zu Verfügung zu stellen.
- An Pseudonymisierung oder Anonymisierung sind konkrete Anforderungen an den Grad der Sicherheit gegen De-Anonymisierung zu stellen und die Wiederherstellung eines Personenbezugs ist ausdrücklich zu verbieten.[524]
- Für bestimmte riskante Datenverarbeitungsvorgänge sind Anforderungen an die Zweckbestimmung und die Absicherung von Zweckbindungen festzulegen und insbesondere Zweckänderungen für Daten zu verbieten, an deren Zweckbindung ein hohes Vertrauen besteht, wie z.B. Protokolldaten zu Sicherungszwecken.
- An die Zulässigkeit der Auftragsdatenverarbeitung und speziell des Cloud Computing sind risikospezifische Anforderungen festzulegen.
- Algorithmenbasierte Entscheidungsverfahren dürfen nur für ihren Einsatzbereich nachgewiesen relevante Merkmale verwenden und müssen für Aufsichtsbehörden in ihrer Entscheidungsfindung nachvollziehbar und für die betroffene Person erklärbar sein.

---

523 Konferenz der unabhängigen Datenschutzaufsichtsbehörden, Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ vom 6./7.4.2016.

524 S. zu dem Beispiel im japanischen Datenschutzrecht Geminn/Laubach/Fujiwara, ZD 2018, 413.

Die Regelungen zu den Voraussetzungen der Zulässigkeit der Datenverarbeitung, zur Zulässigkeit von Zweckänderungen, zu konkreten Rechten der betroffenen Personen und zu den Pflichten der Verantwortlichen müssen spezifisch für bestimmte Technikfunktionen oder bereichsspezifisch für bestimmte Anwendungsprobleme konkretisiert werden. Grundsätzlich sind zwei unterschiedliche Ansatzpunkte für im richtigen Sinn technikneutrale, aber risikospezifische Datenschutzregelungen möglich:

- Entweder regelt das Datenschutzrecht Funktionen von Techniken, die in vielen Wirtschafts-, Gesellschafts- und Verwaltungsbereichen zum Einsatz kommen – wie etwa Videoüberwachung, Cloud Computing oder algorithmenbasierte Entscheidungsverfahren – und fordert für diese bereichsübergreifend die Ausgestaltung einzelner wichtiger Funktionen – wie z.B. die Nachvollziehbarkeit und Begründbarkeit von algorithmenbasierten Entscheidungen.
- Oder es regelt Ausprägungen von Datenschutzvorgaben in spezifischen Anwendungsbereichen – wie z.B. für Smart Cars, Smart Buildings oder Social Networks. In diesen Regelungen fordert es bereichsspezifische Ausgestaltungen von Technikfunktionen – wie etwa im Smart Car bestimmte Anzeigen vor der Verarbeitung von bestimmten personenbezogenen Daten, Möglichkeiten der Intervention von Fahrern oder die Zulässigkeit von Speicherungen oder Weitergaben von Daten an Dritte – und berücksichtigt dabei die spezifischen Bedingungen und Ausprägungen ihrer Anwendung.

Notwendig ist immer, die geeigneten Anforderungen an die Verantwortlichen, aber auch an die Hersteller und Anbieter von Techniksystemen zu stellen, mit deren Hilfe die Verantwortlichen die Anforderungen erfüllen sollen. Darauf zu vertrauen, dass der Markt dafür sorgt, dass rechtzeitig genau die vom Datenschutzrecht geforderten Datenschutzfunktionen von den Herstellern und Anbietern angeboten werden, wäre naiv. In der Praxis der Aufsichtsbehörden ist festzustellen: „Diejenigen, die es richtig machen wollten, waren auch nicht glücklich, weil sie feststellten, dass Hersteller von Produkten und Anbieter von Dienstleistungen ihnen oft keine Hilfe waren und es damit schwierig war, die eigene Rechenschaftspflicht zu erfüllen.“[525] Die Hersteller nicht zu verpflichten, ihre Produkte und Dienstleistungen mit bestimmten Technikfunktionen auszustatten, stürzt Verantwortliche in ein Erfüllungsdilemma und begründet von Anfang an Vollzugsdefizite.

525 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2019, 10.

Auch hier wäre eine abstrakte Verpflichtung über alle Gesellschafts-, Wirtschafts- und Verwaltungsbereiche hinweg verfehlt, vielmehr sollte sie technik- und bereichsspezifisch die jeweils spezifischen Risiken der Produkte und Dienste sowie die Bedingungen ihrer Entwicklung und ihres Angebots berücksichtigen.

Dabei ist es nicht notwendig, die Datenschutz-Grundverordnung durch einen umfassenden Katalog risikospezifischer Regelungen zu überfrachten. Vielmehr könnte die Datenschutz-Grundverordnung als die Regelung gelten, die Datenschutz dem Grundsatz nach regelt und konkretisierende Regelungen anderen Vorschriftenwerken überlässt.[526]

Die Risikoneutralität der Datenschutz-Grundverordnung wird auch deutlich, wenn sie in Art. 2 Abs. 2 lit. c die Datenverarbeitung für persönliche oder familiäre Tätigkeiten unabhängig von ihrem Risiko für betroffene Personen vollständig aus dem Anwendungsbereich des Datenschutzrechts ausnimmt.[527] Da diese Ausnahme keinen Ausgleich zwischen den Grundrechten der Datenverarbeiter und der betroffenen Personen kennt, sondern ohne jede Rücksicht auf die Risiken oder Schäden bei den betroffenen Personen gilt, bedarf sie einer Korrektur. Diese könnte darin bestehen, dass die Datenschutz-Grundverordnung zwischen der Datenverarbeitung für persönliche oder familiäre Tätigkeiten, für die keine Vorschrift der Verordnung gilt und der Datenverarbeitung für nicht persönliche und familiäre Tätigkeiten, für die alle Vorschriften der Verordnung gelten, eine dritte Gruppe bildet. Diese könnte die Datenverarbeitungen für persönliche und familiäre Tätigkeiten umfassen, die nicht zu vernachlässigende Risiken für betroffene Personen begründen. Für diese Gruppe müssten nicht alle Vorschriften der Verordnung gelten. Für sie könnte es ausreichen, wenn für sie etwa die Vorschriften der Art. 5, 6 Abs. 4, 9, 15, 21, 25 und 32 DSGVO gelten.

Zu diskutieren wäre, wie man im Bereich der Datenverarbeitung für persönliche oder familiäre Tätigkeiten mit breiter sozialer Übung umgeht wie die Veröffentlichung von personenbezogenen Daten Dritter aus dem persönlichen und familiären Bereich in Social Media-Plattformen oder auf selbstbetriebenen Webseiten (Urlaubsfotos), die nur für einen sehr eingeschränkten Kreis freigegeben werden. Da diesen unvermeidlich eine Übermittlung personenbezogener Daten an den Betreiber der Plattform zugrunde liegt, ist damit der Ausnahmebereich der „ausschließlich persönlichen und familiären Tätigkeit“ verlassen. Sollte diese Datenverarbeitung

526 S. hierzu Kap. 7.
527 S. hierzu Kap. 3.1.

aber nicht auch in den neuen mittleren Regelungsbereich aufgenommen werden – schlicht um zu verhindern, dass es zu regelmäßigen Rechtsbrüchen bei der Verwendung von sozialen Medien kommt, für die kein Verständnis bei den Nutzern besteht?[528]

6.3.2 Stärkung der Stellung der Verbraucher

Aufgrund der Machtasymmetrie zwischen Anbieter und Verbraucher sind verschiedene Maßnahmen zur Stärkung der Stellung des Verbrauchers zu prüfen. Zum einen könnte die Nutzung der Einwilligung zur vollständigen Befreiung des Verantwortlichen von seinen datenschutzrechtlichen Verpflichtungen dadurch verhindert werden, dass bestimmte Verpflichtungen und Rechte für nicht abdingbar erklärt werden. Dies schränkt zwar die Selbstbestimmung der betroffenen Person ein, schützt sie aber davor, dass sie in sozialen oder psychischen Zwangssituationen verleitet wird, auf eigene zentrale Rechte zu verzichten. Hierfür könnte der bis zum 24. Mai 2018 geltende § 6 BDSG ein Vorbild sein.

Zum anderen könnte der Schutz des Verbrauchers nicht seiner individuellen Entscheidung überantwortet werden, sondern vor allem in „Take it or Leave it"-Situationen objektiviert werden, indem z.B. die Einwilligungserklärungen oder Allgemeinen Geschäftsbedingungen von einer dafür zuständigen kompetenten Stelle objektiv und vor Inkrafttreten geprüft und zugelassen werden müssen.[529] Das Vorhandensein geforderter Datenschutzfunktionen könnte auch in Zulassungen überprüft werden, die in bestimmten Bereichen die Qualität des Systems – auch bezogen auf die Risiken seiner Nutzung – überprüfen. Beispiele hierfür sind die Zulassungen von Kraftfahrzeugen und von Medizinprodukten. Auch wird vorgeschlagen, vor dem Einsatz bestimmter risikoreicher algorithmenbasierter Entscheidungssysteme die Qualität der Daten, die Qualität der statistischen Modelle sowie die Diskriminierungsfreiheit und Nachvollziehbarkeit der Ergebnisse durch eine hierfür vorgesehene Stelle überprüfen zu lassen.[530]

Ein dritter Ansatz ist mit Art. 80 DSGVO angedeutet, nämlich die Kollektivierung der Rechtewahrnehmung: Die Feststellung und Verfolgung eines Rechts wird nicht mehr allein der Privatinitiative einer betroffenen

528 S. Kap. 3.1.2.
529 Roßnagel u.a., 2016, 130.
530 S. z.B. Verbraucherzentrale Bundesverband, 2017, 3; Krafft/Zweig, 2019, 42; Martini, 2019, 73 f.

Person überlassen, sondern professionell von einem Verband übernommen. Die Datenschutz-Grundverordnung hat den Rechtsschutz im Datenschutz deutlich gestärkt. Beschwerde- und Klagerecht[531] sind dabei grundsätzlich bei der betroffenen Person verortet. Art. 80 Abs. 1 DSGVO ermöglicht jedoch, bestimmte Einrichtungen, Organisationen oder Vereinigungen mit ihrer Wahrnehmung zu beauftragen.[532] Vertretungsberechtigt sind unter anderem die Verbraucherzentralen in Deutschland.[533] Ob diese jedoch auch unabhängig von einer Beauftragung durch die betroffene Person tätig werden können, obliegt nach Art. 80 Abs. 2 DSGVO den Mitgliedstaaten.[534] Hier hält das deutsche Recht mit § 2 UKlaG eine entsprechende Regelung bereit, die jedoch kein eigenständiges Beschwerderecht qualifizierter Einrichtungen etabliert. Zudem soll § 2 Abs. 2 Satz 1 Nr. 11 UklaG nach Maßgabe von § 2 Abs. 2 Satz 2 UKlaG nicht greifen, „wenn personenbezogene Daten eines Verbrauchers von einem Unternehmer ausschließlich für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Verbraucher erhoben, verarbeitet oder genutzt werden". Hier sollte eine Ausweitung erfolgen. Die nationale Umsetzung von Art. 80 Abs. 2 DSGVO bleibt hinten den Möglichkeiten zurück, die die Öffnungsklausel bietet. Auch der Kreis der Vertretungsberechtigten könnte mit Blick auf Art. 80 Abs. 1 DSGVO weiter gefasst werden – jenseits von Verbraucherschutzverbänden im Sinne von § 3 und 4 UKlaG. Der nationale Gesetzgeber sollte ein echtes Verbandsklagerecht zulassen, das es ermöglicht, auch unabhängig von Einzelfällen offene Fragen des Datenschutzrechts grundsätzlich zu klären.

Zu beachten ist auch die Problematik hinter Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Auch wenn kein Erlaubnistatbestand nach lit. a bis e greift, so kann dennoch eine Verarbeitung personenbezogener Daten stattfinden, wenn der Verantwortliche eigene Interessen oder Interessen Dritter gel-

531 Art. 77 ff. DSGVO.

532 Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet sind, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind. S. umfassend zur Vertretung betroffener Personen, Verbandsbeschwerde und Verbandsklage Geminn, in: Jandt/Steidle, 2019, B. VI. Rn. 103 ff.

533 S. § 3 und 4 UKlaG.

534 S. hierzu auch Europäische Kommission, Commission Staff Working Document, 20; Weichert, 2017, 13.

tend machen kann. Dazu müssen diese Interessen im Vergleich mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person überwiegen.[535] Zusätzlich ist die Erforderlichkeit der Verarbeitung festzustellen. Die Abwägung und die Feststellung nimmt jedoch der Verantwortliche vor.[536] Daher besteht die Gefahr, dass dieser in der Praxis zu einer Überschätzung der Erforderlichkeit der Verarbeitung und der Bedeutung der eigenen Interessen sowie zu einer Unterschätzung der Interessen der betroffenen Person tendiert. Eine Korrektur dieser Fehleinschätzung findet aber allenfalls erst im Nachgang statt, wenn sich Risiken der fraglichen Verarbeitung für die betroffenen Personen bereits realisiert haben. Der zeitliche Abstand von der Verarbeitung bis zur Korrektur kann im Falle eines Rechtsstreits um die getroffene Abwägung stark anwachsen. Die betroffene Person muss hierzu aber zunächst feststellen können, dass eine rechtswidrige Verarbeitung stattfindet, und sie muss im zweiten Schritt Willens und fähig sein, gegen die Verarbeitung vorzugehen. Zur Stärkung der betroffenen Person sollte der Unionsgesetzgeber die Abwägung nicht den Verantwortlichen überlassen, sondern selbst Regelungen treffen, die in typischen Verarbeitungssituationen (z.B. Werbung oder Profiling) oder bei typischen Geschäftsmodellen (z.B. Suchmaschinen, Social Media) greifen.[537] Klare Regelungen würden auch hier dazu beitragen, die Stellung des Verbrauchers zu stärken und Machtasymmetrien abzubauen.

6.3.3 Verhinderung einer Überforderung der Verbraucher

Den Verbraucher können vor allem ungeeignete (zu viel oder zu wenig) Informationen und Entscheidungszwänge mit unzureichender Übersicht über die Folgen überfordern. Genau dies aber ist die Folge der gegenwärtigen Praxis, über alle vagen, langfristig möglichen Datenverarbeitungen bereits beim ersten Kontakt mit dem Verbraucher durch Verweis auf eine umfassende Datenschutzerklärung zu informieren. Auf Grundlage dieser viel zu umfassenden Informationen zu einem Zeitpunkt, zu dem sich der Verbraucher nicht für alle Details interessieren kann, von ihm eine Einwil-

535 S. zur Berücksichtigung der Interessen Dritter Kap. 6.3.4.

536 Hierauf besteht die Europäische Kommission, Commission Staff Working Document, 15 f.

537 S. hierzu auch Bundesregierung, in: Rat, ST 12756/1/19, 14 f.; für den Fall der Direktwerbung fordert dies auch Datenschutzkonferenz, Erfahrungsbericht, 2019, 22.

ligung zu verlangen oder die Daten auch ohne seine Zustimmung zu verarbeiten, muss den Verbraucher überfordern. Notwendig ist daher über die Regelungen der Art. 12 bis 14 DSGVO und die vorgeschlagenen Detailverbesserungen[538] hinaus ein neues, auch an den Interessen der betroffenen Person und nicht nur an der Aufwandsreduktion für den Verantwortlichen orientiertes Informationskonzept zu etablieren. Dieses muss folgende Eigenschaften der notwendigen Datenschutzinformationen sicherstellen: Die Informationen müssen

- entscheidungsrelevant (die Informationen, die für ein unmittelbar folgendes Handeln der betroffenen Person entscheidend sein können, so dass sie auf ihrer Grundlage entscheiden kann, einen Dienst zu nutzen, eine Funktion einzuschalten oder eine Einwilligung zu erteilen),
- interessenabhängig (die Information, die dem Interesse und der Aufmerksamkeit der betroffenen Person in der jeweiligen Situation entspricht. Sie muss z.B. zwischen mehreren Sichten wählen können: Symbol – Kurzinformation – ausführlichere Information – gesamte Datenschutzerklärung) und
- rechtzeitig (die Information erfolgt immer unmittelbar vor der Handlung der betroffenen Person, die die Datenverarbeitung verursacht, in einer Weise, dass sie diese Handlung auch noch unterlassen kann)

angeboten werden.

Beispielsweise wäre im Smart Car eine situationsangepasste Information notwendig, die mindestens drei Ebenen umfasst:[539] Allgemeine Strukturinformationen sollten ständig – auf einer Website – bereitgehalten werden, auf die mit dem Kaufvertrag und in Allgemeinen Geschäftsbedingungen aufmerksam gemacht wird. Mit der Inbetriebnahme der jeweiligen Funktion muss im Auto eine technische Anzeige erfolgen, dass diese Funktion eingeschaltet ist, und schließlich muss bei der aktuellen Nutzung des Automobils z.B. auf dem Armaturenbrett auf die derzeit genutzten Dienste hingewiesen werden. Bei einer Aktivierung der Anzeige können weitere Informationen zum Datenschutz abgerufen werden. Untersuchungen zur Umsetzung von Transparenzanforderungen im vernetzten Auto zeigen, dass es hier prinzipiell umsetzbare Ansätze gibt;[540] diese bedürfen jedoch der Erprobung und Fortentwicklung mit Blick auf die immer weiter fortschreitende Vernetzung mit der Infrastruktur.[541]

538 S. Kap. 5.9 bis 5.13.
539 S. hierzu auch Husemann, in: Roßnagel/Hornung, 2019, 367 ff.
540 S. z.B. Bönninger/Eichelmann/Methner, in: Roßnagel/Hornung, 2019, 355 ff.
541 S. Roßnagel/Hornung, in: Roßnagel/Hornung, 2019, 475.

Hilfreich ist auch eine Prüfung durch Dritte, denen der Verbraucher vertraut. Hierfür sieht die Datenschutz-Grundverordnung in Art. 42 und 43 als Innovation des Datenschutzrechts eine freiwillige Zertifizierung der Datenschutzkonformität einer Anwendung vor.[542] Fraglich ist, welche rechtlichen und technischen Möglichkeiten der Unterstützung der Verbraucher gegeben sind. Die Zertifizierung sollte für bestimmte Bereiche verpflichtend sein. Orientierungskriterium könnte sein, dass dann, wenn Produkte oder Dienste, denen die Verarbeitung personenbezogener Daten dient, zulassungsbedürftig sind, auch die Feststellung der Datenschutzrechtskonformität der Datenverarbeitung in Form eines Zertifikats obligatorisch ist. Dies würde zum Beispiel für viele Dienste und Produkte, die Gesundheitsdaten verarbeiten, oder für vernetzte und automatisiert fahrende Kraftfahrzeuge zutreffen.[543]

Die Durchsetzung der Datenschutzprinzipien kann durch eine konsequent datenschutzfreundliche Technikgestaltung bewirkt werden. Die Gestaltung insbesondere von komplexen Informationssystemen muss dabei so erfolgen, dass Datenschutz nicht zur Belästigung des Verbrauchers wird, sondern situationsadäquat und wo möglich auch automatisiert erfolgt. Einwilligungen könnten etwa nach vordefinierten Kriterien automatisiert durch ein digitales „Alter Ego" des Verbrauchers in dessen Auftrag erteilt werden und Geräteeinstellungen ebenfalls automatisiert an dessen Vorstellungen zum Datenschutz angepasst werden.[544] Das „Alter Ego" kontrolliert die Einhaltung der gemachten Vorgaben durch den Datenverarbeiter. So könnte Kontrolle über Datenverarbeitungsvorgänge auch bei immer komplexerer Datenverarbeitung erreicht werden, ohne zu einer Überforderung der betroffenen Person zu führen. Erreicht werden kann dies nur, wenn die Technik entsprechende Schnittstellen bereitstellt, über die das „Alter Ego" mit ihr in Kontakt treten und die Vorgaben des Verbrauchers kommunizieren kann.

6.3.4 Verhinderung negativer Auswirkungen auf Dritte

Die Verarbeitung personenbezogener Daten, aber auch anonymer Daten kann Risiken für die Entscheidungs- und Entfaltungsfreiheit Dritter sowie für deren diskriminierende Behandlung in Form gruppenbezogener

542 S. z.B. Maier/Bile, DuD 2019, 478 ff.
543 S. auch Kap. 6.3.1.
544 Roßnagel u.a., 2016, 134 f.

Schlechterstellung bewirken. Werden diese Daten für die Erstellung von Statistiken im Rahmen von Big-Data-Analysen und von selbstlernenden algorithmenbasierten Entscheidungssystemen genutzt, entstehen Bewertungen von Eigenschaften sowie Verhaltensprognosen und -beeinflussungen auch dritter Personen, die gar keine Daten für diese Analysen geliefert haben. Durch die anonyme Vergemeinschaftung aller Merkmalsträger im Rahmen der Statistiken werden ihnen die gleichen Eigenschaften zugeordnet und durch die Normativität der durch die Statistiken beschriebenen Normalität haben diese Statistiken verhaltensbestimmende Wirkung. Viele Verbraucher werden Vorteile daraus ziehen wollen, sich „normal" zu verhalten, sofern diese Normalität als Entscheidungsgrundlage bei Anbietern dient. Hinzu kommt, dass aus diesem Wissen über statistisch wahrscheinliches Verhalten und über statistisch wahrscheinliche Wirkungen bestimmter Anreize gezielte Verhaltenssteuerungen erfolgen.[545]

Datenschutzrecht ist bezogen auf die beeinträchtigten Dritten nicht anwendbar. Soweit anonyme Daten verarbeitet werden, scheidet Datenschutzrecht mangels Personenbezugs der Daten aus. Soweit personenbezogene Daten verarbeitet werden, sind diese Daten anderen betroffenen Personen zuzuordnen und gerade nicht den Dritten. Diese können keine Betroffenenrechte geltend machen. Da der sachliche Anwendungsbereich des Datenschutzrechts mangels Verwendung personenbezogener Daten nicht eröffnet ist, fehlt ein effektiver rechtlicher Schutz des Verbrauchers vor den aufgezeigten Risiken durch statistische Verhaltensmuster.

Dennoch können sie die Grundrechtsausübung und das demokratische Engagement gefährden.[546] Durch das Einordnen des Verhaltens in statistische Handlungsmuster als konform oder nicht konform und durch das so indirekt erzwungene Anpassungsverhalten werden die Entscheidungs- und die Verhaltensfreiheit faktisch eingeschränkt, was das Recht auf informationelle Selbstbestimmung gerade vermeiden soll. Solche statistischen Muster verstärken die Normativität der Normalität und reduzieren „Soziodiversität". Diese ist aber Voraussetzungen für Innovationen und Demokratie.[547] Für die Verwirklichungsbedingungen von Grundrechten und Demokratie hat der Staat aber eine Schutzpflicht. Diese fordert ein angemessenes Handeln und rechtfertigt sogar verhältnismäßige Beschränkungen von Grundrechten, wenn dies zum Schutz von Selbstbestimmung, freier Entfaltung und Funktionsfähigkeit der Demokratie erforderlich ist.

---

545 S. hierzu näher Kap. 6.2.
546 S. z.B. Weichert, ZD 2013, 251 ff.; Roßnagel, ZD 2013, 562 ff.
547 S. Roßnagel/Nebel, DuD 2015, 455.

Rechtliche Schutzmaßnahmen könnten bei der Einwilligung ansetzen. Da der Einwilligende nur für sich, nicht aber zu Lasten Dritter Datenverarbeitung rechtfertigen kann, könnte die Möglichkeit der Einwilligung beschränkt werden, wenn sie nicht nur Folgen für den Einwilligenden, sondern auch für einen Dritten hat. Sie könnte etwa in bestimmten Verarbeitungskontexten als Rechtfertigungsgrundlage für eine Verarbeitung personenbezogener Daten ausgeschlossen oder zumindest befristet werden.[548] Auch könnten die Voraussetzungen für die Wirksamkeit einer Einwilligung je nach Risiko der Verarbeitung skalieren. Sie könnte etwa von der Erfüllung gesteigerter Transparenzpflichten des Verantwortlichen abhängig gemacht werden, der auch über die Folgen der Datenverarbeitung für Dritte informieren muss. Der Einwilligende müsste dann konsequenter Weise auch für die Folgen seiner Einwilligung verantwortlich sein.

Ein solcher Ansatz könnte vor allem dann gerechtfertigt sein, wenn betroffene Personen als Gegenleistung für Rabatte, Boni oder gar die kostenlose Nutzung eines Dienstes mit der Preisgabe ihrer Daten und der Einwilligung zu einer (fast) unbegrenzten Nutzung dieser Daten bezahlen und sich dabei nicht um die negativen Folgen für andere kümmern oder diese zu ihrem Vorteil bewusst in Kauf nehmen.

Gegen diesen Ansatz spricht jedoch, dass die Einwilligung meist nicht der einzige Weg ist, die Daten für statistische Muster oder Modelle zu erlangen. Die statistische Verarbeitung personenbezogener Daten kann auch aufgrund anderer gesetzlicher Erlaubnistatbestände erfolgen. Über eine Zweckänderung für eine statistische Verarbeitung der personenbezogenen Daten muss der Verantwortliche nach Art. 13 Abs. 3 und 14 Abs. 4 DSGVO die betroffene Person zwar informieren. Diese Information kommt aber für eine Verhinderung der statistischen Datenverarbeitung zu spät. Sind die Daten inzwischen anonymisiert, fällt die Verarbeitung ohnehin aus dem Anwendungsbereich des Datenschutzrechts heraus. Von den betroffenen Personen den Verzicht auf (vermeintlich) kostenlose Dienste zu verlangen, auf die sie dringend angewiesen sind, weil die mit ihren Daten erzeugten statistischen Muster oder Modelle zum Nachteil von Dritten genutzt werden können, dürfte meist unverhältnismäßig sein. Auch dürfte es schwer sein, vor der Einwilligung oder vor der Nutzung eines Dienstes zu prognostizieren, was mit den Daten geschieht und für wen die nachfolgende Datenverarbeitung welche Nachteile oder Vorteile verursacht. Außerdem liegt der Schwerpunkt der nachträglichen benachteiligenden Nut-

548 S. Roßnagel u.a., 2016, 130 f.

zung der Daten nicht bei der betroffenen Person, sondern beim Verantwortlichen.

Der Schutz Dritter muss daher beim Verantwortlichen ansetzen. Dieser erhebt die Daten bei der betroffenen Person und verantwortet die statistische Muster- oder Modellerstellung aus diesen Daten als Grundlage für die Anwendung bei anderen Nutzern. Auch wenn der Verantwortliche, der die Daten erhebt, sich von demjenigen unterscheidet, der die statistischen Muster oder Modelle erstellt, und von demjenigen, der die Muster oder Modelle auf Dritte anwendet, so sind sie doch alle Verantwortliche, solange die Daten noch personenbezogen sind. Für den ersten, der die Daten erhebt, und für den zweiten, der personenbezogene Daten in statistischen Mustern oder für solche anonymisiert, handelt es sich um Zweckänderungen, die dem Datenschutzrecht unterfallen. Soweit der Anwender die aus der Statistik gewonnenen Entscheidungsmodelle – im Rahmen algorithmenbasierter Datenverarbeitungen – auf individualisierbare Dritte anwendet, ist er für diese Datenverarbeitung datenschutzrechtlich verantwortlich. Datenschutzrechtlich führt diese Form der Datenverarbeitung zumindest zu drei Fragen:

Auf welcher Rechtsgrundlage dürfen personenbezogene Daten erhoben und für solche statistischen Zwecke verarbeitet werden? Ist die Erhebung nicht durch Einwilligungen gerechtfertigt, kommt eine Rechtfertigung durch überwiegende berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Betracht.[549] Diese Vorschrift erlaubt, auch berechtigte Interessen Dritter zu berücksichtigen. Warum aber ist sie nur mit den „Interessen oder Grundrechte(n) und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern," abzuwägen und nicht auch mit denen aller anderen betroffenen Dritten? Eine Schutzmöglichkeit könnte sein, in den Gesetzestext auch die Interessen oder Grundrechte und Grundfreiheiten Dritter aufzunehmen. Der statistischen Verarbeitung geht im Regelfall eine Zweckänderung voraus. Da diese statistische Verarbeitung nicht unter die Ausnahme für die öffentliche Statistik des Art. 5 Abs. 1 lit. b DSGVO fällt,[550] ist sie als Zweckänderung nach Art. 6 Abs. 4 DSGVO nur zulässig, wenn sie mit dem bisherigen Zweck vereinbar ist. Hier könnte eine Klarstellung in Art. 6 Abs. 4 DSGVO erfolgen, dass dies nicht der Fall ist, wenn die Daten als Material für selbstlernende algorith-

549 S. hierzu auch Kap. 6.3.2.
550 S. Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 Rn. 107.

menbasierte Systeme oder für Big Data-Muster einer bestimmten Risikoklasse[551] verwendet werden sollen.

Soweit statistische Muster erstellt und selbstlernende algorithmenbasierte Systeme trainiert werden sollen, sind qualitative Anforderungen an die Daten und ihre Verarbeitung aufzustellen, die je nach Risikoklasse unterschiedlich stark kontrolliert werden sollten. Ein Vorschlag für solche qualitativen Anforderungen finden sich in dem vorgeschlagenen neuen Abs. 4 von Art. 22 DSGVO.[552]

Die Anwendung der statistischen Muster im Einzelfall, ist vom Datenschutzrecht nur dann erfasst, wenn es dabei wiederum zur Verarbeitung personenbezogener Daten kommt. Werden die personenbezogenen Daten von algorithmenbasierten Entscheidungssystemen verarbeitet, fällt dies in den Anwendungsbereich des bestehenden oder – wie hier vorgeschlagen[553] – modifizierten Art. 22 DSGVO. Die Kontrolle der Wirkungen kann jedoch – insbesondere für Diskriminierungen – aus dem Anwendungsbereich dieser Vorschrift herausfallen.

Letztlich weist das Thema der negativen Auswirkungen der Datenverarbeitung auf Dritte über das Datenschutzrecht hinaus, das dem Schutz der informationellen Selbstbestimmung dient.[554] Es betrifft neben der Selbstbestimmung und Selbstentfaltung auch Fragen der Gleichbehandlung, der Gerechtigkeit und der Rechtsstaatlichkeit. Für dieses Thema sollte daher ein den Datenschutz einbeziehendes, aber über diesen hinausgehendes Schutzkonzept gesucht werden.

Dies gilt vor allem für die Verwendung von anonymen Daten. Diese wirft zum einen Fragen auf nach der Zulässigkeit der Anwendung von Ergebnissen aus Big-Data-Analysen, zum anderen Fragen nach der Notwendigkeit eines Schutzkonzeptes auch für anonymisierte Daten.

Beispiele für solche Schutzkonzepte lassen sich im außereuropäischen Ausland bereits finden. Japan hat etwa im Zuge einer umfassenden Reform seines Datenschutzrechts auch Regelungen für sogenannte „anonymously processed information“ eingeführt.[555] Dabei handelt es sich um

551 S. zur Einteilung in Risikoklassen Krafft/Zweig, 2019, 31 ff.
552 S. Kap. 5.21.
553 S. Kap. 5.21.
554 S. auch Verbraucherzentrale Bundesverband, 2017, 3; Schulz/Dreyer, 2018, 9; Krafft/Zweig, 2019, 16.
555 S. hierzu umfassend Geminn/Laubach/Fujiwara, ZD 2018, 413. Man beachte auch den gescheiterten Versuch der Kriminalisierung einer Re-Identifizierung durch die australische Privacy Amendment (Re-identification Offence) Bill 2016.

personenbezogene Daten, die einer Anonymisierung unterzogen wurden und nun ohne Personenbezug sind. Das japanische Datenschutzrecht sieht für solche Daten Maßnahmen zur Datensicherheit vor, die der Datenverarbeiter ergreifen muss. Diese Maßnahmen betreffen sowohl das Verfahren zur Entfernung des Personenbezuges als auch den Umgang mit den anonymisierten Daten. Darüber hinaus treffen den Datenverarbeiter Informationspflichten bezogen auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind. Ergänzt wird dies durch ein Verbot, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen. Ein Verantwortlicher darf auch im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale nicht erwerben. Werden diese Vorgaben nicht beachtet, sieht das japanische Datenschutzrecht allerdings keine Sanktionen vor. Bezogen auf Datenübermittlungen aus der Europäischen Union gelten Daten nur dann als anonymisiert, wenn Informationen zur Anonymisierungsmethode unwiderruflich gelöscht werden und eine Re-Identifizierung der betroffenen Person unmöglich gemacht wird. Letztere, im Zuge des Angemessenheitsbeschlusses für Japan[556] eingeführte Ergänzung zeigt, dass konzeptionelle Unterschiede bestehen, die eine direkte Übernahme drittstaatlicher Instrumente in der Europäischen Union verhindern. Dennoch können diese Vorbilder dazu anregen, konzeptionell weiter zu denken als die Datenschutz-Grundverordnung.

6.3.5 Stärkung der Datenschutzprinzipien

Die Datenschutzprinzipien stammen weitgehend aus einer Zeit, in der weder PCs noch das Internet bekannt waren. Allgegenwärtige Datenverarbeitung, die Auswertung unendlich vieler personenbezogener Daten aus verschiedensten Quellen, die Datenverarbeitung durch lernfähige Algorithmen und die Erfassung der Welt durch Systeme der Künstlichen Intelligenz machen neue, ergänzende oder präzisierende Grundsätze erforderlich, um die Grundrechte der betroffenen Personen auf Persönlichkeitsschutz und Selbstbestimmung auch in der künftigen Welt zu schützen.

Auch wenn die Datenschutz-Grundverordnung keine spezifischen Antworten auf diese gravierenden Herausforderungen bietet,[557] könnte erwar-

556 S. hierzu Fujiwara/Geminn/Roßnagel, ZD 2019, 204 ff.; Tatsumi, CR 2019, 424 ff.; Geminn/Laubach, ZD 2019, 403 ff.

557 S. Kap. 6.3.1.

tet werden, dass zumindest die allgemeinen Regelungen der Verordnung – vor allem die Grundsätze der Datenverarbeitung in Art. 5 DSGVO – ausreichend Schutz gewähren.[558] Doch diese Grundsätze geraten durch die neuen technischen Herausforderungen unter einen massiven Druck, der ihre künftige Anwendbarkeit in Frage stellt.[559]

So verliert etwa die Zweckbindung bei allen Systemen ihren schützenden und steuernden Charakter, deren Verarbeitungszweck – wie etwa bei Assistenzsystemen im Auto, in der Wohnung, bei der Arbeit oder beim Hobby – in der umfassenden Unterstützung des Verbrauchers liegen. Dafür ist eine möglichst breite Datenbasis über Verhalten, Interessen und Vorlieben unerlässlich. Das eigentliche Ziel der Zweckbindung, Datenverarbeitung auf das erforderliche Maß zu begrenzen, wird dabei konterkariert, denn jede Information kann potenziell der Zweckerfüllung des Assistenten dienen. Der Grundsatz der Transparenz stößt an subjektive und objektive Grenzen. Subjektiv übersteigt die zu erwartende Vervielfachung der Datenverarbeitungsvorgänge in allen Lebensbereichen die mögliche Aufmerksamkeit, die zur Effektivität der Transparenz erforderlich ist, um ein Vielfaches. Objektiv setzen hohe Komplexität, vielfältige Zwecke und lernfähige Systeme der möglichen Transparenz hohe Grenzen. Um ein letztes Beispiel zu geben: Die Grundsätze der Datenminimierung und der Speicherbegrenzung sind an den jeweils begrenzten Zweck gebunden. Ebenso wie dieser werden auch diese Grundsätze ihre Steuerungskraft verlieren. Wenn der Zweck der Datenverarbeitung ohne wirkliche Grenzen ist, führt auch die Frage, welche Datenverarbeitung für diesen Zweck erforderlich ist, nicht mehr zu einer überschaubaren Eingrenzung erlaubter Datenverarbeitung. Wenn etwa das Gedächtnis der Dinge der betroffenen Person helfen soll, sich an vergessene Ereignisse zu erinnern, ist eine nach Umfang und Zeitraum grenzenlose Datenspeicherung erforderlich. Sensorbestückte Gegenstände und Umgebungen sind fast immer aktiv und erheben eine enorme Menge Daten, um den Verbrauchern nach ihrem – sich ständig ändernden – Bedarf jederzeit ihre Dienste anbieten zu können. Alle Systeme, die kontextsensitiv die betroffene Person entlasten oder unterstützen sollen, die Präferenzen des Nutzenden erkennen und ihnen gerecht werden sollen, können ihre Funktionen nur richtig erfüllen, wenn sie den Grundsatz der Datenminimierung und der Speicherbegrenzung ignorieren. In dem Konflikt zwischen modernen Technikanwendungen

558 Dies behautet die Europäische Kommission in ihrem Evaluationsbericht, Commission Staff Working Document, 28.

559 S. z.B. Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 367 ff.

und Datenschutzgrundsätzen dürfte entscheidend sein, dass die neuen Technikanwendungen den betroffenen Personen in den meisten Fällen nicht aufgedrängt werden – in diesem Fall dürften die Grundsätze greifen –, sondern von diesen gewollt werden. Sie wollen sich mit ihrer Hilfe die Träume erfüllen, die sie sich von diesen Technikanwendungen erhoffen.[560] Die Grundsätze zum Schutz der Verbraucher gegen den aktuellen Willen der Verbraucher zur Geltung zu bringen, dürfte nahezu aussichtslos sein.

Obwohl diese Grundsätze durch moderne Datenverarbeitung in Frage gestellt werden, darf dies kein Grund sein, sie als rechtliche Gebote aufzuweichen. Vielmehr sollte durch gesteigerte Anforderungen an technisch-organisatorische Maßnahmen versucht werden, das Regelungsziel der Grundsätze zu erreichen. Viele Vorschläge zur Überarbeitung der Datenschutz-Grundverordnung dienen diesem Ziel.[561]

Neben diesen von der Datenschutz-Grundverordnung in Art. 5 anerkannten Grundsätzen der Datenverarbeitung und den vorgeschlagenen Verbesserungen und Ergänzungen, fordert die technische Entwicklung, neue zusätzliche Grundsätze zu diskutieren, anzuerkennen und umzusetzen. Insbesondere die Anwendungen Künstlicher Intelligenz erfordern neue Grundsätze.[562] Als solche sind etwa zu diskutieren die nachgewiesene Relevanz (Aussagekraft) der Kriterien von Expertensystemen oder der Daten und der Algorithmen für lernende Systeme, die Nachvollziehbarkeit algorithmenbasierter Entscheidungen[563] und die Erklärbarkeit der Ergebnisse gegenüber der betroffenen Person[564] sowie die dauerhafte Überwachung besonders riskanter algorithmenbasierter Entscheidungssysteme.[565]

Um eine Stärkung der Datenschutzprinzipien in der Praxis zu erreichen, sollten greifbare Anreize für Datenverarbeiter zur Gewährleistung eines möglichst hohen Datenschutzniveaus gesetzt werden, um Eigennutz und Gemeinwohl in Einklang zu bringen.[566] Solche Anreize könnten beispiels-

560 S. hierzu Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 DSGVO, Rn. 193.
561 S. zu diesen Kap. 5.
562 Dies bestreitet die Europäische Kommission in ihrem Evaluationsbericht, Commission Staff Working Document, 28.
563 S. hierzu auch Verbraucherzentrale Bundesverband, 2017, 3 ff., 12; Schulz/Dreyer, 2018, 45 ff.
564 S. hierzu auch die Qualitätskriterien, die in Kap. 2.3.20 für automatisierte Entscheidungen im Einzelfall gefordert werden.
565 S. z.B. Krafft/Zweig, 2019, 5; Martini, 2019, 22.
566 Roßnagel u.a., 2016, 138.

weise durch die Einbeziehung von Datenschutzfragen als Vergabekriterien in öffentliche Ausschreibungen gesetzt werden.[567]

Zudem sollte ein umfassendes, institutionalisiertes Kontrollsystem zur Einhaltung von datenschutzrechtlichen Vorgaben eingerichtet werden, das neben Behörden auch Verbände und sonstige Einrichtungen einbezieht. Die Datenschutz-Grundverordnung hat hier bereits eine wesentliche Verbesserung des Status Quo bewirkt. Jedoch sollten die Funktionen und Strukturen von Systemen hier stärker in den Vordergrund gerückt werden, anstelle den Fokus auf das einzelne personenbezogene Datum zu richten.[568]

567 S. hierzu umfassend Bile u.a., in: Friedewald, 2018, 83 ff.
568 S. hierzu auch Roßnagel u.a., 2016, 138 f.