Alexander Roßnagel

Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?

Die Datenschutz-Grundverordnung der Europäischen Union hat hohe Erwartungen geweckt und wird mit großen Hoffnungen erwartet. Der Beitrag untersucht, ob diese berechtigt sind und ob die Verordnung dazu beitragen kann, den Datenschutz tatsächlich zu verbessern. Das Ergebnis ist gemischt: Nüchtern betrachtet führt sie weder zu einem einheitlichen Datenschutzrecht in Europa noch zu Datenschutzregelungen, die den modernen Herausforderungen gerecht werden. Gewisse Hoffnungen sind jedoch berechtigt, dass sie den Vollzug des Datenschutzrechts verbessert.

1. Datenschutz-Grundverordnung – Hoffnungen und Erwartungen

Nach mehreren Jahren vorbereitender Diskussion und einem anschließenden Gesetzgebungsprozess von über vier Jahren ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)[1] am 25. Mai 2016 in Kraft getreten. Sie gilt vom 25. Mai 2018 an mit all ihren Regelungen[2] in allen Mitgliedstaaten unmittelbar und wird Teil ihrer Rechtsordnung.

Die DSGVO sollte durch eine Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation, abkürzend E-Privacy-VO genannt, bereichsspezifisch ergänzt werden. Diese Verordnung soll die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) von 2002 ablösen. Sie sollte ebenfalls am 25. Mai 2018 Geltung erlangen. Da sie aber bisher nur in Form eines Vorschlags der Kommission vom 10. Januar 2017[3] und einer Stellungnahme des Parlaments vom 24. Oktober 2017[4] vorliegt, ist mit ihrer Verabschiedung vor Ende 2018 nicht zu rechnen.[5]

Die DSGVO wurde mit großen Versprechen angekündigt,[6] mit hohen Erwartungen versehen,[7] mit tiefen Enttäuschungen aufgenommen[8] und durch viel Lobby-Arbeit beeinflusst.[9] Sie wird im Ergebnis sehr unterschiedlich bewertet. Sie wird – vor allem von den an ihrem Entstehen Beteiligten – als „Meilenstein" bezeichnet,[10] als „Goldstandard" gepriesen[11] sowie als „*Beginn einer neuen Zeitrechnung im Datenschutzrecht*"[12]

und als „*festes Fundament für die anstehenden Herausforderungen der Digitalisierung*“ gefeiert.[13] Umgekehrt wird sie von anderen zu „*einem der schlechtesten Gesetze des 21. Jahrhunderts*“ gekürt und für das Datenschutzrecht als „*größte Katastrophe des 21. Jahrhunderts*“ bezeichnet.[14]

2. Datenschutz-Grundverordnung – ein weiterer Schritt in der Entwicklung des Datenschutzrechts

Das geltende Datenschutzrecht – auch die DSGVO – stammt konzeptionell aus den 1960er und 1970er Jahren. In dieser Zeit fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten bei der betroffenen Person erhoben worden waren – für diese weitgehend kontrollierbar. Wurde die Zweckbindung beachtet, wusste der Betroffene in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese erste Stufe der Datenverarbeitung sind die grundlegenden Schutzkonzepte des Datenschutzrechts entwickelt worden. Aus dieser Zeit stammen die Regelungen zur Zulässigkeit der Datenverwendung, die Individualisierung der Rechtsdurchsetzung durch Unterrichtung und Benachrichtigung der betroffenen Person, durch ihre Einwilligung und durch ihre Kontrolle in Form von Rechten auf Berichtigung und Löschung, die Anforderungen an Zweckbestimmung, Zweckbindung und Erforderlichkeit der Datenverarbeitung sowie die ergänzende Kontrolle durch Aufsichtsbehörden. Die Nutzung von PCs ab den 1980er Jahren hat die Datenschutzrisiken zwar deutlich erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite, qualitativ neue Entwicklungsstufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. Jede Handlung in diesem Cyberspace hinterlässt Datenspuren, die ausgewertet werden können und auch werden. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können von der betroffenen Person noch kontrolliert werden. Web 2.0 oder Cloud-Computing sind weitere Ausprägungen dieser Entwicklungsstufe. Für sie versuchten die in den 1990er Jahren erlassenen Multimedia-Datenschutzgesetze die Risiken in den Griff zu bekommen. Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem die neuen Prinzipien der Datensparsamkeit und des Datenschutzes durch Technik eingeführt. Diese normativen Vorgaben konnten allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft das komplette Leben im virtuellen Sozialraum, je nach Nutzung des Internet einen großen oder kleinen Ausschnitt des täglichen Lebens. Diesen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative. Jedoch besteht zumindest grundsätzlich die Möglichkeit, bildlich gesprochen, den Stecker zu ziehen.

In einer weiteren, dritten Entwicklungsstufe gelangt die Datenverarbeitung in die körperliche Welt. *Ubiquitous Computing* mit seinen Ausprägungen wie z.B. Smart Cars, Smart Health, Smart Home, Smarten Assistenten, Robotern und sonstige Techniken des Internet der Dinge, die auf der Erfassung der Umgebung durch vielfältige Sensoren und auf der Lernfähigkeit der Systeme durch Künstliche Intelligenz aufbauen, führen zu einer allgegenwärtigen Verarbeitung personenbezogener Daten, die potenziell alle Lebensbereiche und diese potenziell vollständig erfasst. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr. Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es noch keine datenschutzrechtlichen Regelungen.

Und auch die alten Regelungen greifen nicht mehr. In einer Welt allgegenwärtiger Datenverarbeitung laufen die bekannten Anforderungen der Zweckbindung, der Erforderlichkeit, der Transparenz, der Einwilligung und der Betroffenenrechte ins Leere. Wenn die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen soll, wird es niemand akzeptieren, wenn er täglich zur Durchsetzung des Transparenzprinzips tausendfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Wenn die Techniksysteme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, entgegen jeder Zweckbindung im Interesse des Nutzers vielfältige und umfassende Profile erzeugen. Wenn die Nutzer auf die Datenspeicher der sie umgebenden Gegenstände zurückgreifen, um ihr eigenes löchriges Gedächtnis zu erweitern, läuft das Erforderlichkeitsprinzip in Leere. Für die Gedächtnisfunktion ist für sehr lange Zeit eine Datenspeicherung auf Vorrat erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte. Diese Beispiele zeigen: Die allgegenwärtige Datenverarbeitung verursacht nicht nur ein weiteres Vollzugs-, sondern ein grundlegendes Konzeptproblem. Sie stellt die zentralen Schutzkonzepte des Datenschutzrechts in Frage.[15]

Alle drei Entwicklungsstufen bestehen heute parallel und beeinflussen sich gegenseitig. Für jede besteht ein spezifischer Modernisierungsbedarf – für die erste Stufe etwa in der Umsetzung der Datenschutzprinzipien beim Aufbau großer Datenverarbeitungssysteme für staatliche oder private Zwecke. Die unterschiedliche Umsetzung der Datenschutzrichtlinie (DSRL) von 1995 hat zu verschiedenen Datenschutzniveaus geführt, die auch als Standortvorteil genutzt wurden (Stichwort: Irland). Noch immer hat das Datenschutzrecht mit einem großen Vollzugsdefizit zu kämpfen. Für die zweite Stufe besteht der Modernisierungsbedarf vor allem darin, dass global agierende Konzerne mit Suchalgorithmen, sozialen Netzwerken, Plattformen und modernen Kommunikationsmöglichkeiten unverzichtbare Internet-Infrastrukturen ausgebildet haben, die Monopolcharakter haben und deren Geschäftsmodell die massenhafte Verarbeitung personenbezogene Daten voraussetzt. Moderne Datenschutzregelungen müssen den Gefährdungen der informationellen Selbstbestimmung durch diese neuen

Infrastrukturen in einer Weise entgegentreten, die der Abhängigkeit von ihnen gerecht wird. Für die dritte Stufe besteht der Modernisierungsbedarf vor allem darin, neue Schutzkonzepte für die informationelle Selbstbestimmung zu entwickeln, weil die bisherigen gegenüber den neuen Technikanwendungen leerlaufen. Die Zukunftsfähigkeit neuer Datenschutzregelungen muss daran gemessen werden, ob sie den Herausforderungen auf allen drei Entwicklungsstufen gerecht werden und neue Lösungen für die Gefährdungen der Grundrechtsverwirklichung bieten.

3. Zielsetzungen der Datenschutz-Grundverordnung

Die DSGVO erhebt den Anspruch, den genannten Anforderungen an den Datenschutz gerecht zu werden und die festgestellten Defizite zu beseitigen. Ausweislich ihrer Erwägungsgründe (EG) verfolgt sie drei große Zielsetzungen:

- Zum einen will sie das Datenschutzrecht unionsweit vereinheitlichen und einen soliden, „*kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union*“ schaffen (EG 3, 9 und 13).
- Zum anderen will sie einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen in der Union bieten und damit den Binnenmarkt stärken (EG 5, 10, 13). „*Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden*“ (EG 10).
- Schließlich stellt sie fest, dass „*rasche technologische Entwicklungen und die Globalisierung ... den Datenschutz vor neue Herausforderungen gestellt*“ haben (EG 6). Die Verordnung will den Datenschutz angesichts dieser Herausforderungen modernisieren und den Schutz der Grundrechte verbessern (EG 1, 2 und 4).

4. Wirkungen der Datenschutz-Grundverordnung

Um zu verstehen, warum die DSGVO diese Ziele weitgehend verfehlt, ist der Machtkampf um die Zukunft des europäischen Datenschutzrechts während der Entstehung der Verordnung zu berücksichtigen. Da nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche davon abhängig sind, personenbezogene Daten zu verarbeiten, hat derjenige, der über die Fortentwicklung des Datenschutzes bestimmt, ein zentrales Instrument zur Gestaltung der digitalen Gesellschaft in Europa in der Hand. Daher entspann sich ein heftiger Kampf, wer mit welchen Kompetenzen künftig die Datenverarbeitung reguliert (4.1). Er wirkte sich auf die Kontroversen über die Inhalte der Verordnung aus (4.2 – 4.4), mit denen diese Entwicklung begonnen werden sollte.

4.1 Kompetenzen zur Steuerung der Zukunft

Seit einigen Jahren hat die Kommission ihre Strategie zur europäischen Integration verschärft. Sie wechselte von einer „Angleichung der Rechtsvorschriften" (Art. 114 Abs. 1 AEUV) durch die Mitgliedstaaten zur einer „Vereinheitlichung der Rechtsordnungen" durch den Unionsgesetzgeber. Als Instrument nutzt sie nicht mehr vorrangig die Richtlinie, sondern die Verordnung.[16] Während eine Richtlinie durch die Mitgliedstaaten umgesetzt werden muss und diese nur hinsichtlich ihrer Zielsetzungen bindet, gilt eine Verordnung in den Mitgliedstaaten unmittelbar. Verordnungen entziehen daher ganze Politikbereiche der nationalen Demokratie.[17]

In ihrem Entwurf vom 25. Januar 2012[18] schlug die Kommission eine sehr radikale Lösung für die notwendige kontinuierliche Modernisierung des Datenschutzrechts vor: Durch die Wahl einer Verordnung wollte sie die Mitgliedstaaten von der weiteren Gesetzgebung im Bereich des Datenschutzes ausschließen, durch viele unbestimmte und ausfüllungsbedürftige Vorgaben sowie inhaltsleere Generalklauseln wichtige Datenschutzregelungen offen halten und innerhalb der Union sich selbst die Kompetenz vorbehalten, sie auszufüllen und fortzuentwickeln. Zu diesem Zweck sah der Entwurf 26 Ermächtigungen vor, die Verordnung durch delegierte Rechtsakte nachträglich zu konkretisieren, und 23 Ermächtigungen, sie durch Durchführungsrechtsakte auszugestalten. Außerdem behielt sie sich das Recht vor, bei einer Meinungsverschiedenheit zwischen verschiedenen Aufsichtsbehörden am Ende verbindlich zu entscheiden. Dadurch hätte die Kommission die künftige Rechtsetzung im Datenschutzrecht bei sich zentralisiert und monopolisiert.[19]

Dieser Entwurf hätte zur Folge gehabt, dass die Datenschutzregelungen der Mitgliedstaaten, die gerade für öffentliche Stellen stark ausdifferenzierte bereichsspezifische Regelungen enthalten, aufgrund des umfassenden Regelungsanspruchs der Verordnung hinfällig geworden wären. Doch nicht nur für das bestehende Datenschutzrecht hätte der Entwurf gravierende Auswirkungen gehabt. Seine tiefgreifendste Folge wäre die Entmachtung der Mitgliedstaaten und die Ermächtigung der Kommission zur Fortentwicklung des Datenschutzrechts gewesen.

Auf den Angriff der Kommission auf Gewaltenteilung und Demokratie in der Union hat das Parlament nur beschränkt reagiert.[20] Im Machtkampf zwischen Union und Mitgliedstaaten hielt das Parlament am Rechtsinstrument einer Verordnung fest. Insofern trug es die Entmachtung der Mitgliedstaaten mit. Es gab jedoch der Kritik insofern nach, als es Öffnungsklauseln für nationale Regelungen vorsah. Dadurch aber gab das Parlament selbst die Zielsetzung eines einheitlichen europäischen Datenschutzrechts weitgehend auf.

Hinsichtlich der Gewaltenteilung innerhalb der Union reagierte das Parlament stärker. Es beließ der Kommission nur zehn Ermächtigungen und war bemüht, vieles in der Verordnung selbst zu regeln. Die normative Inhaltsleere der Regelungen versuchte es mit vielfältigen Präzisierungen und Erweiterungen auszugleichen, ohne jedoch ein eigenständiges Regelungskonzept zu entwickeln. In den entscheidenden Fragen kam auch das Parlament angesichts der Komplexität und Breite der Regelungsmaterien über abstrakte Regelungen selten hinaus.

Auch der Rat hat die Wahl einer Verordnung, die, soweit sie reicht, den Mitgliedstaaten den Datenschutz als Gegenstand ihrer Politik und Gesetzgebung nimmt, akzeptiert.[21] Nicht akzeptiert hat er aber die Machtkonzentration der Kommission und beließ ihr nur neun Ermächtigungen für nebensächliche Fragen. Der Rat strich auch viele Detaillierungen des Parlaments. Die Macht, über die Zukunft der digitalen Gesellschaft zu bestimmen, sollte zum großen Teil bei den Mitgliedstaaten bleiben – insbesondere, wenn es ihre eigenen Angelegenheiten und nicht den europäischen Binnenmarkt betrifft. Überall, wo die geringe Komplexität der Regelungen des Kommissionsentwurfs Detaillierungen forderten, wurden – statt der Kommission – die Mitgliedstaaten ermächtigt, bestehende eigene Regelungen beizubehalten oder neue zu erlassen.

Im „Trilog", in dem sich Vertreter des Rats und des Parlaments unter Vermittlung der Kommission auf eine gemeinsame, die später verabschiedete Fassung einigten, blieben nur zwei Ermächtigungen der Kommission, delegierte Rechtsakte zu erlassen, und sieben Ermächtigungen für Durchführungsrechtsakte übrig. In Verhältnis der Union zu den Mitgliedstaaten konnte der Rat seine Ziele uneingeschränkt durchsetzen. Die mangelnde Komplexität der Verordnungsregelungen wird dadurch ausgeglichen, dass die Mitgliedstaaten ihre bereichsspezifischen Datenschutzreglungen beibehalten oder neue erlassen können. Der Machtkampf bewirkte aber auch, dass die drei expliziten Ziele der DSGVO weitgehend verloren gingen.

4.2 Ko-Regulierung statt Vereinheitlichung des Datenschutzrechts

Die DSGVO hat ein grundlegendes Problem, das durch den Machtkampf verstärkt und nicht beseitigt wurde: die hohe Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits sowie die Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 50 Artikeln des materiellen Datenschutzrechts die gleichen Probleme behandeln, für die im deutschen Datenschutzrecht Tausende von bereichsspezifischen Vorschriften bestehen. Wer Datenschutz regelt, verursacht Veränderungen in allen Gesellschaftsbereichen – vom Archivwesen bis zum Zeitungsverlag. Wer meint, die vielen und vielfältigen gesetzlichen Regelungen zum Datenschutz in den Mitgliedstaaten durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur diese Aufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, wenn er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und dadurch gewaltige Lücken der Rechtsunsicherheit erzeugt.[22]

Durch diesen unterkomplexen Regelungsansatz muss die DSGVO ihr eigentliches Ziel, einen soliden, kohärenten, einheitlichen Rechtsrahmen für den Datenschutz in allen Mitgliedstaaten der Union zu bilden, verfehlen. Vollzugsfähig und rechtssicher sind die Regelungen der Verordnung nur, wenn sie präzisiert, konkretisiert und ergänzt werden. Dies ist überwiegend Aufgabe der Mitgliedstaaten.[23] Das wichtigste Ergebnis aus dem Machtkampf um die Verordnung sind die 70 Öffnungsklauseln, durch die die Union den Mitgliedstaaten explizit Regelungskompetenzen im Datenschutzrecht überträgt. Diese sind unterschiedlich ausgestaltet. Sie eröffnen den Mitgliedsstaaten

taaten eigene Regelungsbereiche ohne spezifische Vorgaben – wie in Art. 88[24] für den Beschäftigtendatenschutz.[25] Sie ermächtigen aber auch die Mitgliedstaaten, „spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser" zu bestimmen. Die umfangreichsten Ermächtigungen dieser Art sind in Art. 6 Abs. 2 und 3 zu finden.[26] Danach kann jeder Mitgliedstaat für den gesamten Bereich der Datenverarbeitung in öffentlichen Stellen und in nicht öffentlichen Stellen, die zur Datenverarbeitung verpflichtet werden oder diese im öffentlichen Interesse vornehmen, eigene Regeln erlassen oder beibehalten.

Die Öffnungsklauseln verhindern eine unionsweite Vereinheitlichung des Datenschutzrechts. Dies widerspricht zwar den Wünschen und Hoffnungen, die viele mit der Verordnung verbunden haben. Mehr als dieses Nebeneinander von Unions- und nationalem Datenschutzrecht, das im günstigen Fall zu einer Ko-Regulierung führt, hat der Unionsgesetzgeber aber nicht gewollt.

Wie sehr im Ergebnis ein unionsweit einheitliches Datenschutzrecht verfehlt wird, kann in der Anpassung des deutschen Datenschutzrechts an die DSGVO besichtigt werden. Noch in der 18. Legislaturperiode hat der deutsche Gesetzgeber ergänzend zu ihr erste neue Datenschutzgesetze erlassen. Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 vom 30. Juni 2017 [27] enthält in Art. 1 das neue Bundesdatenschutzgesetz (BDSG). Dieses tritt am 25. Mai 2018 in Kraft und wird das bisherige BDSG vollständig ersetzen.[28] Art. 2 bis 6 enthalten Anpassungen des BVerfSchG, des MAD-G, des BND-G, des SiÜG und des G10-G. Außerdem hat der Bundesgesetzgeber im Gesetz zur Änderung des Bundesversorgungsgesetzes vom 24. Juli 2017[29] durch Art. 17 Neuregelungen zum Datenschutzrecht in der AO und durch Art. 19 und 24 im SGB I und X getroffen.

Das in Kürze in den Gesetzgebungsprozess einzubringende Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 wird in etwa 140 Artikeln weitere Regelungen zum Datenschutz in Fachgesetzen des Bundes an die Verordnung anpassen. Auch die Länder haben Gesetzgebungsverfahren angestoßen, in denen ihre jeweiligen Landesdatenschutzgesetze sowie ihre bereichsspezifischen Datenschutzregelungen neu gefasst werden.

Der Regulierungsstil dieser nationalen Anpassungsgesetze ist identisch. Sie sind von der Zielsetzung geprägt, das bestehende materielle Datenschutzrecht zu erhalten und nur formelle Anpassungen vorzunehmen. Es entfällt jedoch kein einziges Datenschutzgesetz und auch kein Abschnitt zum Datenschutz in den Fachgesetzen.

Im Ergebnis verfehlt die DSGVO weitgehend ihr Ziel, das Datenschutzrecht in der Union zu vereinheitlichen. Für Rechtsanwender und Rechtsbetroffene ist die Gemengelage aus DSGVO sowie dem weitgehend unveränderten deutschen Datenschutzrecht schwer zu durchschauen und verursacht ein hohes Maß an Rechtsunsicherheit.

4.3 Kontinuität in den Mitgliedstaaten statt einheitlicher Datenschutzpraxis

Stärker kommt die DSGVO im Bereich der Wirtschaft zur Anwendung. Doch auch wenn in allen Mitgliedstaaten die gleichen Vorschriften gelten, führt dies nicht immer zu unionsweit einheitlichen Wettbewerbsbedingungen. Gerade ihre vielen abs-

trakten und unbestimmten Regelungen bedürfen in der Praxis der Präzisierung und Konkretisierung durch die Verantwortlichen, betroffenen Personen, nationalen Aufsichtsbehörden und Gerichte.

Es ist ein entscheidender Unterschied, ob eine Richtlinie fünf Erlaubnistatbestände als Ziele vorgibt, die eine bereichs- und problemspezifische Konkretisierung durch nationale Gesetze erfahren sollen, oder ob die gleichen fünf Erlaubnistatbestände in einer Verordnung unmittelbare Rechtsgeltung haben und die bestehenden ausdifferenzierten und risikobezogenen nationalen Regelungen ersetzen sollen. Die Auslegung der identischen abstrakten Begriffe wird in jedem Mitgliedstaat nach der jeweiligen Datenschutztradition und -kultur erfolgen. Insbesondere die offene Abwägung berechtigter Interessen der Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person wird in jedem Mitgliedstaat unterschiedlich sein. Dies ist z.B. für die Videoüberwachung, für Werbung, Auskunfteien, Marktforschung, Scoring, Bonitätsauskünfte oder Internetangebote zu erwarten. Europäischer Datenschutz wird hinsichtlich der Zulässigkeit der Datenverarbeitung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Dadurch entsteht kein einheitlich durchgesetztes und gelebtes Recht. Wettbewerbsgleichheit ist so nicht zu erreichen.[30]

Indem die Verordnung die Entscheidung über die Abwägung letztlich auf die Gerichte überträgt, entstehen aber noch viel unterschiedlichere Ergebnisse als unter der DSRL. Bisher waren die typisierten vom Gesetzgeber vorgenommenen Interessenabwägungen wenigstens für Deutschland einheitlich. Jetzt wird es möglich sein, dass sie für lange Zeit von Gerichtsbezirk zu Gerichtsbezirk unterschiedlich ausfallen. Zwar haben für die Anwendung der unbestimmten Rechtsbegriffe die Aufsichtsbehörden des Bundes, der Länder und aller Mitgliedstaaten einen bestimmenden Einfluss. Um diesen unionsweit zu vereinheitlichen, gibt es umständliche Koordinationsmechanismen.[31] Da aber die Beschlüsse des Europäischen Datenschutzausschusses nach Art. 65 DSGVO nur die Aufsichtsbehörden verpflichten und kein allgemeinverbindliches (Exekutiv-)Recht setzen,[32] unterliegen die divergierenden oder vereinheitlichten Versuche der Aufsichtsbehörden, die Verordnung zu interpretieren, der Überprüfung durch die örtlichen Gerichte. Diese können jeden vereinheitlichten Interpretationsversuch durch den Datenschutzausschuss konterkarieren. Eine Vereinheitlichung der Rechtsprechung ist allenfalls in einzelnen Fällen bezogen auf die jeweils enge Fallfrage nach jahrelangen Prozessen[33] durch den EuGH zu erwarten.

4.4 Keine inhaltliche Modernisierung des Datenschutzrechts

Die DSGVO führt für das materielle Datenschutzrecht die Grundkonzeption der Datenschutz-Richtlinie von 1995 fort. Sie enthält keinen grundlegenden innovativen Ansatz, weist jedoch einige sinnvolle Neuerungen auf: Angesichts der Globalisierung der Datenverarbeitung ist die Ausweitung ihres räumlichen Anwendungsbereichs hilfreich. Danach ist die Verordnung auch anwendbar, wenn ein Datenverarbeiter – egal wo – personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten und der er entweder Waren oder Dienstleistungen anbietet oder die er durch seine Datenverarbeitung in ihrem Verhalten beobachtet.[34] Bisher unbekannt ist das Recht

für betroffene Personen in Art. 20 DSGVO, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen. Innovativ sind auch die Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 25 DSGVO[35] und die Datenschutz-Folgenabschätzung in Art. 35 DSGVO.[36]

Inhaltlich verursacht die Verordnung Defizite – auch gegenüber dem bisherigen Datenschutzniveau[37] – und verfehlt ihr Modernisierungsziel vor allem durch ihren spezifischen Ansatz der Technikneutralität.[38] Technikneutralität ist sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische Weiterentwicklungen ausschließen.[39] In der DSGVO wird Technikneutralität aber ideologisch überhöht und im Sinne einer Risikoneutralität[40] genutzt: In keiner Regelung werden die spezifischen Grundrechtsrisiken z.B. von smarten Informationstechniken im Alltag, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen, Künstlicher Intelligenz und selbstlernenden Systemen angesprochen oder gar gelöst. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die wenig riskante Kundenliste beim „Bäcker um die Ecke“ ebenso wie für diese um Potenzen risikoreicheren Datenverarbeitungsformen. Insbesondere durch abstrakte Zulässigkeitsregelungen wie in Art. 6 Abs. 1 werden die spezifischen Grundrechtsrisiken verfehlt.[41] Damit wird die Verordnung keiner der identifizierten Herausforderungen der zweiten und dritten Entwicklungsstufe der Datenverarbeitung[42] auch nur im Ansatz gerecht.

Letztlich muss klar sein, welche Anforderungen an die Verarbeitungsvorgänge gestellt werden. Diese Zielsetzung darf einerseits nicht dazu führen, dass die Vorschriften an technische Detailmerkmale anknüpfen, so dass sie technische Weiterentwicklungen ausschließen. Andererseits dürfen technikunspezifische Regelungen nicht dazu führen, dass der demokratisch legitimierte und zur Regelung berufene Gesetzgeber sich nicht mit den besonderen Interessenlagen und Risiken sowie passenden Lösungen einer Technikanwendung auseinandersetzt. Technikbezogene Regelungen sind gerade in einem so technikgeprägten Bereich wie dem Datenschutz unabdingbar, sollen die rechtlichen Ziele erreicht werden. Daher müssen spezifische Technikfunktionen und die typischen Verarbeitungszwecke, ihre Risiken und Lösungsansätze interessengerecht und risikoadäquat geregelt werden. Nur so kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden. Dass es im Unionsrecht sehr wohl möglich ist, sowohl technikneutrale als auch funktions- und risikobezogene Datenschutzvorgaben vorzusehen, zeigen etwa Art. 6 der eCall-VO (EU) 2015/758,[43] der klare Datenschutzanforderungen an die Zulässigkeit des automatisierten Notrufs stellt, oder die Regelungen zur Datenverarbeitung in der elektronischen Kommunikation, zum Schutz von Endgeräten und zur Steuerung zulässiger Werbung in den Art. 6, 8 und 16 des Entwurfs einer E-Privacy-VO.[44]

Die deutschen Gesetzgeber haben bisher weder im neuen BDSG noch in den Entwürfen zu den neuen Landesdatenschutzgesetzen die innovativen Impulse der DSGVO aufgenommen noch deren Risikoneutralität durch die risikobezogene Regelung moderner Herausforderungen überwunden. Sie haben die Öffnungsklauseln fast ausschließlich dazu benutzt, Möglichkeiten zur Verarbeitung personenbezogener Daten zu erweitern und Rechte der betroffenen Personen zu beschränken. Damit haben sie

im Ergebnis das Datenschutzniveau in Deutschland sowohl gegenüber dem bisherigen BDSG als auch sogar gegenüber der DSGVO reduziert.[45]

5. Innovationen im Vollzug

Die Differenz zwischen Sollen und Sein ist im Datenschutzrecht besonders groß. Daher ist es vor allem relevant, wie die Rechtsdurchsetzung in der DSGVO geregelt ist. Hier dürfte die wirkliche Innovation der Verordnung zu finden sein.

Die Regelung der Unabhängigkeit, der Aufgaben und der Befugnisse der Aufsichtsbehörden sowie deren Zusammenarbeit in der Union umfasst insgesamt 26 Artikel. Die Verordnung hat die Aufgaben und die Befugnisse erheblich ausgeweitet. Wichtig ist vor allem, dass die Aufsichtsbehörde nach Art. 58 Abs. 2 unmittelbare Durchsetzungsbefugnisse hat und z.B. eine rechtswidrige Datenverarbeitung verbieten kann. Eine auffällige Veränderung bringt auch Art. 83, der für Verstöße gegen die Verordnung drastische Sanktionen ermöglicht. Wichtig ist ferner, dass die Aufsichtsbehörde nach Art. 83 Abs. 6 bei Nichtbefolgung ihrer Anweisung Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen kann, je nachdem, welcher der Beträge höher ist.

Bei Vollzug der Verordnung entsteht allerdings ein Spannungsverhältnis zwischen der Sicherung der „völligen“ Unabhängigkeit jeder einzelnen Aufsichtsbehörde in Art. 52 Abs. 1 und dem einheitlichen Vollzug der Verordnung in der Union. Wie der EuGH in drei Entscheidungen zur Stellung der Aufsichtsbehörde in Deutschland, in Österreich und in Ungarn festgestellt hat, darf niemand der unabhängigen Aufsichtsbehörde Weisungen erteilen. Genau dies aber erlaubt Art. 65 Abs. 6 dem Europäischen Datenschutzausschuss. Er kann Entscheidungen treffen, die die betreffende Aufsichtsbehörde binden. Diese ist insoweit nicht mehr unabhängig, sondern muss die Entscheidung der Mehrheit der anderen Aufsichtsbehörden im Ausschuss befolgen. Auch in Deutschland wird die einzelne Aufsichtsbehörde im „kleinen Kohärenzverfahren“ nach § 18 BDSG-neu in ihrer Entscheidung von der Mehrheit der anderen Aufsichtsbehörden abhängig. Ein einheitlicher Vollzug in der Union wird wohl ohne Koordination der Aufsichtsbehörden nicht zu erreichen sein und diese Koordination kann nur nach dem Mehrheitsprinzip erfolgen. Dennoch ist zu konstatieren, dass die Mehrheit die einzelne Aufsichtsbehörde zwingen kann und Art. 65 die in Art. 52 garantierte Unabhängigkeit „auf dem Altar“ des einheitlichen Vollzugs „opfert“.

Wichtig ist aber auch, dass die Zivilgesellschaft in den Vollzug eingebunden wird. Bürger und in ihrer Vertretung Datenschutzverbände können bei der Aufsichtsbehörde Beschwerde einlegen und gegen die Aufsichtsbehörde und gegen den Verantwortlichen Rechtsbehelfe einlegen, wenn sie der Meinung sind, dass gegen die Verordnung verstoßen wird. Haben sie dadurch einen Schaden erlitten, können sie auch Schadensersatz geltend machen.

Ob diese neuen Regelungen die Durchsetzung des Datenschutzrechts in der Wirklichkeit verbessern, hängt davon ab, wie sie in der Praxis angewendet werden. Dies

setzt eine den neuen Aufgaben entsprechende Ausstattung der Aufsichtsbehörden voraus,[46] die derzeit noch fehlt. Daran wird der politische Wille zu besserem Datenschutz zu messen sein.[47] Die bisherigen Regelungen im BDSG und in den Landesdatenschutzgesetzen beschränken jedoch die Aufsicht im öffentlichen Bereich im Vergleich zur Verordnung.

6. Modernisierung des europäischen Datenschutzrechts

Die DSGVO hat weder zu einer Vereinheitlichung und Modernisierung des Datenschutzrechts geführt noch wird sie eine einheitliche Datenschutzpraxis in allen Mitgliedstaaten begründen. Statt einer Monopolisierung und Zentralisierung in der Weiterentwicklung des Datenschutzrechts hat sie eine sinnvolle Arbeitsteilung zwischen Union und Mitgliedstaaten eingerichtet. Nur so ist die notwendige Komplexität der Datenschutzregelungen angesichts einer gesellschaftsweiten Verarbeitung personenbezogener Daten zu erreichen. Die angeordnete Ko-Regulierung kann auch für die Suche nach einem modernen Datenschutzrecht eingesetzt werden: Angesichts der Vielfalt und Dynamik der zukünftigen, heute noch unbekannten Herausforderungen der Informationstechnik und ihrer Anwendungen für die Grundrechte kann auf der Ebene der Mitgliedstaaten mit unterschiedlichen Regelungskonzepten experimentiert werden. Deren Vielfalt kann dazu beitragen, dass sich in der Union ein lebendiger Datenschutz entwickelt. Statt einer Vereinheitlichung der Datenschutzpraxis ermöglichen unbestimmte Rechtsbegriffe und ihre situationsgerechte Konkretisierung, dass in den einzelnen Mitgliedstaaten Datenschutz den lokalen Bedingungen angepasst werden kann. Schließlich bieten die vielen Regelungsmöglichkeiten der Mitgliedstaaten Chancen für eine Modernisierung des Datenschutzrechts, indem dort versucht wird, durch risikoadäquate Regelungen einen ausreichenden Schutz der Grundrechte gegen künftige Herausforderungen zu gewährleisten. In den Evaluationen und Überarbeitungen der DSGVO gemäß Art. 97 kann dann das Bewährte unionsweit übernommen werden.

PROF. DR. ALEXANDER ROßNAGEL ist Universitätsprofessor für öffentliches Recht, Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnikgestaltung (ITeG) und Sprecher der Forums Privatheit.

Anmerkungen:

1 EU ABl. L 119 vom 4.5.2016, 1.
2 Zu den einzelnen Regelungen der DSGVO s. die Beiträge von *Schaar* und *Weichert* in diesem Heft.
3 KOM(2017) 10 endg.
4 Europäisches Parlament, A8-0324/2017.
5 S. *Roßnagel*, MedienWirtschaft 1/2018, 32ff.
6 Mitteilung der Europäischen Kommission: Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg.; Justizkommissarin *Reding*, ZD 2012, 195.
7 S. z.B. *Schaar*, DuD 2012, 154.
8 S. z.B. Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), Positionspapier zum Entwurf der DSGVO vom 25.1.2012.
9 S. z.B. *Albrecht*, CR 2016, 97.
10 *Albrecht*, CR 2016, 97; BfDI *Voßhoff* nach heise-online, http://heise.de/-3179872 vom 21.4.2016.
11 *Albrecht*, CR 2016, 98.
12 *Schantz*, NJW 2016, 1841.
13 *Albrecht*, CR 2016, 97.
14 *Hoeren*, nach heise-online, http://heise.de/-3190299 vom 27.4.2016; ähnlich negativ *Giesen*, Euphorie ist kein Prinzip des Rechtsstaats, in: Stiftung Datenschutz (Hrsg.), Zukunft der informationellen Selbstbestimmung, 2016, 23 ff.
15 S. hierzu *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007.
16 So z.B. in der Mitteilung der Kommission „Eine Vision für den Binnenmarkt für Industrieprodukte“ vom 22.1.2014, KOM(2014) 24 endg., 9.
17 S. hierzu auch *Roßnagel*, in: ders. (Hrsg.), Das neue Datenschutzrecht, 2018, § 1 Rn. 16 ff.
18 KOM(2012) 11 endg.
19 Nach dem Scheitern dieser Strategie werden beide Instrumente der Machtsteigerung vom Generalsekretär der Kommission, Selmayr, nachträglich als geniale Scheingefechte dargestellt, die nie ernst gemeint waren, sondern nur die Mitgliedstaaten zu entsprechenden Entscheidungen verleiten sollten – s. *Selmayr/Ehmann*, in: Ehmann/Selmayr, DSGVO, 2017, Einleitung Rn. 56.
20 EU-Parlament, P7_TA-PROV(2014)0212.
21 Rat der Europäischen Union, 9565/15.
22 S. näher *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – „Smart“ genug für die Zukunft?, 2016, 176f.
23 S. hierzu näher *Roßnagel* (Fn. 17), § 1 Rn. 31 ff. und § 2 Rn. 1 ff.
24 Art. und EG ohne Gesetzesbezeichnung sind solche der DSGVO.
25 S. z.B. *Maier*, DuD 2017, 169; *Roßnagel*, DuD 2017, 292.
26 S. *Roßnagel*, in: Simitis/Hornung/Spiecker, DSGVO, 2018, Art. 6 Abs. 2 Rn. 1 ff. und Art. 6 Abs. 3 Rn. 1 ff.; *Roßnagel* (Anm. 17), § 2 Rn. 21 ff.; *Schaller*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, § 7 Rn. 16f.
27 BGBl. I, 2097.
28 S. dazu den Beitrag von Schaar in diesem Heft.
29 BGBl. I, 2541.
30 So aber *Voßhoff*, in: BfDI-Info 6: Datenschutz-Grundverordnung, 2016, 7.
31 S. Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 77 ff., 146 ff.
32 S. *Roßnagel* (Anm. 31), 151 ff.
33 Das Urteil zur Vorratsdatenspeicherung vom 8.4.2014 erfolgte über acht Jahre nach Erlass der Richtlinie zur Vorratsdatenspeicherung, das Urteil zu Safe Harbor vom 6.10.2015 erging über 15 Jahre nach der Entscheidung der Kommission zur Anerkennung des Safe-Harbor-Systems.

34 Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten.
35 Die Anforderung richtet sich jedoch an den verantwortlichen Technikanwender, statt an den Hersteller.
36 Die sich hoffentlich nicht in einem Formalismus erschöpfen wird.
37 Entgegen der Zusicherung der damaligen Justizkommissarin *Reding*, ZD 2012, 197.
38 S. EG 15; *Reding*, ZD 2012, 198.
39 S. grundsätzlich *Roßnagel,* Technikneutrale Regulierung: Möglichkeiten und Grenzen, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, 323 ff.
40 Der „Risikoansatz" der DSGVO – s. z.B. *Albrecht*, CR 2016, 94 – beschränkt sich darauf, bestimmte Pflichten des Verantwortlichen „entsprechend der Risiken von Datenverarbeitungsprozessen" zu reduzieren; s. kritisch *Roßnagel*, DuD 2016, 565, weil dieser Ansatz bewirkt, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss.
41 S. näher *Roßnagel*, DuD 2016, 565.
42 S. Kap. 2.
43 EU ABl. L 123 vom 19.5.2015, 77.
44 S. hierzu *Roßnagel*, MedienWirtschaft 1/2018, 32ff.
45 S. dazu den Beitrag von Schaar in diesem Heft.
46 *Roßnagel* (Anm. 31), 179 ff.
47 S. zum Datenschutz in der Koalitionsvereinbarung Forum Privatheit, Datenschutz stärken, Innovationen ermöglichen – Wie man den Koalitionsvertrag ausgestalten sollte, Policy Paper, 2018.