Johannes Caspar

Zwischen Symbolik und Gestaltungskraft – Ist die EU-DSGVO eine Mogelpackung?

Neben einigen materiell-rechtlichen Neuregelungen zum Datenschutz stellen die Etablierung des Europäischen Datenschutzausschusses (EDSA) sowie die Regelungen zur Zuständigkeit bei länderübergreifenden Anwendungsfragen und der dabei vorgeschriebenen Kooperation der nationalen Aufsichtsbehörden zentrale Innovationen der Datenschutzgrundverordnung dar. Der folgende Beitrag von Johannes Caspar stellt diese neuen Verfahrensregelungen vor und diskutiert, inwiefern sie dazu beigetragen haben, das Ziel einer Harmonisierung der europaweiten Anwendung des Datenschutzrechts zu verwirklichen. Seine Bilanz fällt indes ernüchternd aus.

1. Einleitung: DSGVO eine Magna Charta für das digitale Zeitalter?

Die Europäische Datenschutzgrundverordnung (DSGVO) ist die zentrale Antwort Europas auf die vielfältigen Herausforderungen der Rechte der Privatsphäre des Einzelnen in einer immer schnelleren Zeit der umfassenden Digitalisierung von Staat und Gesellschaft.[1] Über viele Jahre lang beraten und öffentlich diskutiert, wird die DSGVO mitunter als *Magna Charta* der Privatsphäre bezeichnet.[2] Darin kommt eine besondere Wertschätzung zum Ausdruck, die dem zentralen Regelungswerk für den Schutz der personenbezogenen Daten in der EU als Garant der Rechte und Freiheiten des Einzelnen im digitalen Zeitalter zugeschrieben wird. Der geschichtliche Vergleich signalisiert zudem, dass der Erlass der DSGVO eine rechtshistorische Zäsur darstellt, die aus der Perspektive zukünftiger Betrachter erheblichen Einfluss auf die Rechtsentwicklung in Gegenwart und Zukunft ausüben wird. Klar ist, dass in einer von Daten angetriebenen Welt für wirtschaftliche Prozesse, aber auch ganz allgemein für Verhaltenssteuerung die Verarbeitung von Daten ein zentraler Schlüssel für geschäftlichen Erfolg sowie für die soziale Kontrolle des Verhaltens von Individuen und Gruppen dar-

Zitiervorschlag:
Caspar, Johannes (2020): Zwischen Symbolik und Gestaltungskraft – Ist die EU-DSGVO eine Mogelpackung?, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 231/232 [59(3-4)], S. 99-116.

stellt. Ob der historische Vergleich mit der *Magna Charta* dem Realitätscheck standhält, soll im Folgenden näher betrachtet werden.

Bereits hier kann festgehalten werden, dass zumindest die Verbindung zwischen *Magna Charta* und der Datenschutzgrundverordnung inhaltlich aus historischen Gründen nicht wirklich zutrifft. So war die *Magna Charta* doch ursprünglich eine Regelung, die einer Vereinbarung zwischen dem englischen Adelsstand und dem König von England entsprang und dem Adel Freiheitsrechte gegenüber der Krone einräumte.[3] Die Datenschutzgrundverordnung stellt dagegen alles andere als eine Vereinbarung über Privilegien zwischen Herrschaftsständen dar, sondern zielt gerade darauf ab, die Rechte der Nutzerinnen und Nutzer möglichst wirksam zu schützen. Sie ist geschaffen worden, um die Auswirkungen der extremen Form der Ungleichheit, die sich im digitalen Kapitalismus zwischen Plattformen und Internetdiensten einerseits und deren Nutzerinnen und Nutzern andererseits herausgebildet hat, im Rahmen einer Gewährleistungsverantwortung des Staats auf das Grundrecht der informationellen Selbstbestimmung Betroffener zu beschränken. Die Digitalisierung und die daraus hervorgehenden wirtschaftlichen Strukturen werden zusehends von großen, global agierenden Technikkonzernen gestaltet, die weltweit massenhaft Daten verarbeiten und über scheinbar grenzenlose finanzielle Mittel für den Ausbau ihrer Marktmacht verfügen. Ihnen gegenüber stehen die Nutzerinnen und Nutzer, die bei der Inanspruchnahme von Diensten der Informationsgesellschaft mit der Währung ihrer personenbezogenen Daten bezahlen, ohne zumeist den Preis zu kennen, den sie für die Nutzungsmöglichkeiten entrichten. Zahlt der Kunde jedoch nicht mit Geld, sondern mit den eigenen Daten, die letztlich Verzeichnisse seiner Persönlichkeit sind, dann ist er selbst das Produkt. Das Datenschutzrecht und insbesondere die seit 2018 geltende EU-Datenschutzgrundverordnung enthalten daher materielle Gewährleistungen für die Betroffenen und stärken die Rechte gegenüber einem Buy-Out der individuellen Privatsphäre. Die zur harmonisierten Durchsetzung dieser Rechte erforderlichen Sanktions- und Verfahrensregelungen für ganz Europa führen dazu, dass die Europäische Datenschutzgrundverordnung eine Vollregelung für den Datenschutz mit einer beachtlichen Regelungstiefe von 99 zum Teil sehr umfangreichen Artikeln geworden ist. Zweifellos ist die DSGVO eine starke Antwort auf die zentralen Herausforderungen für den Schutz der Privatsphäre im digitalen Zeitalter. Aber hält sie, fast zweieinhalb Jahren nach ihrer Geltungskraft, die mit ihr verbundenen Versprechen – oder erweist sie sich eher als ein Hindernis für die Rechte und Freiheiten Betroffener? Dieser Frage soll hier nachgegangen werden.

2. Datenschutz als das Recht der kleinen Leute

Zu den gänzlich neuen bzw. zumindest optimierten Rechten für Betroffene zählen in der DSGVO neben der Portabilität der Daten und dem Recht auf Vergessen Transparenzanforderungen, Auskunfts- und Informationsrechte. Sie setzen auf dem Feld des Datenschutzes neue Standards und finden weltweit Beachtung, da sie für alle Unter-

nehmen gelten, die ihre Waren oder Dienstleistungen betroffenen Personen in der Union anbieten.

Die neuen Regelungen der DSGVO bringen in Gestalt einer in allen EU-Mitgliedsstaaten geltenden Verordnung einen harmonisierten Rechtsstandard, der den bisherigen Flickenteppich aus unterschiedlichen Regelungen im nationalen Bereich, der im Zuge der abgelösten Datenschutzrichtlinie[4] entstanden ist, durch eine unmittelbar anwendbare einheitliche Regelung ersetzt. Neben gänzlich neuartigen oder zumindest fortentwickelten subjektiven Rechten wird den Betroffenen darin auch ein Recht auf Schadensersatz für den Fall eingeräumt, dass ihnen aufgrund von Verstößen gegen Datenschutzgesetze materielle oder immaterielle Schäden entstanden sind.

Flankiert werden diese subjektiven Rechtsgewährleistungen in der DSGVO durch entsprechende prozedurale Neuregelungen für den Vollzug und die Rechtsdurchsetzung. Die Möglichkeit für Aufsichtsbehörden, Bußgelder in Höhe von bis zu 20 Millionen Euro oder 4% des jährlichen Gesamtumsatzes eines Unternehmens zu verhängen, stellt insoweit ein extrem scharfes Instrument im Kampf gegen Datenschutzverletzungen dar und dient der Abschreckung.[5]

Recht haben ist allerdings bekanntermaßen etwas anderes als sein Recht zu bekommen. Gerade im Bereich des Datenschutzes besteht seit jeher ein enormes Gefälle zwischen Normativität und Faktizität, zwischen Rechtsgeltung und Rechtswirklichkeit. Die Gründe hierfür sind vielschichtig. Vorschriften mit einem extensiven Anwendungsbereich und auslegungsbedürftiger Offenheit, wie sie in der DSGVO enthalten sind, erschweren in der Praxis den Vollzug. Eine gefestigte höchstrichterliche Rechtsprechung, aber auch gerichtlich überprüfbare Entscheidungen mangels Zeitablaufs seit Geltung der DSGVO fehlen bisher. Deshalb ist eine autonome Rechtsverfolgung durch Betroffene gegenüber Daten verarbeitenden Stellen, seien diese nun staatliche oder private Einrichtungen, besonders schwierig.

Das führt zu einer Besonderheit des Datenschutzrechts: Obwohl es sich bei dem Schutz personenbezogener Daten um höchstpersönliche Rechtsgüter des Einzelnen handelt, ist deren Schutz nicht allein in die Hände des Betroffenen gelegt, wie etwa im Bereich des zivilrechtlichen Persönlichkeitsrechts. Zur effektiven und kostengünstigen Durchsetzung der individuellen Datenschutzrechte und dem Recht auf Privatsphäre ist die Rechtswahrung vielmehr einer unabhängigen Instanz übertragen, die Interessen von Einzelpersonen gerade gegenüber privaten Datenverarbeitern, aber auch gegenüber staatlichen Stellen, die personenbezogene Daten verarbeiten, durchsetzen helfen soll. Diese Aufgabe übernehmen in allen Bundesländern, im Bund, aber auch in allen anderen EU-Mitgliedstaaten besondere Aufsichtsbehörden für den Datenschutz. Deren wichtige Funktion als Kontroll- und Durchsetzungsinstanz des Datenschutzes und als Anwalt von den in ihren Rechten verletzten Bürgerinnen und Bürgern erfordert eine besondere Form der Weisungsfreiheit. Diese ist normalerweise im weisungsgebundenen Bereich exekutiver Funktionen gerade nicht gegeben und kann am ehesten mit der richterlichen Unabhängigkeit verglichen werden.

Das Prinzip der völligen Unabhängigkeit der Aufsichtsbehörden stellt einen unionsrechtlichen Grundsatz dar, der nicht nur vor unmittelbaren und mittelbaren äußeren Einflussnahmen schützt, sondern aus dem auch Rechte auf eine angemessene Ausstattung zur Erfüllung dieser Aufgaben folgen.[6] Dies ergibt sich nicht nur aus der

DSGVO, sondern auch aus dem Primärrecht der Gemeinschaft und ist in Art. 8 der Charta der Grundrechte der Europäischen Union, in Art. 16 Abs. 2 S. 2 AEUV sowie Art. 39 S. 2 EUV verankert. Die Unabhängigkeit erweist sich gegenüber anderen öffentlichen Stellen insbesondere am völligen Freisein von Rechts- und Fachaufsicht, aber auch von einer zumindest umfassenden Dienstaufsicht über den Leiter der Aufsichtsbehörde. Die Unabhängigkeit hat einen stark dienenden Charakter und bezieht sich auf die Funktion der Aufsichtsbehörden als Anwalt der kleinen Leute und ist kein Selbstzweck.

Datenschutzbehörden waren in den vergangenen Jahren verselbständigte, weitgehend unabhängig voneinander agierende Einzelbehörden, die in eigener Regie und nach eigenem Selbstverständnis ihrer Aufgabe nachgingen. Durch ihren Zusammenschluss auf nationaler Ebene im Rahmen der DSK (Konferenz der Unabhängigen Aufsichtsbehörden für den Datenschutz in Bund und Ländern) sowie der früheren sog. Art. 29-Arbeitsgruppe auf EU-Ebene gab es in der Vergangenheit zwei informelle Plattformen für eine Vereinheitlichung aufsichtsbehördlicher Entscheidungen. Die hier verlaufenden Abstimmungen erfolgten auf freiwilliger Basis und hatten für die beteiligten Behörden keine rechtliche Verbindlichkeit. Damit wurde in der Vergangenheit in zentralen Fragen des Datenschutzes eine weitgehend konsistente Anwendungs- und Vollzugspraxis des Datenschutzrechts auf einer übergeordneten Ebene erreicht.

3. Vom Lonely Rider zum Kollegialorgan – Aufsichtsbehörden in der DSGVO

Die Kommunikation zwischen den Aufsichtsbehörden hat sich mit Einführung der DSGVO auf europäischer Ebene grundlegend verändert. An die Stelle des Zusammenschlusses auf Basis der Art. 29-Arbeitsgruppe ist der Europäische Datenschutzausschuss getreten, ein Organ der EU mit eigenen Rechten, das aus dem Zusammenschluss aller mitgliedstaatlichen Datenschutzbehörden sowie dem Europäischen Datenschutzbeauftragten besteht und mit der Mehrheit der Stimmen eigene Entscheidungen zu datenschutzrechtlichen Fragestellungen trifft.

Die wohl größte Neuerung innerhalb der DSGVO betrifft die Struktur der Rechtsdurchsetzung bzw. des Rechtsvollzugs sowie die damit verbundene Änderung der Stellung der Aufsichtsbehörden. Die Einführung der Gesichtserkennung durch Facebook auf europäischer Ebene zu Beginn der 2010er Jahre oder die europaweiten Fahrten von Google für den Panoramadienst *Google Street View* vor 12 Jahren haben gezeigt, dass es im digitalen Zeitalter stärkere und schnellere gemeinsame Rechtsstrukturen braucht, um über die staatlichen Grenzen hinweg einheitlich auf die Herausforderungen in Datenschutzfragen zu reagieren.

Daten sind noch weniger als Handelsgüter an Grenzen gebunden. Ein wirksamer Schutz der Privatsphäre von Nutzern und Verbrauchern von Portugal bis Finnland war dem Projekt der EU daher zumindest denklogisch stets immanent, da Datenströme noch viel schneller Zeit und Raum überwinden. Die EU als einheitlicher Raum von

Rechten und Freiheiten aller Menschen setzt allgemeingültige Vorgaben eben nicht nur im Bereich der Warenströme und Dienstleistungen, im Rahmen des gemeinsamen Binnenmarktes, sondern auch mit Blick auf den grundrechtlichen Schutz der Menschen und ihrer Privatsphäre in der digitalen Welt voraus. Eine zentrale Antwort darauf ergibt sich aus der DSGVO und aus der Rolle, die der Europäische Datenschutzausschuss als oberstes Datenschutzgremium spielt.

3.1 In Kooperation vereint? Das sog. One-Stop-Shop-Verfahren und die Rolle von federführender und betroffener Behörde

Im Zuge der Beratungen zur DSGVO wurde eine unmittelbar geltende Vollregelung geschaffen, die mit einigen Bereichsausnahmen den Schutz persönlicher Daten als gemeinsame europäische Idee versteht. Um die Basis gemeinsamer Entscheidungen zu schaffen, die nicht nur in der Rechtsgeltung, sondern auch im Rechtsvollzug wirksam werden können, wurde mit dem Europäischen Datenschutzausschuss (EDSA) ein umfassendes zentrales Steuerungsgremium etabliert. Grob beschrieben funktioniert der Vollzug des Rechts aus einem kooperativen Zusammenwirken zwischen sog. federführenden und sog. betroffenen Behörden. Fragen zur Rechtsanwendung der DSGVO, die zwischen den beteiligten Behörden zu Dissens führen, münden in ein kollegiales Streitbeilegungsverfahren im Europäischen Datenschutzausschuss, wo sie dann im Rahmen des sog. Kohärenzverfahrens weiter behandelt werden.

Der aktive Teil im Rechtsvollzug fällt in diesem Regelungskonzept den sog. federführenden Behörden zu, die als Ansprechpartner und Regulierungssprachrohr für alle Aktivitäten von datenverarbeitenden Unternehmen in Europa fungieren. Ihnen an die Seite gestellt sind sog. betroffene Behörden. Eine Betroffenheit der Behörde liegt vor, soweit erhebliche Auswirkungen auf Personen mit Wohnsitz im eigenen Mitgliedstaat der Datenverarbeitung bestehen, soweit Beschwerden bei der Aufsichtsbehörde eingelegt werden oder soweit sich eine Niederlassung der verantwortlichen Stelle im jeweiligen Mitgliedstaat der Behörde befindet.[7]

Bestehen im Einzelfall Hinweise auf Datenschutzverstöße bei der verantwortlichen Stelle, haben betroffene und federführende Aufsichtsbehörden in einen Informationsaustausch einzutreten, bei dem sie einander zunächst zweckdienliche Informationen übermitteln. Diese fließen dann in einen Beschlussentwurf der federführenden Behörde ein, den sie auf Basis ihrer rechtlichen Würdigung für eine Entscheidung gegenüber der verantwortlichen Stelle ausfertigt. Der Beschlussentwurf wird an die betroffenen Behörden übermittelt und kann innerhalb einer vierwöchigen Frist von jenen mit einem Einspruch belegt werden. Ist die federführende Behörde nicht bereit, diesem Einspruch abzuhelfen, so wird das Streitbeilegungsverfahren nach Artikel 65 DSGVO eingeleitet, was bedeutet, dass die Entscheidung über die strittigen Punkte durch den Europäischen Datenschutzausschuss nach Maßgabe der Mehrheitsentscheidung des Kollegialgremiums zu fällen ist.

Dieses komplexe Verwaltungsverfahren stellt eine Abkehr vom Prinzip der monokratischen Entscheidung von Verwaltungsbehörden im Bereich des Rechtsvollzugs dar. Es ordnet zudem die Unabhängigkeit der einzelnen Behörde einer kollektiven

Unabhängigkeit aller Behörden unter. Demokratisch legitimierte Amtsträger werden für ein kooperatives Verwaltungsverfahren zusammengeschaltet, um eine besondere Form der demokratischen Rechtsanwendung zu gewährleisten.

Anders als bei der gemeinsamen Verabschiedung von Leitlinien, Empfehlungen und Stellungnahmen durch den Europäischen Datenschutzausschuss, die insbesondere die einheitliche Auslegung von Bestimmungen der DSGVO betreffen, geht es hierbei um die Kernaufgabe exekutiver Verantwortlichkeit, den Vollzug verbindlicher Einzelmaßnahmen ggfs. durch den Erlass von Sanktionen.

Das Verfahren wird auch als One-Stop-Shop bezeichnet, da es die gesamte Kontrolle und Kommunikation mit einem Unternehmen bei grenzüberschreitenden Datenverarbeitungen europaweit auf die federführende Behörde an der Hauptniederlassung des Unternehmens in der EU verweist. Das ist für die Unternehmen angenehm, da sie es nicht mit verschiedenen Behörden in Datenschutzverfahren zu tun haben und für Fragen der Datenverarbeitung in der EU nur einen Ansprechpartner haben, alle datenschutzrechtlichen Angelegenheiten also „in dem einen Shop" erledigen können. Gleichzeitig ermöglicht es gerade von außen kommenden Unternehmen, durch die Wahl der Hauptniederlassung in einem Mitgliedstaat sich die Behörde auszusuchen, die künftig europaweit die federführende Kontrolle über die Datenverarbeitung ausübt.

Umgekehrt gibt das Verfahren den Nutzerinnen und Nutzern in der EU gegenüber außerhalb des eigenen Mitgliedstaats ansässigen Unternehmen bei Beschwerden die Möglichkeit, sich an ihre nationale Aufsichtsbehörde zu wenden, die dann als betroffene Behörde den Fall an die federführende Behörde am Ort der Hauptniederlassung abgibt.

3.2 Die tatsächliche Situation bei der Kontrolle der grenzüberschreitenden Datenverarbeitung

Das Verfahren des One-Stop Shop erscheint auf den ersten Blick als ein tragfähiges Modell, sowohl auf der Seite der Betroffenen als auch auf der Seite der Daten verarbeitenden Unternehmen. Eine Win-Win-Situation schafft es dennoch nicht. Das zeigt ein Blick auf die Statistik: Das One-Stop-Shop-Verfahren bringt eine Fokussierung der Federführung auf einige wenige mitgliedstaatliche Behörden mit sich. So entfielen im Zeitraum vom 25. Mai 2018 bis zum 31. Dezember 2019 nahezu ein Drittel aller Verfahren in den 28 Mitgliedstaaten allein auf die Aufsichtsbehörden in Irland und Luxemburg.[8] Grund hierfür sind die nicht zuletzt aus steuerlichen Gründen dort angesiedelten Hauptniederlassungen der global Daten verarbeitenden Unternehmen. Das betrifft alle sog. Big Five-Unternehmen, die unter dem Akronym GAFAM in Irland (Google, Apple, Facebook, Microsoft) oder in Luxemburg (Amazon) ihre Hauptniederlassung gefunden haben. Aber auch andere große Plattformen (Twitter, Tinder, Linked In) und Internetdienstleister insbesondere aus den USA haben in Irland ihre Hauptniederlassung bezogen. Dublin kann insoweit als die Hauptstadt der außereuropäischen Tech-Industrie genannt werden. Damit sind zwei Mitgliedstaaten, in denen zusammen lediglich 2,1 % der Einwohner der EU (bezogen auf den Zeitpunkt vor dem

Austritt Großbritanniens am 31. Januar 2020) leben, in fast jedem dritten Fall als federführende Behörden zuständig. Dies dokumentiert eine Konzentration, die auf die Beschwerdesituation durchschlägt. Die Vorlage von Beschlussentwürfen nach Art. 60 Abs. 3 DSGVO ist für den Fortgang von Vollzugsverfahren eine zentrale Voraussetzung, ohne die es keine endgültige Entscheidung im Rechtsvollzug geben kann.[9] Von 214 Fällen zu grenzüberschreitenden Verfahren der Datenverarbeitung in den mehr als 1,5 Jahren vom 25.5.2018 bis 31.12.2019 wurde durch die vorbezeichneten Behörden lediglich in vier Fällen (und zwar von der luxemburgischen Aufsichtsbehörde) ein Entscheidungsentwurf vorgelegt. Aus Irland, auf das mit Abstand die meisten federführenden Fälle entfallen, ist in diesem Zeitraum kein Beschlussentwurf vorgelegt worden.[10] Die Problematik hat sich in 2020 verfestigt. Von Juni 2018 bis Mitte Oktober 2020 hat die irische Datenschutzaufsichtsbehörde lediglich drei Entscheidungsentwürfe vorgelegt. In allen drei Fällen liegen bislang noch keine endgültigen Entscheidungen vor, da gegen die Entwürfe durch andere Aufsichtsbehörden Einspruch eingelegt wurde. Ein Verfahren davon befindet sich als erstes Verfahren überhaupt im Stadium der streitigen Entscheidung vor dem EDSA (Stand: Oktober 2020).

3.3 Europäischen Datenschutzrecht mit zwei Geschwindigkeiten

Folge dieser Entwicklung des mitgliedstaatlichen Rechtsvollzugs ist ein Auseinanderfallen zwischen dem nationalen Vollzug des Datenschutzrechts, bei dem nur eine nationale Behörde allein zuständig ist, und dem kooperativen Vollzug bei grenzüberschreitenden Datenverarbeitungen, bei dem unterschiedliche Behörden auf der EU-Ebene zusammenarbeiten sollten. Der Output der beiden Vollzugskonzepte ist vor dem Hintergrund der Sanktionsstatistik (Stand: Oktober 2020) sowohl hinsichtlich der Höhe der Bußgeldbescheide als auch hinsichtlich der Anzahl der abgeschlossenen Bußgeldverfahren eindrücklich: Qualitativ wurden seit Geltung der DSGVO vier Bußgeldverfahren allein in Deutschland mit Bescheiden in einer Gesamthöhe von insgesamt ca. 60 Millionen Euro (Deutsches Wohnen, 1&1, AOK Baden Württemberg, H&M) abgeschlossen. Weitere größere Verfahren wurden in Frankreich (allein 50 Mio. gegen Google) sowie Italien (27,8 Mio. gegen TIM) abgeschlossen. Insgesamt stehen dem auf Ebene des One-Stop-Shop-Verfahrens für den grenzüberschreitenden Datenverkehr Bußgeldverfahren mit einer Gesamthöhe von nicht einmal 500.000 Euro gegenüber (Stand: 16.10.2020). Nachdem die Aufsichtsbehörde des Vereinigten Königreichs (ICO) am 16. Oktober 2020 ein Bußgeld in Höhe von 20 Millionen Britische Pfund gegen die Fluggesellschaft British Airways erlassen hat, die ursprünglich im Verfahren der grenzüberschreitenden Datenverarbeitung erfolgte, ist in diesem Verfahren das erste größere Bußgeld verhängt worden. Es muss jedoch darauf hingewiesen werden, dass das Vereinigte Königreich bereits Anfang 2020 aus dem Verbund der EU ausgetreten ist. Zwar gelten zunächst die Regelungen der DSGVO noch fort, allerdings haben die Regelungen des Kooperationsverhältnisses nach Art. 60 ff. DSGVO mangels Mitgliedschaft der ICO im EDSA derzeit eher symbolischen Charakter bis zum endgültigen Außerkrafttreten der DSGVO.

Ausweislich von statistischen Erhebungen über Bußgeldverfahren wurden sowohl national als auch grenzüberschreitend 593 Verfahren abgeschlossen.[11] Im grenzüberschreitenden Bereich führt die offizielle Statistik des EDSA lediglich 5 Verfahren auf, die mit Bußgeld endeten.[12] Auch für den Bereich der Anordnungen (*Administrative orders / Compliance Orders*) bestätigt sich das Bild, wonach rechtsverbindliche Maßnahmen eher die Ausnahme darstellen: Europaweit gab es in diesem Zeitraum nur 15 Anordnungen, wobei weder Verbote der Datenverarbeitung noch eine Löschung von Daten ausgesprochen wurde. Neben einigen Warnungen und Verwarnungen sind die meisten Verfahren unter den Rubriken „keine Verletzung", „keine Sanktion" sowie Verfahrenseinstellungen (*dismissal of the case*) genannt.[13]

Die darin zum Ausdruck kommende unterschiedliche Behandlung zwischen nationalen und grenzüberschreitenden Fällen der Datenverarbeitung gibt durchaus Anlass zur Sorge. Die mit den neuen datenschutzrechtlichen Regelungen verbundenen Erwartungen eines besseren Schutzes der Nutzerinnen und Nutzer vor globalen Online-Vermittlungsdiensten, die den Kunden Waren oder Dienstleistungen anbieten, Suchmaschinen und soziale Netzwerke bereitstellen oder Cloud Dienste und Online-Versandhandel betreiben, haben sich nicht erfüllt. Im Gegenteil sind sie massiv enttäuscht worden, finden sich doch gerade jene multinationalen Technikkonzerne trotz zahlreicher Datenskandale nicht auf der Liste der Sanktionen im grenzüberschreitenden Datenverkehr. Einzelne Verfahren, wie das Bußgeld gegen Google in Höhe von 50 Millionen Euro, sind gleichwohl nationale Verfahren und wurden ausschließlich von einer Aufsichtsbehörde betrieben. Da Google zu diesem Zeitpunkt noch über keine Hauptniederlassung in der EU verfügte und insoweit die Regelungen des One-Stop-Shops auf das Unternehmen keine Anwendung fanden, war in diesem Verfahren allein die französische Aufsichtsbehörde (CNIL) zuständig.

Dass gerade die durch den Einsatz von Tracking-Tools und Profilbildung besonders auf eine massenhafte Datenverarbeitung setzenden Dienste unter der DSGVO durchtauchen können, ist ein evidenter Grundwiderspruch zu dem zugrundeliegenden Schutzkonzept. Ausdrücklich werden die rasante technologische Entwicklung und die Globalisierung, die es privaten Anbietern ermöglicht, in einem noch nie dagewesenen Umfang auf Daten zuzugreifen, als zentrale Herausforderungen in der Datenschutzgrundverordnung genannt. Es wird ein „*solider kohärenter und klar durchsetzbarer Rechtsrahmen*" für einen hohes und in allen Mitgliedstaaten gleichwertiges Datenschutzniveau gefordert (vgl. DSGVO EG 6, 7; 10).

4. Ursachen für die Fehlentwicklung

Wo nun liegen die Hauptursachen für die mangelnde Umsetzung des Rechts auf Datenschutz innerhalb der EU, obwohl doch die EU-Datenschutzgrundverordnung immer wieder eine der profiliertesten Datenschutzregelungen in der Welt genannt wird?

Sicherlich gibt es für die offenbaren Widersprüche zwischen Rechtsgeltung und -vollzug keine ausschließliche Erklärung. Die Ursachen sind vielgestaltig und dennoch miteinander verbunden. Ansetzen muss die Ursachensuche bei den Webfehlern der

DSGVO in Bezug auf den aufsichtsbehördlichen Kooperations- und Kohärenzmechanismus. Hier wurden in guter Absicht zentrale Weichenstellungen vorgenommen, die zu einem ineffektiven, schwerfälligen und bürokratischen Vollzug führten und die im Praxistest bislang durchfielen.

4.1 Rechtsanwendung in der Diskursfalle – Im Vollzug ersetzt Reden kein Handeln

Problematisch erweist sich, dass der Gesetzgeber die Rechtsanwendung im Bereich des Datenschutzes auf europäischer Ebene in ein Diskursformat gegossen hat, das zu erheblichen Einbußen an Schnelligkeit, Klarheit und Strukturiertheit von behördlichen Entscheidungen führt. Rechtsvollzug muss abschreckend sein, was im Einzelfall zügige und klare Entscheidungen voraussetzt. Die vielen Abstimmungsrunden bei der gegenseitigen Amtshilfe und beim Austausch von Informationen, das Durchlaufen unterschiedlicher Ebenen zwischen federführenden und betroffenen Behörden sowie die Beteiligung des zentralen Gremiums des EDSA mit seinen vielen Subgroups, die Kommunikationsanforderungen auf allen Ebenen und schließlich die unterschiedlichen Sprachen der Beteiligten im Rechtsvollzug sind äußerst zeitintensiv.

Kooperations- wie auch die Kohärenzanforderungen stellen durchweg hohe *bürokratische Anforderungen* an das Verfahren. Die vielfältigen Informations-, Mitentscheidungs- und Abstimmungserfordernisse – für die nationalen Aufsichtsbehörden innerhalb der föderalen Struktur Deutschlands kommt eine Doppelung durch das Erfordernis der Einholung eines gemeinsamen Standpunktes im Rahmen der Bund-Länder-Abstimmung (vgl. § 18 BDSG) hinzu – erfordern immense personelle Ressourcen. Sie fehlen den Behörden bei anderen Aufgaben, insbesondere bei der Wahrnehmung der Rechte Betroffener in Beschwerdeverfahren.

Eine demokratische Rechtsanwendung, ausgerichtet am europäischen Ideal der Diversität, mag eine schöne Idee sein – ihre Erhabenheit zerschellt leider an der Realität. Am Ende geht sie auf Kosten der Rechte der zu schützenden Personen, die mit ihren Beschwerden in immer neue Diskursschleifen geführt werden, ohne in angemessener Zeit eine Entscheidung zu bekommen. Anders als die Schaffung von Rechtsnormen, bei dem demokratische Diskurse im Parlament das Verfahren zwingend bestimmen, ist für den Rechtsvollzug der entscheidende Faktor die Dezision durch eine demokratisch legitimierte Einrichtung. Deutlich gilt hier das Sprichwort: „*Viele Köche verderben den Brei.*“ Damit liegt eine wesentliche Ursache für das Scheitern bereits in der strukturellen Ausrichtung der neuen Regelungen auf eine umfassende Beteiligung möglichst vieler europäischer Aufsichtsbehörden.

4.2 Zu starke rechtliche Stellung der federführenden Behörde

Neben dieser grundsätzlichen Kritik gibt es zahlreiche weitere, detaillierte Regelungsdefizite. Ursprünglich sollte das Kohärenzverfahren, bei dem der EDSA die endgültige Entscheidung bei Meinungsverschiedenheiten trifft, Alleingänge der federführenden

Behörden vermeiden helfen. Die endgültige Zuständigkeit des EDSA und die vorherige Teilnahme der betroffenen Behörden an der Entscheidung der federführenden Behörde sollten als Korrektive einem Forum-Shopping der digitalen Großkonzerne am Ort ihrer Hauptniederlassung entgegenwirken.

Dieser Vorgabe wurde weder durch die gesetzlichen Regelungen noch durch die Auslegung der Regelungen zur Kooperation und zur Zusammenarbeit durch den EDSA entsprochen. Zuvorderst zeigt sich dies für den Fall fehlender Entscheidungsentwürfe durch die federführende Behörde: Bleibt die federführende Behörde untätig bzw. legt keine eigene Entscheidung vor, werden Entscheidungen europaweit blockiert. Verfahren, die seit über zwei Jahren ohne eine entsprechende Stellungnahme der federführenden Behörde ruhen, sind derzeit keine Seltenheit. Dass gegenüber Unternehmen wie Google, Facebook, Microsoft oder Apple bislang trotz zahlreicher anhängiger Verfahren und Beschwerden wegen mutmaßlicher Verstöße gegen Datenschutzbestimmungen nach weit mehr als zwei Jahren nicht ein einziger Entscheidungsentwurf beigebracht wurde, macht das Ausmaß der Abhängigkeit der anderen Aufsichtsbehörden von der federführenden Behörde deutlich. Die Verfahrensregelungen der DSGVO sehen keine entsprechenden Vorschriften vor, die einer Entscheidungsblockade durch die federführenden Behörden wirksam vorbeugen würden.[14]

Eine weitere Problematik stellt das komplexe Verfahren der Übernahme in ein Streitbeilegungsverfahren nach Durchlaufen des Einspruchsverfahrens in Art. 65 DSGVO dar. An dieser Stelle ist der EDSA als Kollegialorgan zur Mehrheitsentscheidung über einen nicht abgeholfenen Einspruch der betroffenen gegenüber der federführenden Behörde aufgerufen. Unklar ist bereits an der Regelungskonzeption, welche *Kontrollmaßstäbe* an das Streitbeilegungsverfahren anzulegen sind. Ist die Ausgestaltung des Streitbeilegungsverfahrens ein Verfahren der Rechtmäßigkeitskontrolle, das an einer gerichtlichen Entscheidung orientiert ist und ist der EDSA damit eine Art gerichtliche Clearingstelle? Oder kommt ihm eine Stellung wie einer vorgeordneten Verwaltungsbehörde im Widerspruchsverfahren nach der VwGO zu, sodass eine Beschlussentwurf auch im Rahmen einer Zweckmäßigkeitskontrolle geändert werden kann, ohne dass es eines Verstoßes der federführenden Behörde gegen die DSGVO bei der Abfassung ihres Entscheidungsentwurfs bedarf? Wer legt im Übrigen den Bezugsrahmen der Überprüfung fest? Ist es die rechtliche Auslegung der federführenden Behörde oder der Sachverhalt, der dem Verfahren der Überprüfung des Beschlussentwurfs zugrunde liegt? Kann der EDSA selbst entscheiden, dass ein Bußgeld zu niedrig ausfällt und kann er sogar eigene konkrete Vorgaben mit verbindlichen Festlegungen hierzu machen? Diese Fragen können in der vorliegenden Darstellung nicht beantwortet werden. Allein die Masse der ungeklärten Auslegungsprobleme des Streitbeilegungsverfahrens zeigt, dass dieses Verfahren Rechtssicherheit gerade nicht schafft.

Die Auslegung des Anwendungsbereichs des Streitbeilegungsverfahrens im Rahmen des Artikel 65 DSGVO beschränkt oder erweitert den autonomen Entscheidungsspielraum der federführenden Behörde nach folgender Regel: Je weiter der Anwendungsbereich des Kohärenzverfahrens, desto eher kann eine Entscheidung der federführenden Behörde auf lokaler Ebene durch den EDSA korrigiert werden. Das entspricht Sinn und Zweck des Kohärenzverfahrens, denn allein eine Stärkung der Entscheidungsbefugnisse des EDSA gegenüber der federführenden Behörde kann zu einer

einheitlichen Rechtsanwendung innerhalb der EU führen. Legt man hingegen die Betonung auf die Unabhängigkeit der federführenden Behörde und deren autonome Entscheidungskompetenzen, so bewirkt dies eine Verfestigung einer partikularen Auslegung und führt damit zu einer inhomogenen Rechtsanwendung in der EU.

Das Streitbeilegungsverfahren mit all seinen Unklarheiten und offenen Auslegungsfragen ist daher eher Ursache von Meinungsstreitigkeiten zwischen den unterschiedlichen Positionen im EDSA. Auslegungsfragen zwischen federführenden und betroffenen Behörden widersprechen insoweit dem eigentlichen Ziel, dem das Verfahren zur Durchsetzung verhelfen sollte

4.3 Die Ausblendung des menschlichen Faktors – Rechtssetzung ohne Berücksichtigung der Interessenkonstellation

Die Entscheidung, gerade jene Behörden in das Verfahrenscockpit als federführend zu setzen, die am Standort der Hauptniederlassung des Datenverarbeiters ansässig sind, stellt eine gravierende rechtspolitische Fehlentscheidung im Gesetzgebungsverfahren zur DSGVO dar. Tatsächlich wird das Vorgehen gegen lokale Anbieter, die über den gesamten Raum der EU Daten verarbeiten, ganz wesentlich erschwert durch die Tatsache, dass die verantwortlichen Stellen am Ort der Hauptniederlassung nicht nur gewöhnlich ihre Steuern entrichten, sondern auch in einem hohen Maße qualifizierte Arbeitsplätze schaffen und damit die lokale Wirtschaft stärken.
Der Druck oder zumindest die allgemeine Stimmung, hier möglichst nicht oder zumindest nicht so hart durchzugreifen, kann durchaus nicht unbeträchtlich sein. Datenschutzrecht zu vollziehen, insbesondere zugunsten von Bürgerinnen und Bürgern, die möglicherweise tausende Kilometer entfernt ihren Lebensmittelpunkt haben, entgegen den lokalen Interessen des Standorts, ist schwierig und voller Widerstände. Dies stellt in keiner Weise einen Vorwurf an die Adresse von einzelnen Aufsichtsbehörden dar. Die Beeinflussbarkeit von menschlichen Entscheidungen durch äußere Umstände ist vielmehr ein empirischer Faktor beim Rechtsvollzug.

Die vom europäischen Gesetzgeber mit Recht so hoch gehaltene völlige Unabhängigkeit der Aufsichtsbehörden, gerade auch vor einer mittelbaren Einflussnahme, wird durch die Zuständigkeit und funktionsbasierte Verlagerung auf die federführende Behörde vor Ort systematisch konterkariert. Soweit es darum geht, ein höchstmögliches Maß an Rechtsgewährleistung für Betroffene zu erzielen, und soweit ein wirksamer Vollzug des europäischen Datenschutzes tatsächlich herbeigeführt werden soll, ist es eine strategische Fehlleistung des Gesetzgebers, gerade die Aufsichtsbehörden am Ort der Hauptniederlassung der zu kontrollierenden überregionalen Datenverarbeiter in die Rolle des Hauptregulierers zu bringen. Mit dem Konzept der federführenden Behörde am Ort der Hauptniederlassung der verantwortlichen Stelle hat der europäische Gesetzgeber ein Gegengewicht gegen Bußgelder und Sanktionsmaßnahmen der Aufsichtsbehörden geschaffen, das in der Praxis den Vollzug wesentlich erschwert.

4.4 Nationale Verfahrensvorschriften als Hindernisse eines einheitlichen Vollzugs

Ein weiteres Problem bei der Bewältigung von aufsichtsbehördlichen Verfahren im Bereich der grenzüberschreitenden Datenverarbeitung ergibt sich aus einer Verlagerung von aufsichtsbehördlichen Maßnahmen in die Abhängigkeit nationaler Verfahrensvorgaben. Nationale Regelungen, die insbesondere die Anhörung von Betroffenen und verantwortlichen Stellen unterschiedlich extensiv vorsehen, die den Austausch von Informationen mit Blick auf zu wahrende Betriebs- und Geschäftsgeheimnisse verantwortlicher Stellen zwischen den Aufsichtsbehörden unterbinden oder Vorschriften zur einvernehmlichen Verfahrensbeilegung schaffen, die im Vorwege eine weitere Befassung des Falles ausschließen oder erschweren,[15] werfen Sand in das Getriebe des Vollzugs und machen die europaweiten Verfahren wesentlich unübersichtlicher und schwieriger. Dabei ist ihre unionsrechtliche Vereinbarkeit mit Blick auf Kooperations- und Kohärenzverfahren im Rahmen der Artikel 60 ff. DSGVO höchst fraglich. In jedem Fall wäre es sinnvoll, über die bisherigen Regelungen des Kooperationsverfahrens gemeinsame europäische Verfahrensregelungen zu schaffen, um künftig die unterschiedlichen Standards der Verfahrensbeteiligten zu vereinheitlichen.

4.5 Zusammenfassung

Insgesamt zeigt der One-Stop-Shop eine bedenkliche Tendenz, das Verfahren der Rechtsanwendung von einem kontradiktorischen Verfahren zwischen Betroffenen, Verantwortlichen und Behörden auf die Ebene einer interorganschaftlichen Streitbeilegung zwischen Betroffenen und federführenden Behörden zu verlagern. Das führt nicht nur zu einer erheblichen Schwerfälligkeit der Aufsicht in grenzüberschreitenden Fällen, die schnelle und klare Entscheidungen verhindert, sondern stellt auch eine völlig intransparente Veranstaltung dar. Über Monate oder sogar über Jahre laufende Verfahren zwischen europäischen Behörden unter Ausschluss der Öffentlichkeit können nicht im Sinne eines offen kommunizierten Datenschutzes sein. Die Behörden werden vielmehr durch die DSGVO in einen redundanten Selbstbeschäftigungsmodus versetzt. Das führt hinter den Kulissen zu Grabenkämpfen um die richtige Anwendung von Gesetzen, durch die die Behörden ihre ohnehin fehlenden Kräfte weiter aufzehren. Es steht insoweit zu befürchten, dass der Datenschutz und der Schutz der Rechte und Freiheiten Betroffener durch die Ausgestaltung dieses Verfahrens am Ende auf die Verliererstraße geraten.

5. Den Tanker umsteuern?

Die gegenwärtige Schieflage beim Vollzug der Datenschutzgrundverordnung wirkt sich nicht allein negativ auf den Schutz von Rechten und Freiheiten der Menschen in einem Zeitalter der grenzenlosen Ökonomisierung personenbezogener Daten und der Optimierung der sozialen Kontrolle aus, sondern stellt auch einen Grundwiderspruch zu einem tragenden Prinzip der Europäischen Union und einer ihrer größten Errungenschaften dar: Sie widersprechen der Gewährleistung und Förderung eines fairen Wettbewerbs auf dem gemeinsamen Binnenmarkt. Dieser beruht auf der Prämisse, dass die EU den Rahmen für einen unverfälschten Wettbewerb innerhalb der EU schafft. Datenschutz- und Wettbewerbsfragen stehen in einem engen Zusammenhang und beeinflussen sich gegenseitig in ihren Auswirkungen.

Unterschiedliche datenschutzrechtliche Vollzugsstandards gegenüber Unternehmen, die an verschiedenen Standorten in Europa ihre Daten verarbeiten, führen zu massiven Verwerfungen auf dem digitalen Binnenmarkt. Sie konstituieren Ungleichheiten im Wettbewerb insbesondere zwischen Unternehmen, die seit jeher in einzelnen Mitgliedstaaten ansässig sind, und solchen, die von außen kommend sich in einem Mitgliedstaat ihrer Wahl niederlassen. Auf dem digitalen Markt werden durch die bestehenden Vollzugdefizite gerade jene Unternehmen prämiert, die ihre Marktmacht ausnutzen, um in datenschutzrechtlich fragwürdiger Weise Daten ihrer Nutzer zu verarbeiten.[16] Zwischen Datenverarbeitung und Wettbewerbsposition besteht ein gefährlicher Synergieeffekt. Das marktbeherrschende Unternehmen setzt seine Marktmacht ein, um mit datenschutzwidrigen Praktiken neue Nutzerinnen und Nutzer zu gewinnen. Dadurch wird wiederum seine Marktmacht gestärkt. Am Ende verfestigen die Verstöße gegen Datenschutz- und Wettbewerbsrecht die Stellung des Unternehmens am Markt und führen zu einer Stärkung des Unternehmens auf Kosten von Betroffenen und Wettbewerbern.

Gleichzeitig besteht ein Regelungsparadoxon, das man als „Datenschutzfalle“ bezeichnen könnte. Denn gerade die Einführung der DSGVO hat durchaus negative Auswirkungen auf die Wettbewerbsgleichheit der Unternehmen, da sie hohe Compliance-Hürden für datenverarbeitende Unternehmen errichtet und damit jene großen Daten verarbeitenden Unternehmen privilegiert, die über die nötigen personellen und finanziellen Mittel für die Umsetzung der Datenschutzstandards verfügen und deren Erfolg in hohem Maße auf der Auswertung von Daten beruht.[17] Es ist denn auch wenig überraschend, dass die globalen Plattformen und Diensteanbieter mit der Einführung des DSGVO-Regimes ihre Marktanteile im Bereich des Webtrackings steigern konnten.[18]

Neben derartigen Konzentrationswirkungen der DSGVO gilt es, zumindest weitergehende wettbewerbsverzerrende Vollzugsdefizite der DSGVO zu vermeiden. Für eine eigenständige europäische Digitalpolitik müssen Strukturen gestärkt werden, die kleinere innovative Unternehmen mit einem nachhaltigen Datenschutzansatz fördern. In den zuvor aufgezeigten Szenarien sind gerade sie die Verlierer in einem Wettbewerb, der auf Massendatenverarbeitung, Marktmacht und mitunter datenschutzwidrigen Praktiken beruht. Eigenständige europäische Digitalpolitik muss ausgerichtet sein auf

den Schutz der informationellen Selbstbestimmung und auf die digitale Souveränität der Menschen. Allein der Verweis auf die DSGVO als fortschrittlichste Regelung zum Schutz der Privatsphäre im globalen Maßstab reicht hier nicht aus. Die Ziele lassen sich nur erreichen, wenn die Vorgaben der Datenschutzgrundverordnung einheitlich durchgesetzt werden. Solange sich die Behörden durch langwierige und überbürokratische Verfahren von einem wirksamen Vollzug der Datenschutzregelungen für die großen digitalen Techfirmen im Bereich der grenzüberschreitenden Datenverarbeitung gegenseitig neutralisieren, kann davon nicht die Rede sein.

Angesichts der offenkundigen Schwierigkeiten im Vollzug, ihrer negativen Auswirkungen auf die Rechte und Freiheiten betroffener Nutzerinnen und Nutzer sowie ihrer wettbewerbsverzerrenden Wirkung auf dem digitalen Markt hätte ein Umsteuern bereits nach der ersten Evaluation der DSGVO erfolgen sollen.[19] Dies ist jedoch nicht geschehen. Die EU-Kommission hat in ihrer Stellungnahme zur Evaluierung der DSGVO weder Aktivitäten zur Neugestaltung ergriffen noch solche nur in Aussicht gestellt. Im Bericht heißt es:

> „Weitere Fortschritte sind erforderlich, um die Bearbeitung grenzüberschreitender Fälle in der gesamten EU effizienter zu gestalten und zu harmonisieren, auch in verfahrensrechtlicher Hinsicht, u. a. in Bezug auf die Bearbeitung von Beschwerden, die Zulässigkeitskriterien für Beschwerden, die Dauer von Verfahren aufgrund unterschiedlicher Zeitrahmen oder das Fehlen von Fristen im nationalen Verwaltungsverfahrensrecht, den Zeitpunkt des Verfahrens, in dem das Recht auf Anhörung gewährt wird, oder die Unterrichtung und Beteiligung der Beschwerdeführer während des Verfahrens. Der vom Ausschuss angestoßene diesbezügliche Reflexionsprozess wird begrüßt, und die Kommission nimmt an den betreffenden Diskussionen teil.“[20]

Der Europäische Datenschutzausschuss, auf den die EU-Kommission im vorangegangenen Zitat verweist, hat die Problematik der fehlenden Effizienz des Rechtsvollzugs zwar erkannt. Allerdings macht er deutlich, dass eine Revision der bestehenden Vorschriften verfrüht wäre, da erst noch weitergehende Erfahrungen mit der DSGVO zu sammeln seien.[21] Insoweit ist zu fragen, worauf derzeit eigentlich gewartet wird. Die rechtlichen Strukturen werden sich nicht von selbst ändern, sondern bedürfen der grundlegenden Veränderung durch legislatives Tätigwerden.

Vorschläge für eine verbesserte Umsetzung von Entscheidungen im grenzüberschreitenden Datenverkehr liegen bereits vor. Dazu zählt zunächst die Stärkung der Rechtsstellung betroffener Behörden gegenüber federführenden Behörden. Eine Regelung, die nach einem bestimmten Zeitraum des Nichtvorlegens eines Beschlussentwurfs ein Selbsteintrittsrecht betroffener Behörden und die Übernahme des konkreten Falles ermöglicht, könnte ein zu langes Untätigbleiben der federführenden Behörde und damit Blockaden verhindern. Gerade auch bei einer Überlast von Fällen bei einer federführenden Behörde wäre dies ein Weg, um einen stärkeren Input von Entscheidungsentwürfen in das Verfahren zu bekommen. So ließe sich eine Verschleppung oder Verzögerung der Verfahren durch erweiterte Befugnisse von betroffenen

Aufsichtsbehörden durch ein Selbsteintrittsrecht und die Übernahme von Fällen durch betroffene Behörden verhindern. Klare Fristvorgaben könnten die Arbeit der federführenden Behörde beschleunigen. Zwar enthält die Regelung in Artikel 60 Absatz 3 DSGVO bereits gegenwärtig die Verpflichtung der federführenden Behörde, den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vorzulegen. Der Begriff der Unverzüglichkeit bleibt jedoch vage und wird nicht zuletzt durch gegenläufige nationale Verfahrensbestimmungen ausgehebelt.

Eine Auslegung des Streitbeilegungsverfahrens nach Art. 65 DSGVO in Richtung einer Stärkung der Kompetenzen des Europäischen Datenschutzausschusses würde zudem eine extensivere Überprüfungskompetenz des EDSA gegenüber dem Entscheidungsentwurf der federführenden Behörde ermöglichen. Nur durch ein möglichst weites Verständnis der Entscheidungskompetenzen des EDSA lässt sich in der EU ein kohärenter Rechtsvollzug herbeiführen. Daher sollte auch die Zweckmäßigkeit von Maßnahmen, die durch die federführenden Behörden erlassen werden – nicht nur deren Rechtmäßigkeit innerhalb des aufsichtsbehördlichen Ermessensspielraums (Bußgeld, Anordnung oder Verwarnung) – durch die Entscheidung des EDSA der federführenden Behörde vorgegeben werden können.

Eine filigrane Nachsteuerung als „kleine Lösung“ der Defizite wird nicht mehr in Betracht kommen, wenn legislative Maßnahmen zu lange auf sich warten lassen. Wenn der Problemdruck der fehlenden Vollzugsgerechtigkeit zu groß geworden ist, dürfte nur noch eine umfassende Neustrukturierung der Datenschutzaufsicht in Europa als „große Lösung“ helfen. Eine zentrale europäische Datenschutzaufsichtsbehörde, die künftig den Platz von 27 einzelnen Behörden einnimmt und für den gesamten Bereich der grenzüberschreitenden Datenverarbeitung ausschließlich zuständig ist, könnte insoweit die angesprochen Defizite wirksam ausräumen.

Fazit

Die DSGVO steht in einem erheblichen Spannungsverhältnis zwischen weitreichenden rechtlichen Gewährleistungen für Betroffene und einer weitgehenden Paralyse der Aufsichtsbehörden im Vollzug, soweit es um die Umsetzung der Rechte und Freiheiten betroffener Personen gegenüber großen globalen Technologieunternehmen geht. Die Regelungen zu den aufsichtsbehördlichen Kompetenzen konstituieren im Datenschutz ein Europa der zwei Geschwindigkeiten: Während auf der einen Seite schnelle und effiziente Verfahren gegenüber nationalen Datenverarbeitern bestehen, funktioniert die diskursorientierte Version des Rechtsvollzugs bei der grenzüberschreitenden Datenverarbeitung nicht. Sie führt nicht nur zu erheblichen Rechtsschutzlücken betroffener Personen in Europa, sondern auch zu Verzerrungen des Wettbewerbs auf dem gemeinsamen Markt, gerade zu Lasten von einheimischen Unternehmen.

Die Ausgangsfrage, ob die DSGVO eine Mogelpackung ist, lässt sich somit wie folgt beantworten: Eine Mogelpackung ist sie nicht, soweit es um Schaffung von Rechten und Freiheiten Betroffener gegenüber verantwortlichen Stellen geht und soweit de-

ren nationale Wirksamkeit betrachtet wird. Auch wenn die Ausstattung der Behörden häufig nicht ausreichend ist und Unsicherheiten der Anwendung von unbestimmten Rechtsbegriffen auf alltägliche ökonomische Vorgänge bestehen, finden Rechtsgeltung und Rechtsvollzug im System des nationalen Datenschutzes mehr und mehr zueinander.

Soweit jedoch die grenzüberschreitende Datenverarbeitung betroffen ist, bleiben die fortschrittlichen, materiell-rechtlichen Gewährleistungen weitgehend ein Muster ohne Wert. Versteht man unter einer Mogelpackung eine äußere Hülle, die einen bestimmten Inhalt suggeriert, den sie tatsächlich nicht enthält, ist dies jedenfalls für die Durchsetzung der materiell-rechtlichen Standards durch die Ahndung und den Vollzug von Rechtsvorschriften der Fall. Hier bleibt vieles symbolisch. Dies gilt insbesondere für die hohen Bußgeldandrohungen gegenüber Unternehmen. Sie verfehlen ihren abschreckenden Charakter, wenn man ihre Anwendung nicht fürchten muss. Im Ergebnis sind dann auch all die Elogen und Sonntagsreden, die die DSGVO in einen rechtshistorischen Kontext – wie etwa mit der *Magna Charta* – setzen, nicht zutreffend und lenken von den massiven Defiziten im Rechtsvollzug ab.

Es ist eine zentrale Aufgabe der Datenschutzaufsichtsbehörden in Europa, der EU-Kommission, letztlich aber auch des Rats und des Europäischen Parlaments, die enorme Spanne zwischen Sein und Sollen im Datenschutz in der Datenschutzgrundverordnung zu schließen. Die Verzerrung zwischen Rechtsideal und Rechtswirklichkeit gefährdet das Projekt der DSGVO und bedroht die soziale Akzeptanz für den Datenschutz. Es muss sehr zügig gehandelt werden, damit künftig das Recht der Privatsphäre für alle Menschen in Europa nicht nur auf dem Papier steht, sondern auch eingelöst wird.

PROF. DR. JOHANNES CASPAR ist seit Mai 2009 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit. Der Jurist promovierte 1992 an der Universität Göttingen mit einer Dissertation über die Rechts- und Staatsphilosophie Jean-Jacques Rousseaus. Nach seiner Habilitation für die Fächer Staatsrecht, Verwaltungsrecht und Rechtsphilosophie 1999 folgte eine Tätigkeit am Deutschen Institut für Internationale Pädagogische Forschung in Frankfurt am Main. Von 2002 bis 2009 war er Referent und später Stellvertretender Leiter des Wissenschaftlichen Dienstes im Schleswig-Holsteinischen Landtag.

Anmerkungen:

1 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 (Datenschutz-Grundverordnung), ABl L 119 v. 4.5.2016.

2 So der damalige Bundesjustizminister Heiko Maas, zitiert in: https://www.online-zzi.de/archiv/ausgabe/artikel/zzi-2-2019/2290-so-schuetzen-sie-die-daten-ihrer-patienten/; Martini/Hohmann/Kolain, Digitale-Versorgung-Gesetz: Widerspruch nicht ganz ausgeschlossen, *netzpolitik.org* v. 3.12.2019, https://netzpolitik.org/2019/ein-bisschen-widerspruch-digitale-versorgung-gesundheitsdaten/; Strohm, Die Datenschutzgrundverordnung steht vor der Tür – 5. Speyerer Forum zur digitalen Lebenswelt, https://idw-online.de/de/news645360.

3 Zum Text der Magna Charta vom 15. Juli 1215 s. http://www.verfassungen.eu/gb/gb1215.htm.

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 v. 23.11.1995. S. 31–50.

5 Ausdrücklich heißt es in Art. 83 Abs. 1 DSGVO: „*Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.*“

6 Ausdrücklich reicht hier bereits die „*Gefahr einer politischen Einflussnahme*“, um gegen den europäischen Unabhängigkeitsbegriff zu verstoßen; vgl. Boehm, Art. 52, Rn. 11, in: Kühling/Buchner, DSGVO-Kommentar, 3. Auflage.

7 S. Art. 4 lit 22 DSGVO.

8 S. Evaluation des EDSA, S. 8, wobei die Gesamtzahl in der Addition nicht 807 Fälle, sondern 704 Fälle betrifft: European Data Protection Board, Contribution of the EDPB to the evaluation of the GDPR under Article 97 v. 18.2.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

9 Art. 60 Abs. 3 DSGVO bestimmt: „*Die federführende Aufsichtsbehörde übermittelt den anderen betroffenen Aufsichtsbehörden unverzüglich die zweckdienlichen Informationen zu der Angelegenheit. Sie legt den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vor und trägt deren Standpunkten gebührend Rechnung.*“

10 S. EDPB v. 18.2.2020 (Anm. 8).

11 S. Übersicht „*Geldbußen für DSGVO-Verstöße und für Verletzungen anderer Datenschutzgesetze*“ der Compliance Essentials GmbH unter https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php; der „*GDPR Enforcement Tracker*“ von CMS Legal Services EEIG (unter https://www.enforcementtracker.com/) geht hingegen lediglich von 418 Einträgen aus.

12 S. https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

13 S. https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

14 Hier ist auch die Regelung des Dringlichkeitsverfahrens in Art. 66 DSGVO nicht hilfreich, da es hohe Hürden setzt und nur eine beschränkte Anwendung ermöglicht; vgl. Caspar, Art. 66, Rn. 4 in: Kühling/Buchner, DSGVO-Kommentar, 3. Auflage.

15 Vgl. hierzu den *Irish Privacy Act*.

16 Dazu BGH, KVR 69/19 – Beschluss v. 23.6.2020, der den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook bestätigt, da die Datenverarbeitungspraxis von Facebook ohne wirksame Einwilligung das Recht der Nutzer auf informationelle Selbstbestimmung verletzt.

17 Hierzu die Bemerkung von P. Fleischer, dem *Global Privacy Counsel* von Google, der anlässlich der

Vorbereitungen auf das Inkrafttreten der DSGVO im Mai 2018 erklärte: „*Wir haben 500 Menschenjahre Arbeit in die Vorbereitung gesteckt*“ (zitiert nach: https://www.heise.de/-4049131); eine Investition, die viele kleinere Firmen sowie Start-Ups so nicht ansatzweise liefern können.

18 Insoweit instruktiv die Untersuchung von Peukert/Bechtold/Batikas/Kretschmer, European Privacy Law and Global Markets for Data (Working Paper). ETH Zürich, Juni 2020, S. 2, https://doi.org/10.3929/ethz-b-000406601.

19 Gem. Art. 97 Abs. 1 DSGVO war bis zum 25. Mai 2020 von der EU-Kommission ein Bericht über die Bewertung und Überprüfung dieser Verordnung vorzulegen.

20 Mitteilung der Kommission an das Europäische Parlament und den Rat, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, COM(2020)264 final vom 24.6.2020, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0264.

21 S. EDPB v. 18.2.2020 (Anm. 8), S. 4.