

Das Rechtsstaatsproblem der DSGVO

Dr. Lutz M. Keppeler / Thea Schenk-Busch, Köln*

Die Datenschutzgrundverordnung (DSGVO) sanktioniert in einem – jedenfalls in Rechtsstaaten – bislang noch nicht vorgekommenen Ausmaß den Verstoß gegen eine Vielzahl „generalklauselartig“ formulierter Vorgaben mit Millionenbußgeldern. Die DSGVO tritt an, um weite Teile der Verarbeitung personenbezogener Daten in Europa in nur 99 Artikeln einheitlich zu regeln. Die hierbei notwendige Abstraktionshöhe in der Formulierung der Vorgaben geht zu Lasten der Präzision. Obwohl sehr viele dieser Vorgaben bereits seit über 20 Jahren im nationalen Datenschutzrecht Bestand haben, erfolgte nur in einem sehr geringem Umfang eine Konkretisierung der vagen Vorschriften durch die Rechtsprechung. Das Rechtsstaatsprinzip aus Art. 20 Abs. 3, 103 Abs. 2 GG, Art. 49 Abs. 1 GRCh verlangt indes, dass Sanktionen nur im Fall von Verstößen gegen festumrissene Tatbestände verhängt werden dürfen. Je schwerwiegender die angedrohten Sanktionen, umso präziser muss der Bürger im Vorhinein anhand klarer gesetzlicher Vorgaben erkennen können, wo genau die Schwelle zu einem Verstoß überschritten wird. Der Beitrag soll zeigen, dass – gemessen an den bisherigen Maßstäben der Rechtsprechung – der überwiegende Teil der Bußgeldtatbestände der DSGVO vor einer weiteren Konkretisierung in der Rechtsprechung nicht als rechtsstaatskonform angesehen werden kann.

A. „Regelungsneutralität“ und Unbestimmtheit der Vorgaben der DSGVO

Die DSGVO¹ stellt den Rechtsanwender vor eine schwierige Aufgabe: Anstatt die Vielzahl der modernen Erscheinungen wie Industrie 4.0, Connected Car, Smarthome, Internet of Things, Social Media, Apps, Software as a Service usw. detailliert zu regeln, rühmt sich die DSGVO ihrer „Technikneutralität“.² Spezialregelungen des nationalen Rechts, wie etwa der Sonderdatenschutz im

Telemediengesetz³ oder der Smart-Meter-Datenschutz⁴ in dem neuen Messstellenbetriebsgesetz, werden von der DSGVO verdrängt. Mehrfach wurden die sich daraus ergebenden weiten Interpretationsspielräume der datenschutzrechtlichen Vorgaben deutlich kritisiert, wobei sich die Kritik bislang auf die Frage der Erlaubnistatbestände bezog.⁵ Da jedoch darüber hinaus auch zahlreiche weitere bußgeldbewehrte Verpflichtungen der DSGVO zu umfangreicher Rechtsunsicherheit führen, muss der Blick auf die gesamte DSGVO gelenkt werden.

Verständlicherweise war im langwierigen Gesetzgebungsverfahren die Regelung allzu vieler Details nicht möglich und zudem hat die Technikneutralität auch in der Hinsicht etwas Gutes, dass zukünftige Entwicklungen ebenfalls durch die Rechtsprechung adäquat behandelt werden können. Anstatt jedoch wie im BGB eine Vielzahl von Detailregelungen vorzugeben und wenige Generalklauseln gewissermaßen als „Backup“ zu verwenden, muss der DSGVO aufgrund der Vielzahl der vagen, unbestimmten und „generalklauselartig“ formulierten Rechtsbegriffe letztlich eine deutliche „Regelungsneutralität“ attestiert werden. Es entsteht der Eindruck, die Legislative habe bewusst die Kompetenz zur Regelung von Details in einem historisch einmaligen Maß an die Judikative delegiert. Und das in einem Rechtsgebiet, in dem – anders als bei den zivilrechtlichen Generalklauseln – keine traditionellen Auslegungsleitlinien seit der Antike zur Verfügung stehen.⁶

Freilich fehlt an dieser Stelle der Raum, um die Unbestimmtheit in ihrer ganzen Dimension auszubreiten.

* Dr. Lutz M. Keppeler ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht bei Heuking Kühn Lüer Wojtek in Köln. Thea Schenk-Busch ist wissenschaftliche Mitarbeiterin in dieser Sozietät.

¹ Die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ist ab dem 25.05.2018 anzuwenden.

² Die Technikneutralität wird in Erwägungsgrund 15 hervorgehoben. Dazu auch Pohl, PinG 2017, 85 (86), Schulz, in: Gola (Hrsg.), DSGVO, 2017, Art. 6 Rn. 5 und Roßnagel, DuD 2016, 561 (564 f.).

³ Siehe hierzu Keppeler, MMR 2015, 779 ff.; überblicksartig Holznapel, in: Hoeren/Sieber/Holznapel (Hrsg.), Multimedia-Recht, 45. EL Juli 2017, Teil 3 Rundfunk und Telemedien, Rn. 193 ff.; Schulz, in: Roßnagel (Hrsg.), Beck'scher Kommentar zum TMG, 2013, § 11 Rn. 1 ff.

⁴ Kritisch zu den Spielräumen des nationalen Gesetzgebers Keppeler, EnWZ 2016, 99 (104 f.).

⁵ Dazu etwa Pohl, (Fn. 2), (86); Nolde, PinG 2017, 114 (115); Bergt, CR 2016, 670 (670 f.); Roßnagel/Richter/Nebel, ZD 2013, 103 (104); dies., ZD 2015, 455 (460); Dahlke, ZD 2012, 353 (354); Traung, CRI 2012, 33 (41); Ziegenhorn/Heckel, NVwZ 2016, 1585 (1587); Reimer, in: Sydow (Hrsg.), EU-DSGVO, 2017, Art. 6 Rn. 88.

⁶ Siehe die Übersicht bei Haferkamp, in: Schmoeckel/Rückert/Zimmermann (Hrsg.), Historisch-kritischer Kommentar, Bd. 1, 2003, § 138 BGB S. 708–752 und § 242 (19. und 20. Jh.) Bd. 2, 2007, § 242 S. 274–364; Duve, in: Schmoeckel/Rückert/Zimmermann (Hrsg.), Historisch-kritischer Kommentar, Bd. 2, 2007, § 242 (Antike bis 18. Jh.), S. 274–364.

Insbesondere der Mangel an konkretisierender Rechtsprechung kann nur sehr punktuell erfolgen. Vor diesem Hintergrund konzentriert sich die folgende Darstellung ausschließlich auf Vorgaben, die nach Art. 83 DSGVO mit einem maximalen Bußgeld von bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes sanktioniert werden können.

I. Beispiel 1: Erlaubnistatbestände

Schon die elementarste Frage „Dürfen personenbezogene Daten im konkreten Einzelfall verarbeitet werden?“ lässt sich nur anhand von Wertungen und Abwägungen entscheiden. Es gilt das Verbot mit Erlaubnisvorbehalt, sodass personenbezogene Daten nur verarbeitet werden dürfen, wenn ein Erlaubnistatbestand dies gestattet. Da nahezu jede Aktivität in der vernetzten Informationsgesellschaft die Verarbeitung personenbezogener Daten beinhaltet, ist eine Vielzahl von – teils trivialen – Handlungen datenschutzrechtlich zu prüfen. Für die Vielfalt und Komplexität der modernen Datenverarbeitungsvorgänge hält die DSGVO lediglich sechs Erlaubnistatbestände in Art. 6 Abs. 1 DSGVO bereit,⁷ die dementsprechend abstrakt formuliert sind. So ist jede Verarbeitung personenbezogener Daten, die zur Durchführung eines Vertrages „erforderlich“ ist, auch datenschutzrechtlich erlaubt (Art. 6 Abs. 1 lit. b) DSGVO). Gleiches gilt für jede Verarbeitung für personenbezogene Daten, die für die Wahrung der „berechtigten Interessen“ des Datenverarbeiters erforderlich ist, solange die „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen nicht das berechnete Interesse des Konzerns überwiegen“ (Art. 6 Abs. 1 lit. f) DSGVO).

Diese vagen Vorgaben über das „berechnete Interesse“ entscheiden darüber, ob eine Videoüberwachung außerhalb des öffentlichen Raums,⁸ die Weitergabe von personenbezogenen Daten von einer Konzerngesellschaft zu einer anderen,⁹ das Speichern von IP-Adressen in Server-Logfiles,¹⁰ die Kommunikation zwischen Privat-

personen außerhalb des engen familiären Bereiches,¹¹ Bonitätsdatenbanken und Datenverarbeitungen durch Auskunftsteile,¹² Datenverarbeitungen im Inkassowesen,¹³ Datenverarbeitungen auf Webseiten und Apps,¹⁴ die Erhebung und Auswertung von Nutzerdaten für die Zwecke der IT-Sicherheit,¹⁵ der Umfang der Zulässigkeit von Personenbewertungsportalen im Internet,¹⁶ Datenverarbeitung durch Suchmaschinen¹⁷ und eine Vielzahl weiterer Aktivitäten¹⁸ rechtlich zulässig sind. Die genauen Grenzen sämtlicher angesprochenen und auch vieler weiterer Fragen können derzeit kaum benannt werden. Ein Überschreiten der Grenze kann mit einem Millionenbußgeld, insgesamt mit „Milliardenbußgeldern“,¹⁹ sanktioniert werden, die grundsätzlich gleichermaßen für die Organisation eines Handwerksbetriebs mit zwei Angestellten oder einem DAX-notierten Konzern sowie für Private gelten.²⁰

II. Beispiel 2: Compliance und Nachweispflichten

Einige mit Bußgeld bedrohte Tatbestände sind solche der Gefährdungshaftung. Sie beziehen sich auf Normen, die den Datenverarbeiter verpflichten, bestimmte organisatorische Maßnahmen – nämlich ein Datenschutz-Compliance-Management-System – zu treffen. Ein Verstoß gegen diese Verpflichtung ist – unabhängig davon, ob tatsächlich eine sonstige Vorgabe der DSGVO verletzt wurde – zumindest im Rahmen von Art. 25 und Art. 5 DSGVO bußgeldbewehrt. Der Wortlaut verlangt, dass diejenigen Compliance-Maßnahmen umgesetzt werden müssen, die „unter Berücksichtigung des Stands der Technik, [...] [und] der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere [der Datenschutzrisiken]“ angemessen sind (Art. 25 Abs. 1 DSGVO). Diese Berücksichtigung eines Angemessenheitsmaßstabs ist sehr hilfreich, da die Verarbeitung von personenbezogenen

⁷ Die Verarbeitung besonders sensibler Daten gemäß Art. 9 DSGVO und die spezifischeren Erlaubnistatbestände aus dem BDSG n. F. wurden hier zur Reduktion der Komplexität ausgeklammert. Gleiches gilt für möglichen weiteren Erlaubnistatbestände aus der zukünftigen e-Privacy-VO.

⁸ Siehe zum Diskussionsstand Schwartmann, in: Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DSGVO, 2018, Anhang „Videoüberwachung“ zu Art. 6 DSGVO, Rn. 16 zu „berechtigten Interessen“ nach § 6 BDSG n. F. und Rn. 21 ff. zur Rechtfertigung über Art. 6 Abs. 1 lit. f); Lachenmann, ZD 2017, 407 ff.

⁹ Moos/Zeiter, in: Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, 2. Aufl. 2017, Kap. 1 Rn. 4–11.

¹⁰ Diesbezüglich ist zumindest eine baldige Klärung in der Rechtsprechung zu erwarten, siehe BGH, CR 2017, 662 ff., mit Anm. Keppeler zur Bedeutung des zukünftigen Urteils des LG Berlin in dieser Sache.

¹¹ Siehe hierzu Reimer, in diesem Heft unter S. 11 („Wirkung für Private“). Gemäß Art. 2 Abs. 2 lit. c) DSGVO, werden zwar persönliche und familiäre Tätigkeiten vom Geltungsbereich der DSGVO ausgenommen, tendenziell wird diese „Ausnahme“ aber sehr eng ausgelegt. Vgl. hierzu Zerdick, in: Ehmann/Selmayr (Hrsg.), DSGVO, 2017, Art. 2 Rn. 10.

¹² Siehe Gola/Schulz, in: Gola, (Fn. 2), Art. 6 Rn. 127 ff.

¹³ Siehe Ziegenhorn/Gaub, PinG 2016, 89, (90 f.); Keppeler/Berning, ZFM 2018, 8 ff.; Gola/Schulz, in: Gola, (Fn. 2), Art. 6 Rn. 144 ff.

¹⁴ Wenngleich hierzu möglicherweise eine Klärung durch die e-Privacy-VO erfolgt.

¹⁵ Siehe Buchner/Petri, in: Kühling/Buchner (Hrsg.), DSGVO, 2017, Art. 6 Rn. 167 ff.

¹⁶ Siehe Buchner/Petri, (Fn. 15), Art. 6 Rn. 169 ff.

¹⁷ Siehe Buchner/Petri, (Fn. 15), Art. 6 Rn. 172 ff.

¹⁸ Siehe insbesondere die Fallgruppen in den umfangreichen Kommentierungen bei Gola/Schulz, in: Gola, (Fn. 2), Art. 6 Rn. 62 ff. und Buchner/Petri, (Fn. 15), Art. 6 Rn. 157 ff.

¹⁹ So der Aufsatztitel von Faust/Spitka/Wybitul, ZD 2016, 120 ff.: „Milliardenbußgelder nach der DSGVO?“

²⁰ Zu diesem Themenkomplex auch Reimer, in diesem Heft unter S. 11 („Wirkung für Private“).

Daten etwa in einem herkömmlichen Friseurbetrieb nur ganz geringe Risiken mit sich bringt. Leider ist weder ein Kommentator noch ein Rechtsanwalt in der Lage, präzise abzuleiten, ab welcher exakten Schwelle unter Berücksichtigung des Stands der Technik usw. im Einzelfall eine technische und organisatorische Maßnahme angemessen gewesen wäre. Die vorzunehmende persönliche Wertung wird durch Richter gefällt und hoffentlich gut begründet. Welches Maß an Datenschutz-Compliance ist angemessen? Dies ist ebenso unklar, wie die Frage, welches das angemessene Maß an IT-Sicherheit darstellt (Art. 32 DSGVO) und ab wann ein hohes Risiko im Rahmen einer Datenschutzfolgeabschätzung anzunehmen ist (Art. 35 DSGVO). Dürfen Anwälte in der Zukunft nur verschlüsselte E-Mail-Kommunikation verwenden und setzt man sich bereits dem Risiko eines Millionenbußgeldes aus, wenn man auf signaturbewährte Verschlüsselungsmethoden wie PGP in der Praxis verzichtet?²¹

III. Beispiel 3: Grundsätze für die Verarbeitung personenbezogener Daten

Noch abstrakter sind in Art. 5 DSGVO die Grundsätze für die Verarbeitung von personenbezogenen Daten bezeichnet.²² Hier werden basale Regeln wie beispielsweise das Prinzip der Datenminimierung und der Zweckbindung oder der Rechtmäßigkeit der Verarbeitung in einem sehr hohen Abstraktionsgrad festgeschrieben. Die Vorgabe des Prinzips der Datenminimierung liest sich etwa so: „Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).“ Nun hielt es der europäische Gesetzgeber nicht nur für klug, jeden Verstoß gegen Grundsätze aus Art. 5 DSGVO mit einem Maximalbußgeld zu bedrohen, sondern zusätzlich eine klare Beweislastumkehr in Art. 5 Abs. 2 DSGVO zu normieren.²³ Jedes Unternehmen – vom Handwerksbetrieb bis zum DAX-Konzern – muss also für sämtliche Datenverarbeitungsvorgänge nachweisen können, dass das Prinzip der Datenminimierung und weitere Prinzipien eingehalten wurden. Wann genau die abstrakten Prinzipien aus Art. 5 DSGVO in Grenzfällen als erfüllt angesehen werden, kann – Stand heute – niemand voraussehen.

IV. Umgang mit diesem Problem

Die Beispiele könnten noch lange fortgeführt werden. Beispielhaft formuliert das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), wie auch die Behörden im Hinblick auf die DSGVO „in der Luft hängen“: „*Wie die Anforderungen des Art. 17 Abs. 1 DSGVO in der Pra-*

xis durch die Verantwortlichen umzusetzen sind, lässt sich der DSGVO nicht ohne Weiteres entnehmen.“²⁴

Freilich sind die Exegeten schon fleißig bemüht, in den zahlreichen nun erscheinenden Kommentaren kluge Hinweise zur Auslegung zu geben. Der deutsche Rechtsanwender, der lange vor der Anwendbarkeit der DSGVO über ein Dutzend Kommentare in seinem Rücken wusste,²⁵ fragt sich, wie sich Unternehmen in anderen EU-Ländern, die zum Teil noch keinen einzigen landessprachigen Kommentar aufweisen können, auf die DSGVO vorbereiten (während man sich außerhalb von Deutschland – zu Recht – fragt, wer das alles lesen soll). Zudem veröffentlichen Datenschutzaufsichtsbehörden Papiere über ihre Auslegung der DSGVO, teilweise auch abgestimmt über die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder („DSK“). Doch genügen diese – nicht rechtsverbindliche Aussagen –, um dem europäischen Gesetzgeber zu gestatten, im Angesicht des Rechtsstaatsprinzips hohe Bußgelder für derart unbestimmte Vorgaben anzudrohen? Die Frage könnte allenfalls dann bejaht werden, wenn bereits viele Zweifelsfragen durch die Rechtsprechung geklärt und Fallgruppen gebildet worden wären. Das ist leider nicht der Fall.

B. Geringe Rechtsprechungsdichte im Datenschutzrecht

Wie weist man eine geringe „Rechtsprechungsdichte“ und eine daraus folgende geringe gerichtliche „Klärungsreichweite“ eines Rechtsgebiets nach, zumal methodische und theoretische Grundlagen zu dieser Frage – soweit ersichtlich – nicht zur Verfügung stehen? Was wäre eine zu erwartende Datenschutz-Prozessrate²⁶ und wie misst man die Klärungswirkung einer Entscheidung? In den folgenden Zeilen kann nur eine Annäherung erfolgen, die den Anspruch erhebt, eine deutliche Tendenz aufzuzeigen, ohne erschöpfend sein zu wollen.

²⁴ Das weitere Zitat lautet: „Umso wichtiger ist es, dass der europäische Datenschutzausschuss so schnell wie möglich Leitlinien, Empfehlungen und bewehrte Verfahren zum Art. 17 DSGVO bereitstellt. Dies hilft nicht nur den Verantwortlichen, sondern ist auch für die Aufsichtsbehörde entscheidend – denn diese haben künftig die Befugnis, die Vorgaben des Art. 17 durchzusetzen.“ Kurzpapier IV. des BayLDA https://www.la.bayern.de/media/baylda_ds-gvo_4_right_to_be_forgotten.pdf, S. 2 a. E. (Abruf vom 22.12.2017).

²⁵ Z. B. Plath, DSGVO, 2. Aufl. 2016; Paal/Pauly, DSGVO, 2017; Wolff/Brink, BeckOK DSGVO, 2017; Gola, DSGVO, 2017; Kühling/Buchner, DSGVO, 2017; Ehmann/Selmayr, DSGVO, 2017 und aktuell Gierschmann/Schlender/Stentzel/Veil (Hrsg.), DSGVO, 2018; Eßer/Kramer/von Lewinski, DSGVO/BDSG, 5. Aufl. 2017; Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht mit DSGVO und BDSG, 2018; Sydow (Hrsg.), EU-DSGVO, 2017; Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), DSGVO, 2018; Däubler/Wedde/Weichert/Sommer (Hrsg.), EU-DSGVO/BDSG, 2018; Taeger/Gabel (Hrsg.), DSGVO/BDSG, 2018.

²⁶ In Anlehnung an die „Zivilprozessrate“, siehe hierzu zuletzt Wolf, NJW 2015, 1656 (1657).

²¹ Dies scheint sich aus dem 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten (01.04.2015–31.03.2017) S. 138 f. zu ergeben.

²² *Bülte*, StV 2017, 460 (465).

²³ *Pötters*, in: Gola, (Fn. 2), Art. 5 Rn. 34.

I. Keine vergleichbare Rechtsprechungsdichte im Datenschutzrecht

Es gehört zum eigentümlichen Wesenszug des Datenschutzrechts, dass klärende Rechtsprechung – zumal obergerichtliche – Seltenheitswert hat. Das zeigt schon ein Blick auf die bisherigen datenschutzrechtlichen Ordnungswidrigkeitstatbestände.²⁷ Auf das erste Urteil, welches im Rahmen des Streits um ein Bußgeld nach § 43 BDSG Fragen des Datenschutzrechts klärt, musste sehr lange gewartet werden. Zwischen 2001²⁸ und 2016 ist kein solches Urteil in der Datenbank juris verzeichnet. Für das Jahr 2017 finden sich allerdings gleich vier Urteile, wobei sich drei von diesen mit sogenannten „Dash-Cams“ beschäftigen.²⁹ Ehmann, der die bisherige Bußgeldpraxis umfassend dargestellt hat, kann ebenfalls nur Presseerklärungen zu Tätigkeitsbericht von Datenschutzaufsichtsbehörden heranziehen.³⁰ Er vermutet, dass in größeren Fällen eher ein „Deal“ verhandelt wird, als dass sich die Parteien auf das Glatteis eines Gerichtsverfahrens einlassen.³¹ Befindet man sich hier in einer den Rechtsstaat weiter schwächenden Abwärtsspirale? Weil der Ausgang eines Datenschutzbußgeldverfahrens – mangels Praxis hierzu – nicht vorherzusehen ist, lässt man es lieber nicht darauf ankommen (und verfestigt somit die Unsicherheit)?

Auch wenn es nicht um Bußgelder ging, sondern nur um die Zulässigkeit einer Datenverarbeitung, finden sich verhältnismäßig wenige Urteile. Für ganz wesentliche Normen – wie etwa § 28 Abs. 1 Nr. 1 BDSG, der als „datenschutzrechtliche Generalklausel“ die Datenerhebung und -speicherung für eigene Geschäftszwecke im Rahmen eines Vertragsverhältnisses erlaubt, – findet sich nur eine äußerst dürftige Ausbeute an klärender Rechtsprechung. Nominell nennt juris zwar „34 Treffer“, jedoch erwähnen die meisten gefundene Urteile § 28 Abs. 1 Nr. 1 BDSG nur am Rande, ohne den zentralen Begriff der „Erforderlichkeit“ zu konkretisieren. Maßgebliche Kommentare zum BDSG erwähnen zur Interpretation der „Erforderlichkeit“ im Rahmen von § 28 Abs. 1 Nr.

1 BDSG lediglich vier³² bzw. drei³³ Urteile, die jeweils bei genauerer Betrachtung die Auslegung von § 28 Abs. 1 Nr. 1 BDSG nur sehr mittelbar betreffen. Auch außerhalb der Standard-Kommentare findet sich nur äußerst wenig Rechtsprechung zu diesem Thema.³⁴

II. Höchststrichterliche Urteile typischerweise durch „Einzelkämpfer“ erwirkt

Auffallend ist auch, dass die wenigen wegweisenden Entscheidungen der letzten Jahre ausschließlich aufgrund der Tätigkeit von Einzelkämpfern vor Gericht (und dann in der Regel auch vor den EuGH) gelangt sind: Ohne den Datenschutzaktivisten Maximilian Schrems gäbe es kein EuGH-Urteil zum Safe-Harbor-Abkommen,³⁵ ohne den spanischen Anwalt Mario Costeja González kein EuGH-Urteil zum Recht auf Vergessen³⁶ und ohne den Piratenpolitiker Patrick Breier kein EuGH-Urteil zu IP-Adressen.³⁷ Das alles ist nicht Ausdruck einer breiten Masse an Bürgern, die es genau mit dem Datenschutz wissen will. Weder „Abmahnanwälte“ noch Datenschutzaufsichts- oder Verbraucherschutzbehörden können als massive Treiber der gerichtlichen Verfolgung von Datenschutzverstößen benannt werden.

III. Vergleich der Rechtsprechungsdichte zwischen § 7 UWG und §§ 4a, 28 Abs. 3 und 4 BDSG

Das Ausmaß der fehlenden datenschutzrechtlichen Rechtsprechung kann auch anhand des Vergleichs der Rechtsprechungsdichte zu § 7 Abs. 2 und Abs. 3 UWG einerseits und §§ 4a, 28 Abs. 3 und 4 BDSG andererseits deutlich gemacht werden. Beide Normen regeln das Direktmarketing – also die direkte werbliche Ansprache ei-

²⁷ Die ebenfalls spärlich gesäten Urteile zu datenschutzrechtlichen Ordnungswidrigkeitstatbeständen außerhalb des BDSG (etwa § 16 TMG, § 85 SGB X oder § 149 TKG) bleiben vorliegend außer Betracht, da diese kaum zur Konkretisierung der DSGVO beitragen können.

²⁸ Zuvor gab es keine Bußgeldnorm gegenüber privaten Stellen; siehe Ehmann, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 43 Rn. 79.

²⁹ OLG Celle, Urt. v. 04.10.2017 – 3 Ss (OWi) 163/17 und das vorangehende Urt. des AG Hannover v. 10.04.2017 – 265 OWi 7752 Js 14214/17; zudem AG München, Urt. v. 09.08.2017 – 1112 OWi 300 Js 121012/17.

³⁰ Ehmann, (Fn. 28), § 43 Rn. 82 ff.

³¹ Ehmann, (Fn. 28), § 43 Rn. 85 f.

³² Gola/Klug/Körffler, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 28 Rn. 14–23 nennen nur vier Urteile, welche § 28 Abs. 1 Nr. 1 BDSG interpretieren, nämlich OLG Köln, CR 2011, 680 ff. (welches sich zumindest mit der „Erforderlichkeit“ im Sinne des § 28 Abs. 1 S. 1 Nr. 2 BDSG beschäftigt); BAG, RDV 1987, 129 ff. (zu einer anders lautenden Vorgängervorschrift aus dem Arbeitsrecht) und AG Rendsburg, WUM 1990, 507 ff.; LG Itzehoe, RDV 2008, 210 ff. (jeweils zu einer ausschließlich anhand des BGB geklärten Frage der Auskunftspflicht eines Mieters).

³³ Simitis, (Fn. 28), § 28, Rn. 56–97 zitiert drei Urteile: BGHZ 95, 362 (364 f.) zur AGB-Prüfung einer Schufa-Klausel; BVerwG, NJW 1987, 1657 zum Verbot der Zusammenführung von Personalakten im öffentlich-rechtlichen Bereich und OLG Düsseldorf, NJW-RR 1990, 372 f. zur datenschutzrechtlichen Zulässigkeit der Weitergabe von Informationen durch einen Makler nach Beendigung des Maklervertrages.

³⁴ OLG Köln, Beschl. v. 17.11.2010 – 18 U 149/10 –, juris, Leitsatz 4; LG Köln, Urt. v. 09.05.2007 – 26 O 358/05 –, juris, Rn. 31; OLG Celle, WM 2004, 1384 ff., Leitsatz 2.

³⁵ EuGH, Urt. v. 06.10.2015, C-362/14 – Safe Harbor.

³⁶ EuGH, Urt. v. 13.05.2014, C-131/12 – Recht auf Vergessen.

³⁷ EuGH, Urt. v. 19.10.2016, C-582/14 – Personenbezug bei dynamischen IP-Adressen.

nes potentiellen Kunden, wie etwa die Zusendung einer Werbe-E-Mail. § 7 UWG regelt die wettbewerbsrechtliche Zulässigkeit der Frage, das BDSG regelt die datenschutzrechtliche Zulässigkeit des identischen Lebenssachverhalts. Somit besteht immerhin eine Konstante, die einen Vergleich – trotz aller methodischen Bedenken – möglich macht.

Dabei ging das UWG grundsätzlich den Weg von einer Generalklausel im UWG von 1909 hin zu einer ausdifferenzierten Spezialregelung seit der UWG-Reform von 2004.³⁸ Gewissermaßen wurde also der umgekehrte Weg beschritten: Während das ausdifferenzierte nationale Datenschutzrecht den allgemeinen und abstrakten Regelungen der DSGVO auf Geheiß der EU weichen muss, differenzierten sich die Regeln des UWG auf Basis der Harmonisierung weiter aus. Das UWG von 1909 regelte das Wettbewerbsrecht in einer bis zum 07.07.2004 geltenden Zentralnorm, die sich auf „die guten Sitten“ stützte.³⁹ Anhand dieser Generalklausel entwickelte der BGH seit den 1970er Jahren Vorgaben zu Einwilligungserklärungen von Werbeanrufern.⁴⁰ Das BDSG spielte in diesen wegweisenden Entscheidungen des BGH zunächst gar keine und dann später eine sehr untergeordnete Rolle.⁴¹ Vor dem BGH stand stets die wettbewerbsrechtliche Zulässigkeit im Vordergrund: Konnte diese anhand von § 7 UWG eindeutig verneint werden, spielte das BDSG eine klare Nebenrolle. Auch deshalb entschied sich der deutsche Gesetzgeber dazu, die Vorgaben der sogenannten e-Privacy-Richtlinie (RL 2002/58/EG)⁴² zu Werbeanrufern und Werbe-E-Mails im Rahmen der Reform des UWGs von 2004 in § 7 UWG – und damit nicht im BDSG – umzusetzen, was keineswegs zwingend war.⁴³ Dies führt dazu, dass die Kommentierung zur Werbeeinwilligung in BDSG-Kommentaren klar durch die Rechtsprechung zu § 7 UWG dominiert wird. Trivial aber aussagekräftig ist auch die in juris vorhandene Rechtsprechung: Zu § 7 Abs. 2 UWG erscheinen 299 Urteile für den Zeitraum von 2004 bis Januar 2018, zu § 4a BDSG, der allgemeinen Regel zur Einwilligung – also einer Norm mit weitaus größerem Anwendungsbereich im Vergleich zu § 7 UWG –, sind für den Zeitraum von 1990 bis Januar 2018 nur 88 Urteile verzeichnet. Von diesen 88 Urteilen beschäf-

tigen sich wiederum die meisten primär mit § 7 Abs. 2 UWG.⁴⁴ Kein einziges dieser Verfahren zog eine Streitigkeit um ein datenschutzrechtliches Bußgeld nach sich. Dies zeigt, wie gering die Rechtsverfolgungsintensität im Datenschutzrecht im Vergleich zu anderen Rechtsgebieten ist. Eine gefestigte Rechtsprechung zum Thema der Werbeeinwilligungen verdanken wir zu einem ganz hohen Anteil der intensiven Rechtsverfolgung durch Wettbewerber und Verbraucherschutzzentralen über § 7 Abs. 2 UWG. Dies macht zugleich deutlich, wie gering die Anzahl der Urteile zu allen anderen Fragen des bisherigen Datenschutzrechts und der DSGVO ist.

IV. Bisherige Rechtsverfolgungspraxis des Datenschutzrechts in Deutschland

Hintergrund der geringen Rechtsverfolgung, die als Hauptverursacher der geringen Rechtsprechungsdichte genannt werden kann, ist auch die Personalausstattung: Nur wenige Vollzeitstellen waren bislang in Bund und Ländern dem Datenschutz und dessen Aufsicht gewidmet. So beschäftigen sich beispielsweise im Saarland gerade einmal 12,5 Vollzeitkräfte mit der Datenschutzaufsicht.⁴⁵ In diesem Kontext steht die Stellungnahme des baden-württembergischen Innenministeriums, wonach es „[e]ntgegen einer weit verbreiteten Auffassung [...] nicht primäres Ziel einer datenschutzrechtlichen Überprüfung [sei], im Falle eines Datenschutzverstößes ein Bußgeld [...] zu verhängen.“⁴⁶ Im Zeitraum von September 2005 bis August 2006 ergingen bundesweit lediglich 44 Bußgeldbescheide; der Jahreschnitt pro Bundesland lag bei 2,75 Bußgeldbescheiden.⁴⁷ Auf europäischer Ebene sind im Rahmen des bis 2015 geltenden Safe-Harbor-Abkommens mit den USA nahezu lächerliche Bußgelder gegen Ponica (9.000 €), Adobe (8.000 €) und Unilever (11.000 €) verhängt worden.⁴⁸ Die Großwetterlage der Verfolgung des Datenschutzrechts in Deutschland war also nicht auf Rechtsstreitigkeiten aus. Wurden Bußgelder erlassen, so waren diese häufig so gering, dass der anwaltliche Rat nur lauten konnte, die Bußgeldbescheide zu akzeptieren oder Gerichtsurteile frühzeitig durch einen Vergleich zu vermeiden.⁴⁹

³⁸ Siehe hierzu etwa *Henning-Bodewig*, GRUR 2004, 713 ff.

³⁹ § 1 UWG vom 07.07.1909 (RGBl. S. 499) lautet vollständig: „Wer im geschäftlichen Verkehr zu Zwecken des Wettbewerbes Handlungen vornimmt, die gegen die guten Sitten verstoßen, kann auf Unterlassung und Schadensersatz in Anspruch genommen werden.“

⁴⁰ BGHZ 54, 188 (191) – Telefonwerbung I; *BGH*, GRUR 1989, 753 (754) – Telefonwerbung II; *BGH*, GRUR 1990, 280 (281) – Telefonwerbung III; BGHZ 113, 282 (286) = GRUR 1991, 764 (765) – Telefonwerbung IV; *BGH*, GRUR 1995, 220 (221) – Telefonwerbung V; *BGH*, GRUR 2000, 818 (820) – Telefonwerbung VI.

⁴¹ Bspw. *LG Bonn*, Urt. v. 31.10.2006 – 11 O 66/06.

⁴² Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.06.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

⁴³ Kritisch hierzu *Köhler*, in: *Köhler/Bornkamm/Feddersen*, UWG, 36. Aufl. 2018, § 7 Rn. 124a–124c.

⁴⁴ Stand: 01.02.2018.

⁴⁵ *Ehmann*, (Fn. 28), § 43 Rn. 82 ff., *Holländer*, RDV 2009, 215 ff. m.w.N. und *Lüdemann/Wenzel*, RDV 2015, 285 (287 ff.).

⁴⁶ Fünfter Tätigkeitsbericht des Innenministeriums Baden-Württemberg nach § 39 des Landesdatenschutzgesetzes 2009, <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/5.-T%C3%A4tigkeitsbericht-des-Innenministeriums-2009.pdf>, S. 6 (Abruf vom 22.12.2017).

⁴⁷ *Holländer*, (Fn. 45), 215 ff.

⁴⁸ Pressemitteilung vom 06.06.2016: https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-dateneuebermittlungen-in-die-usa.html?tx_ttnews%5BbackPid%5D=170&cHash=d-21026cc72d2a53525c7c40d6c6baa6e2 (Abruf vom 07.02.2017).

⁴⁹ Eine Ausnahme dazu stellte das Bußgeld gegen Verkäufer und Käufer eines Unternehmens wegen Verstoßes gegen die datenschutzrechtlichen Vorschriften im Umgang mit Kundendaten dar, das das BayLDA verhängte. Dazu die Pressemitteilung vom 30.07.2015: https://www.lida.bayern.de/media/pm2015_10.pdf (Abruf vom 28.12.2017).

V. Weitere Gründe für bislang nicht ausreichende dogmatische Durchdringung des Datenschutzrechts

Das Datenschutzrecht weist mithin eine Reihe von Besonderheiten auf.⁵⁰ Dazu gehört etwa auch, dass – im Vergleich zu herkömmlichen juristischen Themen – eine hohe Anzahl von quereinsteigenden technisch- und/oder naturwissenschaftlich ausgebildeten Autoren das Fach begleitet. Zudem sind in der Praxis viele betriebliche Datenschutzbeauftragte nicht juristisch, sondern technisch ausgebildet. Auch Universitätslehrstühle und Forschungsinstitute, die auf das Datenschutzrecht spezialisiert sind, gibt es relativ wenig, was dazu führt, dass die Anzahl an Lehrveranstaltungen zum Datenschutzrecht sehr niedrig ist. Dementsprechend sind „Anfängerlehrbücher“ oder gar „Fallbücher“, die datenschutzrechtliche Praxisfälle im Gutachtenstil durchdeklinieren, spärlich zu finden.⁵¹ Demgegenüber werden in großer Zahl außeruniversitäre Praxisausbildungslehrgänge für Datenschutzbeauftragte angeboten, die schließlich auch bislang nach § 4f Abs. 2 BDSG über eine ausreichende Fachkunde verfügen mussten. Die Gesamttekonik der datenschutzrechtlichen Ausbildung und Literaturproduktion wird sich im Zuge der gewachsenen Bedeutung des Datenschutzrechts in Zukunft vermutlich auf die Universität verlagern.

Diese Analyse basiert freilich auf Praxiserfahrungen und damit weder auf empirischen Untersuchungen noch auf einer rechtstheoretischen Durchdringung der spezifischen Phänomene, die das Datenschutzrecht bis dato kennzeichnen. Eine entsprechend tiefere Beschäftigung mit dieser Perspektive und damit mit den Eigengesetzlichkeiten des sozialen Systems „Datenschutzrecht“ muss daher als Desiderat bezeichnet werden. Es wäre zweifelsohne wertvoll gewesen, wenn eine Beschreibung der inneren Operationen des Systems bereits vorgelegen hätte, als man begann, sich mit der EU-Kommission über die DSGVO Gedanken zu machen. Die Darstellung sollte hier nur andeuten, dass die im Falle von unklaren gesetzlichen Regelungen erwartbaren Operationen zur Klärung einer Rechtslage (Rechtsverfolgung, Rechtsprechung, Forschung und Lehre, behördliche Tätigkeit) im Datenschutzrecht nur in sehr geringen Umfang ausgeprägt waren (im Verhältnis zur Bedeutung des Schutzes personenbezogener Daten in einer Informationsgesellschaft und im Vergleich zu anderen Rechtsgebieten).

C. Rechtsstaatliche Problematik der Generalklauseln

Generalklauseln stellen ein hilfreiches und altbewährtes Regelungsinstrument des Gesetzgebers dar. Indes sind sie im Hinblick auf das Rechtsstaatsprinzip und damit

insbesondere in Zusammenhang mit dem Bestimmtheitsgebot nicht unbedenklich, sondern gewissermaßen „mit Vorsicht zu genießen“.

I. Anforderungen aus dem Rechtsstaatsprinzip

Das Bestimmtheitsgebot wird aus dem Rechtsstaatsprinzip⁵² abgeleitet und fordert, dass jede Norm eindeutig und bestimmt sein muss, sodass es dem Bürger möglich ist, sein Verhalten der Norm entsprechend auszurichten.⁵³ Aus europäischer Sicht stellt das Gebot der Bestimmtheit von Normen einen höherrangigen Rechtssatz dar, der den Maßstab für sekundäre Rechtsakte der EU bildet.⁵⁴

Vor dem besonderen Hintergrund von Normen, die sanktionsbewehrt sind, statuiert Art. 103 Abs. 2 GG das strafrechtliche Gesetzlichkeitsprinzip als Justizgrundrecht in der deutschen Verfassung; Art. 49 Abs. 1 GRCh stellt auf europäischer Ebene eine parallele Regelung dar.⁵⁵ Zum einen bietet das strafrechtliche Gesetzlichkeitsprinzip individuellen Schutz für das Individuum,⁵⁶ zum anderen gebietet es dem Gesetzgeber, in generell-abstrakter Weise über die Strafbarkeit eines Verhaltens zu bestimmen.⁵⁷ Ausprägung des strafrechtlichen Gesetzlichkeitsprinzips ist der spezielle Grundsatz der Bestimmtheit von Strafnormen „nulla poena sine lege certa“. Dabei ist Art. 103 Abs. 2 GG sowohl auf strafrechtliche Sanktionen als auch auf Sanktionen im Bereich des Ordnungswidrigkeitenrechts anwendbar.⁵⁸

Der Grundsatz nulla poena sine lege certa bedeutet für die Exekutive und die Judikative einerseits, dass Sanktionen aufgrund eines unbestimmten Gesetzes nicht verhängt werden dürfen.⁵⁹ Für die Legislative bedeutet er andererseits, dass diese bei der Ausgestaltung von Straf- und Bußgeldnormen die Tatbestände so formulieren muss, dass sich aus dem Wortlaut – oder jedenfalls mithilfe der üblichen Auslegungsmethoden – die Voraussetzung für den Anwendungsbereich der Sanktionen ergibt, sodass

⁵² Nach dem EuGH wird das Bestimmtheitsgebot aus dem Prinzip der Rechtssicherheit abgeleitet: *EuGH*, Urt. v. 12.12.1996, C-74/95 und C-129/95 – Strafverfahren gegen X, Rn. 25.

⁵³ BVerfGE 13, 153 (160 f.); 48, 210 (222); 78, 205 (226); 79, 106 (120); *Greszick*, in: Maunz/Dürig (Hrsg.), GG, 81. EL September 2017, Art. 20 Rn. 58.

⁵⁴ *EuG*, Urt. v. 27.09.2006, T-43/02, Rn. 40 m.w.N.

⁵⁵ Ferner sind die strafrechtlichen Garantien in Art. 7 Abs. 1 EMRK verankert und gemäß Art. 6 Abs. 3 EUV als allgemeiner Grundsatz Teil des Unionsrechts. Dass das Bestimmtheitsgebot im Rahmen von sanktionsbewehrten Normen eine besondere Ausprägung erfährt, ist zudem den Verfassungstraditionen der EU-Mitgliedstaaten gemein und stellt damit eine gemeinsame Verfassungstradition dar, die als allgemeiner Grundsatz des Gemeinschaftsrechts gemäß Art. 6 Abs. 3 EUV zu beachten ist. Siehe *Soltész/Steinle/Bielez*, *EuZW* 2003, 202 (205).

⁵⁶ So BVerfGE 75, 329 (341) m.w.N.; *BVerfG*, Beschl. v. 23.06.2010 – 2 BvR 2559-08, Rn. 71.

⁵⁷ So BVerfGE 75, 329 (341) m.w.N.; *BVerfG*, Beschl. v. 23.06.2010 – 2 BvR 2559-08, Rn. 70.

⁵⁸ Vgl. BVerfGE 38, 348 (371 f.); 71, 108 (114); 81, 132 ff.; 87, 399 ff.

⁵⁹ *Remmert*, in: Maunz/Dürig, (Fn. 53), Art. 103 Rn. 1.

⁵⁰ Siehe hierzu auch jüngst *Schmidt-Jortzig*, *DÖV* 2018, 10 ff.

⁵¹ Eine rühmliche Ausnahme bildet das Werk: Gola/Reif, *Praxisfälle Datenschutzrecht*, 2. Aufl. 2016.

jedermann voraussehen kann, welches Verhalten sanktioniert wird.⁶⁰ Ferner ist Voraussetzung, dass die Strafandrohung als solche ebenso bestimmt sein muss.⁶¹ Fehlende Genauigkeit im Gesetz kann hierbei grundsätzlich durch Rechtsprechung ausgeglichen werden.⁶²

II. Anwendbarkeit des Bestimmtheitsgebots auf die Sanktionsvorschriften der DSGVO

Ein Aspekt des Bestimmtheitsgebots ist, dass die Norm „umso präziser bestimm[t] [sein muss,] je schwerer die angedrohte Strafe ist.“⁶³ Im Hinblick auf den Charakter und die Natur der Norm, die eine stark belastende finanzielle Konsequenz befürchten lässt – erinnert sei an den Maximalbußgeldrahmen von bis zu 20 Mio. € oder 4 % des Jahresumsatzes –, ist die Anwendbarkeit des strafrechtlichen Bestimmtheitsgrundsatzes zwingend geboten.⁶⁴

III. Entsprechen die Sanktionsnormen der DSGVO dem strafrechtlichen Bestimmtheitsgebot?

Art. 83 DSGVO verweist auf die Normen der DSGVO, deren Verletzung mit erheblichen Geldbußen sanktioniert wird. Diese Tatbestände sind – anlehnend an die obigen Erläuterungen – weder bestimmt gefasst noch durch bewährte Leitlinien, Stellungnahmen oder gar Rechtsprechung konkretisiert worden.⁶⁵ Zwar ist eine Norm nicht schon deshalb unbestimmt, weil der Betroffene fachkundigen Rechtsrat einholen muss, um sein Verhalten entsprechend zu disponieren,⁶⁶ doch sieht sich der Rechtsanwender – sei es der Anwalt, der Richter, die Verwaltungsbehörde oder das Individuum selbst – erheblichen „Bewertungsproblemen“⁶⁷ und Zweifeln ausgesetzt, die bis zu den ersten Gerichtsentscheidungen nicht aus dem Weg geräumt werden können.⁶⁸ Die bußgeldbewehrten Normen der DSGVO greifen aufgrund ihrer Unbestimmtheit in das dem Individuum zugesicherte Schutzrecht der Bestimmtheit von Rechtsnormen ein. Im Hinblick auf Unternehmen, die Daten verarbeiten,

stellt die Unbestimmtheit der Rechtsnormen zudem einen Eingriff in die Planungssicherheit dar, da die datenverarbeitenden Unternehmen ihr unternehmerisches Handeln schwerlich entsprechend den Vorgaben der DSGVO ausrichten können.

IV. Vergleich mit Kartellrecht

Ein Vergleich mit einem ähnlich gelagerten Problem im Kartellrecht soll helfen, dass datenschutzrechtliche Problem praxisnaher darzustellen und zu verstehen: Art. 23 der Kartellverfahrensverordnung (VO 1/2003) sanktioniert Kartellrechtsverstöße mit Geldbußen. Nach Art. 23 Abs. 2 VO 1/2003 kann einem Unternehmen beispielsweise für eine Zuwiderhandlung durch die Kommission eine Geldbuße von bis zu 10 % des im vorausgegangenen Geschäftsjahres erzielten Gesamtumsatzes auferlegt werden. Zwar normiert Art. 23 Abs. 3 VO 1/2003, dass die Schwere und die Dauer der Zuwiderhandlung zu berücksichtigen sind, indes werden keine weiteren Kriterien für die Bestimmung der Geldbuße genannt und die Berechnung somit größtenteils ins Ermessen der Kommission gestellt.⁶⁹ Zudem waren und sind die kartellrechtlichen Tatbestände, insbesondere etwa in § 1 GWB oder auf europäischer Ebene in ihrer Fassung von Art. 101 f. AEUV und ihren früheren Fassungen sehr abstrakt und generell formuliert.⁷⁰ Trotzdem hat der EuGH die Norm für ausreichend bestimmt erachtet und entgegnet der Kritik damit, dass das Ermessen der Kommission durch ausreichend objektive Kriterien⁷¹ beschränkt sei und ferner den Zweck verfolge, wettbewerbspolitisch flexibel zu handeln.⁷² Im Gegensatz zum Datenschutzrecht bestanden und bestehen im Kartellrecht indes (ausreichende oder besser gesagt: wenigstens) Konkretisierungen der Rechtsmaterie durch Rechtsprechung und Verwaltungspraxis, sodass die Adressaten des Kartellverbots ihre Rechte und Pflichten erkennen konnten und können.⁷³

Soweit im Hinblick auf die Anwendbarkeit des Grundsatzes „nulla poena sine lege certa“ auf Bußgelder nach der DSGVO jüngst ein Urteil des EuG vom 08.07.2008⁷⁴

⁶⁰ BVerfGE 78, 205 (212); 84, 133 (149).

⁶¹ BVerfGE 86, 288 (311).

⁶² BVerfG, Beschl. v. 23.06.2010, 2 BvR 2559/08 – „Die Rechtsprechung ist gehalten, Unklarheiten über den Anwendungsbereich von Strafnormen durch Präzisierung und Konkretisierung im Wege der Auslegung nach Möglichkeit auszuräumen (Präzisierungsgesetz).“ siehe auch BVerfGE 45, 363 (371 f.); 86, 288 (311).

⁶³ BVerfGE 14, 245 (251).

⁶⁴ Schon der Verordnungsgeber selbst hat in Art. 83 Abs. 1 DSGVO bestimmt, dass die Geldbuße „abschreckend“ sein soll. Und so auch im Hinblick auf das Kartellrecht *Soltész/Steinle/Bielez*, EuZW 2003, 202 (206).

⁶⁵ Dazu auch *Bergt*, CR 2016, 670 (671).

⁶⁶ Dazu *EuGH*, Urt. v. 22.10.2015, C-194/14, Rn. 52.

⁶⁷ *Nolde*, (Fn. 5), (115).

⁶⁸ Ähnlich in Bezug auf Art. 6 DSGVO auch *Reimer*, in: Sydow (Fn. 5), Art. 6 Rn. 88.

⁶⁹ So auch *Dannecker/Biermann*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht: EG, VO (EG) 1/2003, 5. Aufl. 2012, Art. 23 Rn. 89.

⁷⁰ *Dannecker/Biermann*, (Fn. 69), Art. 23 Rn. 98 f.

⁷¹ *EuGH*, Urt. v. 18.07.2013, C-501/11, Rn. 58 – *Schindler Holding u.a./Kommission* zu Art. 23 Abs. 2; zu der Vorgängervorschrift Art. 15 Abs. 2 VO 17/62: *EuG*, Urt. v. 05.04.2006, T-279/02 – *Degussa/Kommission*, Rn. 72.

⁷² *EuG*, Urt. v. 14.05.1998, Rs. T-304/94, Rn. 89 – *Europa Carton/Kommission*; *EuGH*, Urt. v. 07.06.1983, C-100/80 – *Musique diffusion française u.a./Kommission*, Rn. 109.

⁷³ In diesem Sinne auch *EuGH*, Urteil v. 07.06.1983, C-100/80 – *Musique diffusion française u.a./Kommission*, Rn. 108: „Die Kommission durfte auch dem Umstand Rechnung tragen, daß derartige Praktiken [...] immer noch verhältnismäßig häufig sind, obwohl ihre Rechtswidrigkeit von Beginn der gemeinschaftlichen Wettbewerbsordnung an feststand[.]“

⁷⁴ *EuG*, Urt. v. 08.07.2008 – T-99/04.

ins Feld geführt wurde,⁷⁵ ist zu beachten, dass gerade in diesem Urteil der Verstoß gegen das Rechtsstaatsprinzip aufgrund der hohen Anzahl vorangegangener klärender Rechtsprechung scheiterte. Das Gericht betonte, dass „*der Grundsatz der Gesetzlichkeit der Straftatbestände und Strafen (nullum crimen, nulla poena sine lege) nicht dahin ausgelegt werden [kann], dass er die schrittweise Klärung der Vorschriften über die strafrechtliche Verantwortlichkeit durch richterliche Auslegung verböte.*“⁷⁶ Das EuG führte weiter aus: „*Bei der Beurteilung der Bestimmtheit verwendeter Begriffe berücksichtigt der Europäische Gerichtshof für Menschenrechte dementsprechend neben dem Gesetzestext auch die ständige und veröffentlichte Rechtsprechung.*“⁷⁷ Vor diesem Hintergrund sei die in dem Verfahren konkret vorgenommene Auslegung durch ein Gericht grundsätzlich vorhersehbar gewesen, da sich aufgrund zahlreicher Entscheidungen eine ständige Rechtsprechung gebildet habe, so das EuG.⁷⁸ Diesbezüglich verwies das EuG auf zahlreiche Entscheidungen, genau diese Situation ist aber für die DSGVO für sehr viele Fragestellungen nicht gegeben. Grundsätzlich ist zudem festzuhalten, dass das EuG in einem Fall, in dem es lediglich um ein Bußgeld in Höhe von 1000 € ging, das Rechtsstaatsprinzip sehr ernst genommen und auf das Bußgeldverfahren angewendet hat.

V. Fazit und Auswege aus der Rechtsstaatsmisere

Auch wenn der EuGH die Zweifel der Unbestimmtheit der Rechtsnormen im Hinblick auf das Kartellrecht aus dem Weg geräumt hat, ist bei der Frage der Vereinbarkeit der DSGVO mit den rechtsstaatlichen Prinzipien dessen Besonderheit – nämlich die fehlende Rechtsprechung sowie die unzureichenden Auslegungshilfen – zu beachten. Dabei ist die Unbestimmtheit der DSGVO selbstverschuldet. Hätte es in den vergangenen 20 Jahren deutlich mehr Rechtsstreitigkeiten um das BDSG und die Auslegung der RL 95/46/EG gegeben, wären viele nun offene Auslegungsfragen vermutlich geklärt. Ebenfalls selbstverschuldet ist die abstrakte und unbestimmte Formulierung ganz neuer datenschutzrechtlicher Institute, die über die RL 95/46/EG hinausgehen, wie etwa das Recht auf Datenportabilität.⁷⁹ Stand jetzt dürften – gemessen an der bisherigen Rechtsprechung des BVerfG – viele Bußgeldtatbestände als zu unbestimmt gelten und damit rechtswidrig und in der Praxis nicht anwendbar sein. Im Vorfeld zukünftiger Bußgeldbescheide müssen vermutlich viele Verfügungen ergehen, um die dann im Einzelfall gestritten werden kann, wodurch langfristige rechtliche Klarheit entstehen wird.

⁷⁵ *Bülte*, StV 2017, 460 (466).

⁷⁶ *EuG*, Urt. v. 08.07.2008 – T-99/04, Rn. 141.

⁷⁷ *EuG*, Urt. v. 08.07.2008 – T-99/04, Rn. 141.

⁷⁸ *EuG*, Urt. v. 08.07.2008 – T-99/04, Rn. 143, 145, mit Verweis auf die Rn. 115–128.

⁷⁹ Art. 20 DSGVO.