

# Das Datenschutzrecht im Wandel der Zeit

*Aqilah Sandhu*, Augsburg

Dem übergreifenden Thema der Festschrift entsprechend, widmet sich dieser Beitrag den Wandlungsprozessen im Datenschutzrecht, die seit den 1960er Jahren stattfanden. Die Geschichte des Datenschutzes ist bereits vielerorts nachgezeichnet worden – auch in Referaten auf der Jubilarin dieses Bandes selbst<sup>1</sup> – sodass darauf hier verwiesen werden kann. Nach einer kurzen Einführung (I.), die sich zunächst dem Datenschutzrecht aus dem Blickwinkel der Tagungsgeschichte nähert, sollen nachfolgend fünf wesentliche Entwicklungen in den Fokus gerückt werden. Dies betrifft die gewandelte gesellschaftliche Perzeption des Datenschutzes (II.), seine rechtliche Wandlung vom Datensicherheitsrecht hin zum Datenumgangsrecht (III.), den Wandel in der Schutzrichtung, die zunächst primär von der staatlichen Gefährdungslage ausging, hin zu einer weitreichenden Geltung zwischen Privaten (IV.), die gewandelte Funktion der Datenschutzgesetzgebung (V.) und abschließend die Verlagerung der Datenschutzgesetzgebung von der Landesebene im föderalen Bundesstaat auf die supranationale Ebene (VI.). Der Beitrag rundet mit einem kurzen Fazit ab (VII.).

## *I. Einführung: Das Datenschutzrecht im Spiegel der Assistententagungen*

Seit die Tagung der wissenschaftlichen Assistentinnen und Assistenten im Öffentlichen Recht vor einem Jahrzehnt ihr letztes Jubiläum gefeiert hat,<sup>2</sup> fand das Datenschutzrecht auf den nachfolgenden Tagungen nur wenig Beachtung,<sup>3</sup> obwohl in diesem Zeitraum (2010 bis heute) mit der „EU-Da-

- 
- 1 *Kai von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt/Betz/Farahat/Goldmann/Huber/Keil/Láncos/Schaefer/Smrkolj/Sucker/Valta (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht, 2009, 196.
  - 2 Dalibor/Debus/Gröblichhoff/Kruse/Lachmayer/Peters/Scharrer/Schröder/Seifert/Sicko/Stirn/Stöger (Hrsg.), Perspektiven des Öffentlichen Rechts. Festgabe 50 Jahre Assistententagung Öffentliches Recht, 2011.
  - 3 Zu den Beiträgen, die das Datenschutzrecht betreffen, s. aber sogleich.

tenschutzreform“<sup>4</sup> ein großer Umbruch im Datenschutzrecht stattgefunden hat. Es ist in der relativ jungen Geschichte des Datenschutzrechts die bisher größte Datenschutzreform auf Unionsebene. Umso erfreulicher ist es, dass sich die Jubiläumstagung 2020 in Trier dem Thema „Der digitalisierte Staat“<sup>5</sup> widmete. Die Organisatorinnen und Organisatoren bleiben damit am Zahn der Zeit. Frühere Assistententagungen waren ihrer Zeit fast schon voraus. Zum ersten Mal wurde der Datenschutz 1970 auf der Assistententagung in Wien diskutiert.<sup>6</sup> Als die Tagung 1973 erstmals in der Schweiz ausgetragen wurde, begnügten sich die Assistentinnen und Assistenten nicht nur mit der theoretischen Sicht *Gerhard Stadlers* auf den „Computer als neues Medium der Demokratie“, sie verbanden dies praxisnah mit einem Besuch im Forschungszentrum des US-amerikanischen Unternehmens IBM in der Schweiz,<sup>7</sup> dem damals marktbeherrschenden Unternehmen auf dem Gebiet der Datenverarbeitung. Und fünf Jahre vor dem magischen „Orwell’schen Jahr“ 1984,<sup>8</sup> keine zwei Jahre nach Verabschiedung des Bundesdatenschutzgesetzes (BDSG 1977),<sup>9</sup> widmeten sich die Assistentinnen und Assistenten 1979 in Hamburg unter dem Tagungsthema „Der technologische Fortschritt und seine rechtliche Bewältigung“<sup>10</sup> umfassend den noch heute aktuellen Fragestellungen des Daten-

---

4 Beginnend mit der Mitteilung der Europäischen Kommission 2010 „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4.11.2010, KOM (2010) 609 endg., 17, die im Erlass der Verordnung (EU) 2016/279 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO) sowie der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JIRL) mündete.

5 <https://www.uni-trier.de/index.php?id=68738> (letzter Abruf aller angegebenen Links: 28.11.2019).

6 Dies berichtete *Paul Kirchhof* 2008 auf der Tagung in Heidelberg, von *Lewinski* (Fn. 1), 197 dort Fn. 6.

7 S. den Tagungsbericht von *Hans-Jürgen Schmidt*, Demokratie und Föderalismus, in: *DÖV* 1973, 672, 673.

8 *George Orwell*, *Nineteen Eighty-Four*, 1949.

9 „Gesetz zum Mißbrauch personenbezogener Daten bei der Datenverarbeitung“ (Bundesdatenschutzgesetz – BDSG) vom 27.1.1977, BGBl. I 201.

10 Rückblickend *Ralf Bernd Abel*, Der Zeit voraus – Informations- und Technikrecht 1979 in Hamburg, in: *Dalibor/Debus/Gröblichhoff/Kruse/Lachmayer/Peters/Scharrer/Schröder/Seifert/Sicko/Stirn/Stöger* (Hrsg.) (Fn. 2), 239; s. auch *Armin Dittmann*, Tagungsbericht Hamburger Assistententagung, in: *JZ* 1979, 278.

schutzrechts. *Ralf Bernd Abel* referierte über den „Datenschutz im grenzüberschreitenden Datenverkehr“<sup>11</sup> und wies dabei auf die territoriale Begrenztheit nationaler Datenschutzgesetze und den Mangel an überstaatlichen Regeln hin. Auf europäischer Ebene befand man sich zu dieser Zeit noch im Prozess, den gesetzgeberischen Handlungsbedarf auszuloten. Die im Oktober 1985 in Kraft getretene Datenschutzkonvention des Europarats enthielt erstmals eine völkerrechtliche Mindestregelung zum grenzüberschreitenden Datenverkehr zwischen den Vertragsstaaten.<sup>12</sup> Die 1995 erlassene Datenschutzrichtlinie 95/46/EG (DSRL) sowie nun die DSGVO (vgl. Art. 3 Abs. 2, 44 DSGVO) schufen unionsweit einheitliche Regelungen zur Übermittlung personenbezogener Daten in Drittstaaten, konkretisiert durch die Rechtsprechung des EuGH im Lichte der Art. 7 und 8 GRCh.<sup>13</sup> *Hansjürgen Garstka*, späterer Berliner Datenschutzbeauftragter, referierte zum Thema „Rechtsstaatspostulate und Automation im Recht“<sup>14</sup> und nahm insbesondere die Automatisierung des Verwaltungsverfahrensrechts in den Blick. *Carl-Eugen Eberle* befasste sich mit dem Schutz medizinischer Daten und stellte die Forderung nach besonderen Bedingungen für deren Verarbeitung auf.<sup>15</sup> Gesundheitsdaten stehen nunmehr als besonders sensible Daten unter einem grundsätzlichen Verarbeitungsverbot, von dem nur in eng umgrenzten Fällen eine Ausnahme gemacht werden darf (vgl. Art. 4 Nr. 15 und Art. 9 DSGVO). Das Datenschutzrecht entwickelte sich seither von einem von der Rechtswissenschaft nur am Rande beachteten „Orchideenthema“<sup>16</sup> hin zu einem unüberschaubaren Massenthema. Es hat sich aber auch emanzipiert, weg von dem Nischendasein des weit verstandenen Informationsrechts – oder des „Rechts

---

11 S. die Zusammenfassung im Tagungsbericht von *Ralf Bernd Abel*, in: DVBl. 1979, 907, 908.

12 Art. 12 Datenschutzkonvention, ETS Nr. 108, BGBl. II 538.

13 EuGH, Urt. v. 6.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems, Rn. 79 ff. Zum Nachfolgebeschluss der Europäischen Kommission s. die anhängige Vorlagefrage des Irish High Court v. 9.5.2018 beim EuGH, Rs. C-311/18 und die Schlussanträge des Generalanwalts *Saugmangaard Oe* v. 19.12.2019, Rs. C-311/18 – Data Protection Commissioner/Facebook Ireland Ltd., Maximilian Schrems.

14 S. die Nachw. im Tagungsbericht von *Dittmann*, JZ 1979 (Fn. 10), 278.

15 *Carl-Eugen Eberle*, Der Schutz medizinischer Daten durch Verfassung, allgemeine und bereichsspezifische Datenschutzvorschriften, in: Kilian/Porth (Hrsg.), Juristische Probleme der Datenverarbeitung in der Medizin, 1979, 79.

16 *Abel*, in: Dalibor/Debus/Gröblichhoff/Kruse/Lachmayer/Peters/Scharrer/Schröder/Seifert/Sicko/Stirn/Stöger (Hrsg.) (Fn. 10), 242.

der Informationsgesellschaft“<sup>17</sup> unter dem es auf der Tagung 1996 diskutiert wurde – hin zu einem eigenständigen Rechtsgebiet. Die Tagung in Mainz 1996 war gleichzeitig eine der frühesten,<sup>18</sup> die sich mit den Fragen des Informationsrechts auseinandersetzte. Das Referat von *Marion Albers* über die „Neukonzeption des grundrechtlichen ‚Daten‘ schutzes“ befasste sich kritisch mit den Schutzzinhalten des informationellen Selbstbestimmungsrechts sowie grundlegend mit dem Informationsbegriff.<sup>19</sup> In der jüngeren Geschichte begleiteten die Assistentinnen und Assistenten den Datenschutz überwiegend aus der grundrechtlichen Perspektive, wie sich insbesondere an den Referaten von *Matthias Lachenmann* und *Martin Heidebach* in Augsburg 2015, sowie *Gabriele Buchholtz* in Hagen 2017 zeigte, auf die im Folgenden noch zurückzukommen sein wird.<sup>20</sup> Insgesamt bleibt festzuhalten, dass das Datenschutzrecht auf der Assistententagung kontinuierlich und sehr vorausschauend thematisiert wurde. Die Tagung war stets der Ort für wesentliche datenschutzrechtliche Impulse von auf diesem Gebiet namhaften Autorinnen und Autoren.

- 
- 17 S. den Tagungsband: Haratsch/Kugelmann/Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft. 36. Tagung der Wissenschaftlichen Mitarbeiterinnen und Mitarbeiter der Fachrichtung „Öffentliches Recht“, 1996.
  - 18 Die Vereinigung der deutschen Staatsrechtslehrer widmete sich ein Jahr später dem Thema „Der Grundrechtseingriff. Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung“, VVDStRL 57 (1998) mit den Berichten von *Friedrich Schoch*, 158 und *Hans-Heinrich Trute*, 216.
  - 19 *Marion Albers*, Neukonzeption des grundrechtlichen „Daten“ schutzes, in: Haratsch/Kugelmann/Repkewitz (Hrsg.) (Fn. 17), 113, 117 ff.; zur Tagung s. *Dieter Kugelmann*, Herausforderungen an das Recht der Informationsgesellschaft, in: *Dalibor/Debus/Gröblichhoff/Kruse/Lachmayer/Peters/Scharrer/Schröder/Seifert/Sicko/Stirn/Stöger* (Hrsg.) (Fn. 2), 431.
  - 20 *Matthias Lachenmann*, Das Ende des Rechtsstaats aufgrund der digitalen Überwachung durch die Geheimdienste und *Martin Heidebach*, Die NSA-Affäre in Deutschland – Stößt der Grundrechtsschutz an seine Grenzen?, jeweils in: *Hölzlwimmer/Engel/Krönke/Schmidl/Bebert/Faber* (Hrsg.), Rechtsfrieden – Friedensrecht. 55. Assistententagung Öffentliches Recht, 2016, 95 und 119; *Gabriele Buchholtz*, Grundrechte und Datenschutz im Spannungsfeld zwischen „Europäisierung und Emanzipation“, in: *Piecha/Holljesiefken/Fischer/Haaß/Herberg/Kracht/Safoklov* (Hrsg.), Rechtskultur und Globalisierung. 57. Assistententagung Öffentliches Recht, 2017, 97, 113 f.

## II. Vom Heilsbringer zum Schreckensgespenst

Gewandelt hat sich nicht nur der Fokus der Fachwelt, sondern auch der Blickwinkel der Gesellschaft auf das Datenschutzrecht: galt in den Anfangszeiten die staatliche Übermacht an Information als abzuwehrende Bedrohung und der Datenschutz fast schon als Heilsbringer, so überwiegt in der Bevölkerung heute, in Zeiten ubiquitärer und noch viel tiefgreifender Erfassung der Persönlichkeit durch die Informationstechnologie fast schon eine diffuse Angst vor dem Datenschutz selbst.<sup>21</sup> Dabei wird der Datenschutz angesichts der zunehmend intransparenten und allgegenwärtigen Datenvernetzung, der fragilen IT-Sicherheit und der Digitalisierung des privaten und öffentlichen Raums immer dringender.<sup>22</sup> Die Zeiten, in welchen die Gefahr der Datenverarbeitung noch darin gesehen wurde, dass gespeicherte Informationen „in Form eines Magnetophonbandes im Aktenkoffer“ oder „per Kabel oder Funk in jeden Teil der Welt“ verbracht werden konnte,<sup>23</sup> muten aus heutiger Sicht angesichts der globalen Massendatenverarbeitung und ihrer Übermittlung ohne Einsatz physischer Datenträger idyllisch und harmlos an. Dennoch löst Datenschutz bei den „betroffenen Personen“ im Sinne von Art. 4 Nr. 1 DSGVO oftmals nur noch ein müdes Augenrollen, ein gleichgültiges Schulterzucken aus. Die Ausübung der Datenhoheit, die Wahrnehmung der informationellen Selbstbestimmung, wird als lästiges Häkchensetzen wahrgenommen.<sup>24</sup> Diese veränderte Wahrnehmung liegt primär an der gewandelten Schutzrichtung des Datenschutzrechts. Das Datenschutzrecht nimmt zunehmend auch diejenigen in die Pflicht, die es zu schützen bestimmt ist. In den frühen 1970er und 1980er Jahren hatte der Gesetzgeber die Betreiber von Großrechenanlagen und Datenbanken im Blick. In Zeiten des haushaltsüblichen Privatcomputers und des „user generated content“ (des nutzergenerierten Inhalts) im Internet wird potenziell jede Person zur datenverarbeitenden Stelle – und damit auch zum Adressat der Verarbeiterpflichten, die das Da-

---

21 Statt vieler anlässlich der Geltung der DSGVO *Christina Hertel*, „Die Angst vor dem Datenschutz“, in: *Süddeutsche Zeitung* vom 25.5.2018, 36.

22 Zu den Risiken der Informationsgesellschaft s. *Horst Opaschowski*, in: *Roßnagel* (Hrsg.), *Handbuch Datenschutzrecht*, 2003, Kap. 2.1 Rn. 8 ff.

23 So das Szenario bei *Peter Karpenstein*, *Zur Zuständigkeit der Europäischen Gemeinschaften auf dem Gebiet des Datenschutzes*, in: *Bieber/Bleckmann/Capotorti* (Hrsg.), *Das Europa der zweiten Generation. Gedächtnisschrift für Christoph Sasse*, Band II, 1981, 889, 891.

24 *Christoph Gieseler*, *Öffentliche Kommunikation auf sozialen Netzwerkplattformen*, 2018, 35; vgl. auch *Opaschowski*, in: *Roßnagel* (Hrsg.) (Fn. 22), Rn. 59 ff.

tenschutzrecht vorsieht.<sup>25</sup> Die Angst mag insofern auch mit dem durch die DSGVO eingeführten Sanktionsregime (Art. 83 DSGVO) sowie der im Vergleich zum bisherigen Recht verschärften<sup>26</sup> und unmittelbar unionsrechtlich geregelten Haftung (Art. 82 DSGVO) Verantwortlicher bei Verstößen gegen das Datenschutzrecht begründet liegen. Das Datenschutzrecht hat sich angesichts der geänderten Bedrohungslage aus guten Gründen von seinem Ausgangspunkt als „spezifisches Abwehrmittel gegen die Folgen der Computernutzung“<sup>27</sup> durch den Staat und seine Einrichtungen hin zu einem vom Datenträger unabhängigen, allgemeinen „Datenumgangsrecht“ gewandelt, das auch die private sowie die manuelle Verarbeitung personenbezogener Daten reguliert, wenn diese in einem Dateisystem gespeichert sind oder werden sollen (vgl. EG 15 DSGVO).

### III. Von der Datensicherheitsgesetzgebung zum Datenschutzrecht

Deutlich lässt sich der Wandel in der Datenschutzgesetzgebung nachzeichnen, wobei diese maßgeblich durch die Rechtsprechung des BVerfG geprägt ist.<sup>28</sup> Das kodifizierte Datenschutzrecht nahm seinen Ausgangspunkt in dem Hessischen Datenschutzgesetz 1970 (HDSG).<sup>29</sup> Dieses galt für Daten unabhängig von ihrer Qualität oder eines etwaigen Personenbezugs.<sup>30</sup> Maßgeblich war vielmehr, dass die Verarbeitung von Daten maschinell und durch öffentliche Stellen erfolgte. Die Zielsetzung war damals noch nicht die Begrenzung der Datenerhebung, sondern die Verhinderung von

---

25 Vgl. auch Hannes Federrath/Andreas Pfitzmann, in: Roßnagel (Hrsg.) (Fn. 22), Kap. 2.2. Rn. 1; eingehend Matthias Lachenmann, Datenübermittlung im Konzern, 2016, 29 m. w. N.

26 Vgl. zur Haftung nach §§ 7 Abs. 1 und 8 Abs. 1 BDSG 2001 Peter Wedde, in: Roßnagel (Hrsg.) (Fn. 22), Kap. 4.4 Rn. 90 f.

27 Deutscher Juristentag (Hrsg.), Grundsätze für eine gesetzliche Regelung des Datenschutzes, 1974, 20 ff.

28 Vgl. Sebastian Bretthauer, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 Rn. 4.

29 Gesetz vom 7.10.1970, GVBl. I 625; Spiros Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung – Zur Problematik des „Datenschutzes“, in: NJW 1971, 673.

30 Vgl. § 1 HDSG 1970: „Der Datenschutz erfasst alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.“

Datenmissbrauch durch den unbefugten Zugriff Dritter sowie der Ausgleich von Informationsasymmetrien zwischen Exekutive und Legislative.<sup>31</sup> In der Regulierung auf Landesebene stand zu Beginn noch die Datensicherheit *bei* der Verarbeitung personenbezogener Daten durch öffentliche Stellen in zentralisierten Datenbanken und die Verhinderung von Datenmissbrauch stärker im Fokus als der Schutz des Individuums *vor* der Erhebung personenbezogener Daten.<sup>32</sup> So enthielten weder das HDSG 1970 noch das wenig später erlassene bayerische Datenschutzgesetz<sup>33</sup> Tatbestände über die Beschränkung der Datenerhebung durch die öffentliche Verwaltung. „Datenschutz“ wurde in § 2 HDSG 1970 vielmehr dahingehend präzisiert, dass die vorhandenen Daten nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies galt es durch personelle und technische Vorkehrungen sicherzustellen. So stand der Begriff „Datenschutz“<sup>34</sup> in den Anfängen primär für Datensicherheit, während er nunmehr den Schutz *personenbezogener* Daten bzw. der durch den Datenträger transportierten Information bei der Datenverarbeitung bezweckt.<sup>35</sup> Die Datensicherheit dient dem Schutz der Daten durch Vermeidung von Datenmissbrauch, -verlust oder -fälschung. Datenschutz hingegen bezweckt primär die Begrenzung des Umgangs mit personenbezogenen Daten durch die eingeschränkte Zulässigkeit der Verarbeitung.<sup>36</sup> Heutige Datenschutzgesetzgebung ist individualrechtlich orientiert, nimmt aber den Systemdatenschutz<sup>37</sup> bzw. den Datenschutz durch Technik stets mit in den Blick, wie beispielsweise in Art. 25 DSGVO und Art. 32 DSGVO. Aspekte der Datensicherheit sind nur noch ein Teilbereich des Datenschutzes.<sup>38</sup> Das grundsätzliche Verbot der Verarbeitung personenbezogener Daten sowohl für öffentliche als auch private Stellen wurde erstmals mit dem BDSG 1977 in § 3 S. 1 Nr. 1 und 2 BDSG gesetzlich veran-

---

31 *Laura Schulte*, Vom quantitativen zum qualitativen Datenschutz, 2018, 37.

32 Zur graduellen Verschiebung des Schutzgegenstands *Schulte* (Fn. 31), 38 f.

33 „Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern“ (EDVG) v. 12.10.1970, GVBl. 457.

34 Zur begrifflichen Unschärfe s. *Wilhelm Steinmüller/Bernd Lutterbeck/Christoph Mallmann/Uwe Harbort/Gerhard Kolb/Jochen Schneider*, Grundfragen des Datenschutzrechts, Gutachten im Auftrag des Bundesinnenministeriums, BT-Drs. VI/3826, 44 ff.; *Wilhelm Steinmüller*, Das informationelle Selbstbestimmungsrecht, in: RDV 2007, 158, 161.

35 Vgl. *Schulte* (Fn. 31), 105.

36 Vgl. *Federrath/Pfitzmann*, in: Roßnagel (Hrsg.) (Fn. 2), Rn. 5.

37 Hierzu grundlegend *Adalbert Podlech*, Verfassungsrechtliche Probleme öffentlicher Datenbanken, in: DÖV 1970, 473.

38 Vgl. *Schulte* (Fn. 31), 37.



kert. Die Verarbeitung personenbezogener Daten war danach nur zulässig, wenn ein Gesetz dies erlaubte oder wenn die Einwilligung des Betroffenen vorlag. Seither bildet dieses Regel-Ausnahme-Verhältnis ein Kontinuum auch im europäischen Datenschutzrecht. Die Erlaubnistatbestände wurden allerdings im Laufe der Zeit erweitert (vgl. nun Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO<sup>39</sup>). Ein zentraler Wandel im Datenschutzrecht ist damit in der Schwerpunktsetzung der Datenschutzgesetzgebung auszumachen.

#### IV. Vom Schutz Privater zur Bändigung privater Datenmacht

Grundrechtlich ist Datenschutz als Schutz der informationellen Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) im allgemeinen Persönlichkeitsrecht verankert. Er ist deshalb aber nicht auf den Privatsphärenschutz beschränkt.<sup>40</sup> Den verfassungsrechtlichen Grundstein für das Grundrecht auf informationelle Selbstbestimmung legte das BVerfG in dem wegweisenden Volkszählungsurteil.<sup>41</sup> Darin prägte der Erste Senat den Satz, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr“ gibt.<sup>42</sup> Geschützt sind deshalb auch Daten, die nicht aus der Privatsphäre stammen, deren Verknüpfung und Verarbeitung aber Auswirkungen auf die Verhaltensfreiheit der Betroffenen zeitigen können.<sup>43</sup> Das BVerfG hatte damals über mehrere Verfassungsbeschwerden gegen das Volkszählungsgesetz 1983 zu entscheiden, die sich gegen die im Gesetz angeordnete stichprobenartige Erhebung bestimmter personenbezogener Daten zur statistischen Bestandsaufnahme über die Bevölkerung, ihre Zusammensetzung und ihre wirtschaftliche Be-

---

39 Teilweise ergänzt durch § 3 BDSG i. d. F. des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 1. DS-AnpUG-EU) v. 30.7.2017, BGBl. I 2097.

40 Zum kontextbezogenen Schutzgehalt des Begriffs „Privatsphäre“ s. *Marion Albers*, Informationelle Selbstbestimmung, 2005, 387 ff.; krit. zur Verengung des Datenschutzes auf die Persönlichkeitssphäre *Spiros Simitis/Gerrit Hornung/Indra Spiecker gen. Döhm*, in: dies. (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, 2019, Einl. Rn. 27 m. w. N.

41 BVerfGE 65, 1.

42 BVerfGE 65, 1, 45.

43 St. Rspr. BVerfGE 65, 1, 45; BVerfGE 118, 168, 184 f.; BVerfGE 130, 151, 183 f.; BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 128; s. auch die weite Auslegung des Begriffs „Privatleben“ in Art. 8 EMRK: EGMR, Urt. v. 16.12.1992, *Niemietz v. Germany*, Nr. 13710/88, Rn. 29 ff.



tätigung wandten.<sup>44</sup> Das BVerfG erachtete eine Volkszählung zwar für prinzipiell vereinbar mit dem in dieser Entscheidung definierten Recht auf informationelle Selbstbestimmung, erklärte das Gesetz jedoch in Teilen für nichtig.<sup>45</sup> Das Recht auf informationelle Selbstbestimmung schütze gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der persönlichen Daten und gewährleiste dem Einzelnen die Befugnis „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.<sup>46</sup> Es verleihe dem Einzelnen nicht das Recht „im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine‘ Daten“, vielmehr habe er als soziales, auf Kommunikation angewiesenes Wesen innerhalb einer Gemeinschaft Einschränkungen des Rechts im überwiegenden Interesse der Allgemeinheit grundsätzlich hinzunehmen.<sup>47</sup> Das Volkszählungsurteil erging noch vor dem Hintergrund der Informations- und Machtasymmetrie zwischen dem Staat und seinen Bürgerinnen und Bürgern, die sich durch breite staatliche Datensammlungen einer Übermacht und damit einer Gefährdung ihrer privaten Selbstbestimmung ausgesetzt sahen. Grundrechtlich flankiert wird dieser Anspruch durch das aus dem allgemeinen Persönlichkeitsrecht abgeleitete und vom BVerfG in der Entscheidung zur Online-Durchsuchung geschaffene „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“.<sup>48</sup> Dieses soll dem Umstand gerecht werden, dass der Einzelne zunehmend auf die Nutzung informationstechnischer Systeme angewiesen ist und diesen persönliche Daten anvertraut oder zwangsläufig liefert.<sup>49</sup> Ist der heimliche Zugriff auf private Computersysteme einmal erreicht, werden ganze Lebensachverhalte offenbart, ohne dass der Einzelne von seinem informationellen Selbstbestimmungsrecht überhaupt Gebrauch machen kann. Es handelt sich insofern um einen grundrechtlichen Vorfeldschutz zur Ermöglichung der selbstbestimmten Nutzung von internetgestützten Privatcomputern,<sup>50</sup> der insbesondere eine objektiv-rechtliche Dimension entfaltet, indem er den Gesetzgeber zur Schaffung positiver Schutzmaßnahmen verpflichtet und das Ausnutzen von Sicherheitslücken durch staatliche Ak-

---

44 BVerfGE 65, 1, 12 f.

45 Zur Verfassungswidrigkeit der Kombination der Volkszählung mit dem Melderegisterabgleich s. BVerfGE 65, 1, 63 ff.

46 BVerfGE 65, 1, 43.

47 BVerfGE 65, 1, 43 f.

48 BVerfGE 120, 274, 313.

49 BVerfGE 120, 274, 313.

50 *Schulte* (Fn. 31), 194; *Simitis/Hornung/Spiecker gen. Döbmann*, in: dies. (Hrsg.) (Fn. 40), Rn. 16.

teure untersagt.<sup>51</sup> Der grundrechtliche Datenschutz ist von der Abwehr staatlicher informationsbezogener Maßnahmen unter den Bedingungen der modernen Datenverarbeitung geprägt. Entsprechend bildet die Datenverarbeitung durch öffentliche Stellen, insbesondere Polizei-, Strafverfolgungs- und Sicherheitsbehörden den Schwerpunkt der bundesverfassungsgerichtlichen Judikatur zum Datenschutzrecht.<sup>52</sup> Als der Bundesgesetzgeber mit dem BDSG 1977 erstmals auch die private Datenverarbeitung der Regulierung unterwarf, hatte er vorrangig Auskunfteien, Banken, Handelsfirmen und Versicherungen vor Augen<sup>53</sup> – Wirtschaftszweige, die geschäftlich personenbezogene, oftmals auch sensible Daten in einem großen Umfang verarbeiten und eine gewisse soziale Mächtigkeit aufweisen. Dem lag die Erwägung zu Grunde, dass die Datenverarbeitung in der freien Wirtschaft grundsätzlich freiwillig erfolge, während die staatliche Datenverarbeitung auf Zwang beruhe.<sup>54</sup> Personenbezogene Daten werden aber nicht mehr nur primär im Rahmen von Geschäftstätigkeiten marktmächtiger Unternehmen verarbeitet, sie sind vielmehr zum Gegenstand alltäglicher Tätigkeiten im Privat- und Sozialleben geworden.<sup>55</sup> Das europäische Datenschutzrecht regelt die Datenverarbeitung im privaten und im öffentlichen Bereich nun im Grundsatz einheitlich (nun Art. 2 Abs. 1 und Art. 6 Abs. 1 DSGVO). Bis zu diesem mit der DSRL initiierten Paradigmenwechsel differenzierte das BDSG noch zwischen der Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen, wobei nur erstere unter einem Erlaubnisvorbehalt stand. Zur Umsetzung der DSRL wurde im BDSG 2001<sup>56</sup> auch die Erhebung personenbezogener Daten durch nicht-öffentliche Stellen unter Erlaubnisvorbehalt gestellt.<sup>57</sup> So gilt die Erlaubnispflichtigkeit für die als Gedächtnisstütze von Hand angefertigten Notizen der Zeugen Jehovas bei ihrer Verkündungstätigkeit von

---

51 BVerfGE 120, 274, 313; Dirk Heckmann, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), Festschrift für Gerhard Käfer, 2009, 129, 135 ff.

52 BVerfGE 93, 181, 187 ff.; BVerfGE 109, 279, 318 ff.; BVerfGE 115, 320, 341; BVerfGE 118, 168, 184; BVerfGE 120, 274, 315 ff.; BVerfGE 133, 277, 320 f.; BVerfGE 125, 260, 309 ff.; s. aber jüngst zur Übertragung auf das Verhältnis zwischen Privaten BVerfG, Beschl. v. 6.11.2019 – 1 BvR 16/13, Rn. 84 f.

53 Vgl. die Beispiele in der Gesetzesbegründung, BT-Drs. 7/1027, 21.

54 Irene Wind/Michael Siebert, Entwurf für eine EG-Richtlinie zum Datenschutz, in: CR 1993, 46, 49.

55 Vgl. BVerfG, Beschl. v. 6.11.2019 – 1 BvR 16/13, Rn. 85; allgemein zur Problematik Carmen Langhake, Daten als Leistung, 2018.

56 Vgl. § 1 Abs. 2 Nr. 3, § 27 Abs. 1 S. 1 BDSG 2001.

57 BT-Drs. 14/4329, 29.

Haustür zu Haustür genauso,<sup>58</sup> wie für den global agierenden Suchmaschinenbetreiber, der Milliarden von Nutzerdaten verarbeitet und diese für gezielte Werbung, für die Ermittlung persönlicher Präferenzen oder für die Verknüpfung mit anderen Diensten, wie beispielsweise der Videoplattform YouTube, verwendet.<sup>59</sup> Die soziale, zwischenmenschliche Kommunikation erfolgt im Internet durch „verdatete Information“,<sup>60</sup> so dass alltägliche, öffentliche Online-Kommunikation unter dem grundsätzlichen Verarbeitungsverbot des Datenschutzrechts steht.<sup>61</sup> Insbesondere greift nach der restriktiven Lesart des EuGH<sup>62</sup> auch nicht die Anwendungsbereichsausnahme des Art. 2 Abs. 2 lit. c DSGVO für Tätigkeiten natürlicher Personen zur Ausübung ausschließlich persönlicher Tätigkeiten (sog. Haushaltsausnahme). Zwar gilt die Anwendungsbereichsausnahme grundsätzlich für die Nutzung sozialer Netzwerke im Internet (EG 18 S. 2 DSGVO), allerdings nur dann, wenn die Kommunikation in geschlossenen, privaten Chats oder Messenger-Diensten im engen Freundes- und Familienkreis erfolgt.<sup>63</sup> Sobald die Kommunikation im Internet einem unbegrenzten Kreis von Personen zugänglich ist, gilt die DSGVO.<sup>64</sup> Es gelten im Verhältnis der Nutzer zu den Anbietern der Online-Dienstleistungen einerseits und im Verhältnis der Nutzer untereinander andererseits jeweils grundsätzlich dieselben datenschutzrechtlichen Regeln, obwohl sich die Machtverhältnisse fundamental unterscheiden. Die Informations- und Machtasymmetrie verläuft nicht mehr nur eindimensional zwischen den Privaten und dem Staat, sondern immer mehr zwischen Bürgerinnen und Bürgern auf der einen und privaten Konzernen und Internetintermediären<sup>65</sup> auf der anderen Seite – also zwischen Privaten. Zudem besteht eine zunehmende Verflechtung von privater und öffentlicher Datenverarbeitung, wenn Private ihre Datenbestände dem Staat zu Nutze machen müssen, indem sie zur Weitergabe der im Rahmen ihrer gewerblichen Tätigkeit erhobenen personenbezogenen Daten an staatliche Ermittlungsbehörden verpflichtet

---

58 EuGH, Urt. v. 10.7.2018, Rs. C-25/17, ECLI:EU:C:2018:551, Rn. 52 ff. – Jehovan todistajat.

59 S. die Google-„Datenschutzerklärung“, abrufbar unter: <https://policies.google.com/privacy>.

60 Zum Begriff *Gieseler* (Fn. 24), 27, 29.

61 Krit. *Gieseler* (Fn. 24), 30.

62 Zu Art. 3 Abs. 2 DSRL: EuGH, Urt. v. 6.11.2003, Rs. C-101/01, Slg. 2003, I-12971, Rn. 47 – Lindqvist.

63 *Alexander Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.) (Fn. 40), Art. 2 DSGVO Rn. 29.

64 EuGH, Urt. v. 6.11.2003, Rs. C-101/01, Slg. 2003, I-12971, Rn. 27, 47 – Lindqvist.

65 Zu diesen s. BVerfG, Beschl. v. 6.11.2019 – 1 BvR 16/13, Rn. 85.

werden<sup>66</sup> oder wenn ihre privaten Server zur Speicherung staatlich erhobener Daten verwendet werden.<sup>67</sup> Private Datenmacht trifft dann auf intensive staatliche Informationseingriffe.<sup>68</sup> Problematisch ist dieses Zusammenreffen insbesondere deshalb, weil die Verarbeitung personenbezogener Daten durch private Unternehmen auch auf Grund der Einwilligung der Betroffenen oder überwiegender berechtigter Interessen des Datenverarbeiters erfolgen kann (Art. 6 Abs. 1 UAbs. 1 lit. a und f DSGVO), dies jedoch keine Erlaubnistatbestände für die Verarbeitung personenbezogener Daten durch Polizei- und Strafverfolgungsbehörden sind (vgl. Art. 8 JIRL).<sup>69</sup> Datenschutz zielt nach dem Verständnis der Technologiekonzerne auf den Schutz vor Dritten, also primär anderen Internetnutzern, ab.<sup>70</sup> Im Unterschied dazu soll das Datenschutzrecht gerade vor der Macht der datenverarbeitenden Stellen schützen. Auf die Frage, wie unter diesen Umständen die digitale Selbstbehauptung gelingen kann, hat das Datenschutzrecht noch keine adäquate Antwort gefunden – der derzeitige Ansatz eines „one size fits all“ für sämtliche Verarbeiter erscheint jedenfalls zu undifferenziert.

---

66 S. bspw. die Übermittlung von Fluggastdaten an Sicherheitsbehörden, hierzu EuGH, Gutachten 1/15 v. 26.7.2017, ECLI:EU:C:2017:592 – PNR Canada oder die auf der 210. Konferenz der Innenminister und -senatoren der Länder vom 12.-14.6.2019 in Kiel diskutierte Auswertung von Daten aus Smart-Home-Geräten zu Zwecken der Strafverfolgung (Spurensicherung in der digitalen Welt), Sammlung der zur Veröffentlichung freigegebenen Beschlüsse, 18, abrufbar unter [www.innenministerkonferenz.de](http://www.innenministerkonferenz.de); zur auf Grundlage von Algorithmen regierenden Staatsgewalt s. *Adrian Lobe*, Speichern und Strafen. Die Gesellschaft im Datengefängnis, 2019.

67 Beispielsweise die Speicherung von Bodycam-Aufnahmen der Bundespolizei auf Servern von Amazon in den USA s. *Adrian Lobe*, Hilfssheriff Amazon, in: SZ.de vom 27.11.2019, abrufbar unter <https://sz.de/1.4698724>.

68 Hierzu *Wolf-Rüdiger Schenke*, Verfassungsrechtliche Probleme des polizeilichen Einsatzes von Bodycams, in: *VerwArch* 2019, 436.

69 Gem. Art. 8 JIRL ist die Verarbeitung personenbezogener Daten durch Polizei, Strafverfolgungs- und Justizbehörden nur rechtmäßig, „wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommen wird [...]“.

70 Auch die Fälle rund um das „Recht auf Vergessen“ wenden sich nur gegen die Auffindbarkeit durch andere Internetnutzer, nicht aber gegen die datenverarbeitenden Konzerne selbst, vgl. BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17; BVerfG, Beschl. v. 6.11.2019 – 1 BvR 16/13; EuGH, Urt. v. 24.9.2019, Rs. C-507/17, ECLI:EU:C:2019:772 – Google LLC/CNIL; EuGH, Urt. v. 13.5.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google Spain.

V. Von der Begrenzung zur Legitimierung staatlicher Eingriffe

Als Querschnittsmaterie scheint sich der Datenschutz zunehmend als „Law of the horse“<sup>71</sup> in unübersichtlicher Detailgesetzgebung zu verlieren. Regeln, die einst zur Begrenzung staatlicher Datenmacht gedacht waren, tragen zuweilen erst zur Datenakkumulation bei, indem sie oftmals nur der Legalisierung von Datenerhebungen dienen.<sup>72</sup> Die Schaffung bereichsspezifischer Ermächtigungsgrundlagen für die staatliche Datenverarbeitung seit dem Volkszählungsurteil hat nicht immer zu einer Begrenzung der zulässigen Datenverarbeitung oder zu einem Mehr an Datenschutz geführt. Datenschutzgesetzgebung erschöpft sich vielmehr oftmals nur noch in der „Schaffung von Erlaubnistatbeständen“.<sup>73</sup> Beispiel hierfür mag das jüngst in Kraft getretene Zweite Datenschutzanpassungs- und Umsetzungsgesetz EU sein,<sup>74</sup> das im Wege der Omnibusgesetzgebung in 155 bereichsspezifischen Gesetzen Anpassungen vornimmt, dabei jedoch neue Verarbeitungsbefugnisse einführt und in vielen Bereichen die Betroffenenrechte einschränkt.<sup>75</sup> Insbesondere ab Beginn des 21. Jahrhunderts wird der Datenschutz verstärkt in seiner Abwehrdimension und unter dem Blickwinkel der Sicherheitsgesetzgebung betrachtet.<sup>76</sup> Diese Entwicklung wurde auch auf der Assistententagung verfolgt, indem das Datenschutzrecht zunehmend mit Blick auf die erweiterten Strafverfolgungs-, Gefahrenabwehr- und Überwachungsbefugnisse behandelt wurde. So befasste sich ein ganzes Panel auf der dem Rechtsfrieden gewidmeten Augsburger Assistententagung 2015 mit der Fragestellung „Frieden durch staatliche Überwachung – oder Ende des Rechtsstaates?“. Die Beiträge von *Matthias Lachenmann* über „Das Ende des Rechtsstaates aufgrund der digitalen Überwachung

---

71 *Frank H. Easterbrook*, Cyberspace and the Law of the Horse, in: University of Chicago Legal Forum 1996, 207 und die Replik von *Lawrence Lessig*, The Law of the Horse: What Cyberlaw might teach, in: Harvard Law Review 113 (1999), 501.

72 Pointiert von *Lewinski*, in: Arndt/Betz/Farahat/Goldmann/Huber/Keil/Láncos/Schaefer/Smrkolj/Sucker/Valta (Hrsg.) (Fn. 1), 204: „Normierung von Datenmacht“.

73 *Schulte* (Fn. 31), 96.

74 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) vom 20.11.2019, BGBl. I 1626.

75 S. nur die Kritik an den Eingriffsbefugnissen für das BSI bei *Hartmut Aden*, Stellungnahme, Ausschuss-Drs. 19(4)187 H und an der Einschränkung der Betroffenenrechte bei *Kirsten Bock*, Stellungnahme, Ausschuss-Drs. 19(4)187 G.

76 Vereinzelt schon in den 1980er Jahren, s. *Schulte* (Fn. 31), 107.

durch die Geheimdienste“ und *Martin Heidebach* über den Grundrechtsschutz gegen die im Zuge der NSA-Affäre bekannt gewordenen Überwachungsmaßnahmen beleuchteten sehr kritisch die weiterhin hochaktuellen Fragen rund um den Missbrauch staatlicher Datenmacht aus grundrechtlicher Perspektive.<sup>77</sup> Das BVerfG spricht in diesem Kontext von dem gebotenen Schutz vor dem „Gefühl des Überwachtwerdens“. <sup>78</sup> In den Hintergrund gerät durch diese Entwicklung freilich, dass sich der Datenschutz nicht in der pauschalen Abwehr von Datenverarbeitung erschöpft, sondern dass die Schutzpflicht sowie die objektiv-rechtliche Dimension des Rechts auf informationelle Selbstbestimmung den Staat vielmehr zur freiheitsgerechten Ausgestaltung bestimmter Bereiche sowie Schaffung einer datensichereren Infrastruktur verpflichtet.<sup>79</sup>

## VI. Von der Landes- zur Unionsgesetzgebung

Schließlich ist auf die letzte große Wandlung im Datenschutzrecht einzugehen, der Verlagerung des Datenschutzrechts auf die supranationale Ebene beginnend in den frühen 1990er Jahren. Waren für den nationalen Gesetzgeber die Automatisierung und der Einsatz elektronischer Datenverarbeitung anstoßgebend,<sup>80</sup> so geht es im Zeitalter der grenzenlosen Datenverarbeitung und -übermittlung und der allgegenwärtigen Digitalisierung um Fragen der Grenzen souveräner Staatlichkeit.

---

77 *Lachenmann* und *Heidebach*, in: Hölzlwimmer/Engel/Krönke/Schmidl/Bebert/Faber (Hrsg.) (Fn. 20), 95, 119.

78 St. Rspr. BVerfGE 107, 299, 328; BVerfGE 150, 244, 268, Rn. 51.

79 Zum objektiv-institutionellen Verständnis *Marion Albers*, Informationelle Selbstbestimmung, 460; *dies.*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.) (Fn. 19), 124 f.; *Heckmann*, in: Rüßmann (Hrsg.) (Fn. 51), 129; *Nikolaus Marsch*, Das europäische Datenschutzgrundrecht, 2018, 111 ff.

80 *Simitis/Hornung/Spiecker gen. Döhmann*, in: *dies.* (Hrsg.) (Fn. 40), Einleitung, Rn. 6 ff.

1. *Datenschutz als Unionsaufgabe: vom Handelshemmnis zum Individualgrundrecht*

Als Aufgabe entdeckte die Europäische Union den Datenschutz auf Druck des Europäischen Parlaments,<sup>81</sup> dem die Europäische Kommission erst etwas zögerlich nachgab. Sie war lange Zeit der Überzeugung, dass die innerstaatliche Ratifikation der völkerrechtlichen Datenschutzkonvention des Europarats durch die EU-Mitgliedstaaten ausreichend sein würde.<sup>82</sup> Datenschutz wurde zwar als individualschützendes Grundrecht anerkannt, nicht aber als genuine Aufgabe der damaligen EWG, die noch primär auf den reibungslosen Binnenmarkt fokussiert war. Soweit sich die Europäische Kommission mit dem Datenschutz befasste, erfolgte dies primär zur Förderung der neuen Informationstechnologien und zur Schaffung eines reibungslosen Informationssektors.<sup>83</sup> Datenschutz stellte zunächst eine Begrenzung des freien Informationsflusses dar, was der Eigenrationalität des freien Marktes auf den ersten Blick widerspricht. Diese Auffassung wandelte sich jedoch bereits in den späteren 1980er Jahren<sup>84</sup> und endgültig mit der zunehmenden Politisierung der Union unter dem Vertrag von Maastricht sowie der Anerkennung von Grundrechten durch den EuGH im Wege der wertenden Rechtsvergleichung,<sup>85</sup> so dass heute der Schutz personenbezogener Daten als Regelungsgegenstand wie selbstverständlich „zur Seele Europas“<sup>86</sup> gehört. Seit dem Vertrag von Lissabon ist der grundrechtliche Datenschutz in Art. 7 und 8 GRCh rechtsverbindliches Primärrecht (vgl. Art. 6 Abs. 1 EUV).

---

81 S. bspw. die Entschließung des Europäischen Parlaments „zum Schutz der Rechte des Einzelnen angesichts der fortschreitenden Entwicklung auf dem Gebiet der automatisierten Datenverarbeitung“, ABl. EG C 60/48 vom 13.3.1975.

82 Empfehlung der Europäischen Kommission v. 29.7.1981, ABl. EG L 246/31 v. 29.8.1981.

83 *Reinhard Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990, 537 ff.; *Spiros Simitis*, Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, in: NJW 1997, 281, 281; vgl. auch Europäische Kommission, Mitteilung über eine Gemeinschaftspolitik auf dem Gebiet der Datenverarbeitung, KOM (75) 467; BT-Drs. 8/37, 36.

84 Zu den ersten Richtlinienentwürfen der Europäischen Kommission s. *Ellger* (Fn. 83), 542.

85 Im Ansatz ist der Datenschutz als Grundrecht auf europäischer Ebene schon seit EuGH, Urt. v. 12.11.1969, Rs. 29/69, ECLI:EU:C:1969:57 – Stauder anerkannt. Dies ist aber keine datenschutzrechtliche Entscheidung i. e. S., vgl. *Birte Siemen*, Datenschutz als europäisches Grundrecht, 2006, 216.

86 *Eugen Ehmann/Martin Selmayr*, in: dies. (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. 2018, Vorwort, V.



## 2. Pfadabhängiges Sekundärrecht: von der Richtlinie zur Verordnung

Im Zuge der jüngsten EU-Datenschutzreform wurde die DSRL aufgehoben und durch die DSGVO sowie die JIRL über die Datenverarbeitung im Bereich der Strafverfolgung und der Strafvollstreckung ersetzt. Markant ist der Rechtsformwechsel im Datenschutzrecht von der Richtlinie zur Verordnung. Doch allein dem Inhalt und den Rechtswirkungen nach zu urteilen, handelt es sich nicht um eine revolutionäre Neuerung. Denn schon die DSRL entfaltete nach der Rechtsprechung des EuGH eine grundsätzlich abschließende Harmonisierungswirkung, ihre Erlaubnistatbestände in Art. 7 DSRL waren bereits unmittelbar anwendbar.<sup>87</sup> Zudem bedarf die Anwendbarkeit der DSGVO trotz ihrer grundsätzlich unmittelbaren Wirkung (Art. 288 Abs. 2 AEUV) umfassender Umsetzungs- und Anpassungsgesetze in den Mitgliedstaaten,<sup>88</sup> weil sie an vielen Stellen lückenhaft und sehr allgemein konzipiert ist. Der hohe Abstraktionsgrad ist im Sinne eines technikneutralen Ansatzes grundsätzlich zu begrüßen, da er entwicklungs-offen ist.<sup>89</sup> Gleichzeitig löst er Konkretisierungspflichten durch die Europäische Kommission und die Mitgliedstaaten aus. Es stellt sich die Frage nach dem Mehrwert einer supranationalen Regelung, wenn sie sich letztlich nur dort durchzusetzen vermag, wo auch der territorial begrenzte Schutz nationaler Gesetze greift: das finnische Datenschutzrecht bietet in seinem Geltungsbereich gegen die Datenverarbeitung der Zeugen Jehovas letztlich denselben Schutz, wie das französische „Loi relative à l’informatique, aux fichiers et aux libertés“<sup>90</sup> im Fall Google II. Wenn Ralf Bernd Abel auf der Assistententagung 1979 über ein globales Konzept für den Datenschutz referierte, um transnational tätige Unternehmen einheitlichen Regelungen zu unterwerfen,<sup>91</sup> bleibt 40 Jahre danach, trotz Bestehen eines supranational harmonisierten Datenschutzrechtsrahmens, nur der ernüchternde Befund, dass das Unternehmen Google nicht einmal innerhalb der Union einheitlich zur Löschung von Suchmaschinenergebnissen verpflich-

---

87 EuGH, Urt. v. 24.11.2011, Rs. C-468/10, 469/10, ECLI:EU:C:2011:777 – ASNEF.

88 S. nur das 1. und 2. DSAnpUG-EU sowie die Anpassungs- und Umsetzungsgesetze in den Ländern.

89 Zum Für und Wider *Simitis/Hornung/Spiecker gen. Döbmann*, in: dies. (Hrsg.) (Fn. 40), Einleitung, Rn. 241.

90 Das französische Datenschutzgesetz Loi n° 78-17 vom 6.1.1978, wörtlich das „Gesetz über die Informatik, die Dateien und die Freiheiten“.

91 S. die Zusammenfassung von Abel (Fn. 11), 908.

tet werden kann, wie der EuGH feststellte.<sup>92</sup> Zwar ist darauf hinzuweisen, dass die jeweiligen nationalen Gesetze ihr Schutzniveau wesentlich auch der DSRL zu verdanken haben, die alle Mitgliedstaaten auf einen gemeinsamen Datenschutznenner sowohl im öffentlichen, als auch im privaten Bereich verpflichtet. Doch gleichzeitig muss sich das Unionsrecht gemäß dem in Art. 5 Abs. 3 UAbs. 1 EUV verankerten Subsidiaritätsprinzip daran messen lassen, ob der Regelungsgegenstand wegen seines Umfangs oder seiner Wirkungen auf Unionsebene „besser zu verwirklichen“ ist. Im Datenschutzrecht ist dies nicht durchgehend der Fall, vielmehr erweist sich der pauschale Regelungsansatz der DSGVO als weniger effektiv, wenn er sich nicht bei der Regulierung transnationaler Unternehmen bewährt. Problematisch ist zudem der dezentrale Vollzug<sup>93</sup> und die gebotene gerichtliche Einbindung des EuGH in Datenschutzfragen im Wege des Vorlageverfahrens, die den Individualrechtsschutz aufgrund des erforderlichen Zwischenverfahrens erheblich verzögert.<sup>94</sup>

### *3. Datenschutz im Jurisdiktionskonflikt: vom zentralen zum dezentralen Grundrechtsschutz*

Dass die Verlagerung des Datenschutzrechts auf das Europarecht neue Konfliktfelder aufwirft, wurde auch auf der Assistententagung diskutiert. Zuletzt befasste sich auf der Tagung in Hagen 2017 das Referat von *Gabriele Buchholtz* unter dem Titel „Grundrechte und Datenschutz im Span-

---

92 So der EuGH im Urt. v. 24.9.2019, Rs. C-507/17, ECLI:EU:C:2019:772, Rn. 64 – Google LLC/CNIL.

93 Dem wird institutionell durch die Einführung des Europäischen Datenschutzausschusses und die Regelungen zur Zusammenarbeit der Aufsichtsbehörden (Art. 56 Abs. 2 und Art. 60 DSGVO) sowie des Kohärenzverfahrens (Art. 63 ff. DSGVO) begegnet. Auf diese kompensatorische Funktion hinweisend EuGH, Urt. v. 24.9.2019, Rs. C-507/17, ECLI:EU:C:2019:772, Rn. 68 – Google LLC/CNIL.

94 S. nur die Vorratsdatenspeicherung, die wiederholt (u. a. Vorlage des BVerwG, Beschl. v. 25.9.2019 – 6 C 12.18) vor dem EuGH verhandelt wird; Schlussanträge des Generalanwalts *Sánchez-Bordona* vom 15.1.2020, Rs. C-623/17, verb. Rs. C-511/18 u. C-512/18, Rs. C-520/18. Zur Problematik *Aqilah Sandhu*, Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union, in: *EuR* 2017, 453.

nungsfeld zwischen ‚Europäisierung und Emanzipation‘<sup>95</sup> mit dem Jurisdiktionskonflikt im Datenschutzrecht. Sie plädierte dabei für eine ‚Europäisierung des bundesverfassungsgerichtlichen Prüfungsprogramms‘, indem die GRCh ähnlich wie die EMRK als Auslegungshilfe für die nationalen Grundrechte herangezogen und inzident im Rahmen der Grundrechtskontrolle mitgeprüft werden solle. Während die These von den Teilnehmerinnen und Teilnehmer auf der Tagung damals äußerst kritisch diskutiert wurde,<sup>96</sup> ging der Erste Senat des BVerfG mit seiner jüngsten Entscheidung über die – ansonsten progressiven Vorschläge der Tagungsteilnehmerinnen und Teilnehmer – hinaus, indem er die GRCh selbst zum Prüfungsmaßstab erklärte.<sup>97</sup> Die Verletzung von Unionsgrundrechten kann nach dem Wortlaut von Art. 93 Abs. 1 Nr. 4 a GG, § 90 Abs. 1 BVerfGG nicht vor dem BVerfG gerügt werden.<sup>98</sup> Dies bedeutete in unionsrechtlich geprägten Sachverhalten selbst bei paralleler Anwendbarkeit des Grundgesetzes neben der GRCh, dass die Durchsetzung der Unionsgrundrechte im Wesentlichen durch die nationalen Fachgerichte zu erfolgen hatte, deren Prüfungsmaßstab auch das Unionsrecht umfasst.<sup>99</sup> Diese haben bei Verstößen des nationalen Rechts gegen Unionsrecht die Unionsgrundrechtswidrigkeit selbst festzustellen, ohne zur Vorlage an das BVerfG verpflichtet zu sein.<sup>100</sup> Damit konnte bei einem Verstoß gegen Unionsgrundrechte die jeweilige innerstaatliche Regelung im konkreten Fall für unanwendbar erklärt werden, während ein Verstoß gegen die Grundrechte des Grundgesetzes die Nichtigkeit der Norm zur Folge hätte. Um gleichwohl im unionsrechtlich vollharmonisierten Datenschutzrecht die Deutungshoheit zu behalten, ist der Erste Senat des BVerfG nun in seiner hi-

---

95 *Buchholtz*, in: Piecha/Holljesiefken/Fischer/Haaf/Herberg/Kracht/Safoklov (Hrsg.) (Fn. 20), 113 f.; *dies.*, Grundrechte und Datenschutz im Dialog zwischen Karlsruhe und Luxemburg, in: DÖV 2017, 837.

96 Zur Tagung s. *Franziska Huber/Cornelia Kibler/Victoria Kugelman/Aqilah Sandhu*, Bericht über die 57. Assistententagung Öffentliches Recht vom 21.–24. Februar 2017 in Hagen – Thema: Rechtskultur und Globalisierung, in: BayVBl 2017, 841, 843.

97 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 57; hierzu *Julian Nusser*, Grundrechtsschutz im Mehrebenensystem, 591 ff. (in diesem Band).

98 BVerfGE 115, 276, 299 Rn. 77; BVerfGE 110, 141, 154 f.

99 Die Fachgerichte agieren insofern als „funktionale Unionsgerichte“, *Bernhard Wegener*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 267 AEUV Rn. 1.

100 St. Rspr., EuGH, Urt. v. 11.9.2014, Rs. C-112/13, ECLI:EU:C:2014:2195, Rn. 36 – A und B; EuGH, Urt. v. 19.1.2010, Rs. C-555/07, ECLI:EU:C:2010:21, Rn. 54 f. – Kücükdeveci; BVerfG, Beschl. v. 9.1.2001, NJW 2001, 1267, 1268; BVerfGE 118, 79, 95.

storischen Leitentscheidung („Recht auf Vergessen II“)<sup>101</sup> dazu übergegangen, die Unionsgrundrechte zum unmittelbaren bundesverfassungsgerichtlichen Prüfungsmaßstab zu erheben und zog im Rahmen einer Urteilsverfassungsbeschwerde erstmals die Grundrechte aus Art. 7 und Art. 8 GRCh als Prüfungsmaßstab heran.<sup>102</sup> Dogmatisch folgte er die Prüfungskompetenz aus Art. 23 Abs. 1 GG, wonach die Integrationsverantwortung allen Staatsorganen, auch dem BVerfG obliege.<sup>103</sup> Die Entscheidung betraf die Klage einer Unternehmerin, die sich zivilrechtlich gegen den Suchmaschinenbetreiber Google auf Entfernung einer Verlinkung wandte (sog. Auslistung), weil bei Eingabe ihres Namens in die Suchmaschine als eines der ersten Suchergebnisse eine Verlinkung auf einen Fernsehbeitrag über „Die fiesen Tricks der Arbeitgeber“ erschien. Da die DSGVO die Datenverarbeitung durch Private abschließend regle, ging das BVerfG von einem unionsrechtlich vollständig determinierten Sachverhalt aus. Nach der bisherigen Rechtsprechung wäre das BVerfG in diesem Fall auf die Überprüfung der Vereinbarkeit fachgerichtlicher Entscheidungen mit Art. 101 Abs. 1 S. 2 GG beschränkt gewesen. Dieser setzt voraus, dass die Fachgerichte eine Vorabbeurteilung des EuGH nach Art. 267 AEUV willkürlich unterlassen hatten.<sup>104</sup> Nun können Betroffene im Wege der Verfassungsbeschwerde unmittelbar die Verletzung des unionsrechtlichen Datenschutzgrundrechts in Art. 7 und 8 GRCh vor dem BVerfG rügen. Dies könnte dem europäischen Datenschutzrecht innerstaatlich neue Durchsetzungskraft verleihen. Denn das BVerfG reagiert damit ausdrücklich auf die Problematik, dass es die Grundrechtsprüfung bei zunehmender Europäisierung sonst den Fachgerichten und im Wege der Vorlage im Zweifel dem EuGH überlassen müsste.<sup>105</sup> Gleichzeitig ermöglicht dies die aktive Gestaltung des Grundrechtsschutzes im Bereich des Datenschutzes trotz sekundärrechtlicher Vollharmonisierung: So ließ es sich der Erste Senat in der genannten Entscheidung nicht nehmen, bei der Abwägung in Abgrenzung zur Google Spain-Entscheidung des EuGH u. a. mit Blick auf die Grundrechte mitbetroffener Dritter im Internet eigene Akzente zu setzen sowie

---

101 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 47 f.; s. bereits die Kritik des Berichterstatters in diesem Verfahren: *Johannes Masing*, „Ein Abschied von den Grundrechten“, in: *Süddeutsche Zeitung* vom 9.1.2012, 10.

102 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 32, 50, ausdrücklich auf die Schutzlücke Bezug nehmend in Rn. 61.

103 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 55 f.

104 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 64.

105 BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17, Rn. 51, 61.

klarzustellen, dass der Schutz personenbezogener Daten keinen grundsätzlichen Vorrang vor der Meinungsfreiheit genießt.

### *VII. Ausblick*

Bei allen Wandlungen im Recht des Datenschutzes ist – neben der zentralen Konzeption des grundsätzlichen Verbots mit Erlaubnisvorbehalt für die Verarbeitung personenbezogener Daten – noch eines konstant geblieben. Unverändert inhärent ist seit jeher der von *Frank Easterbrook* in seinem legendären Aufsatz mit dem Titel „Cyberspace and the Law of the Horse“ besonders für das Gebiet der Technik konstatierte, ausgeprägte „interdisziplinäre Dilettantismus“,<sup>106</sup> weshalb sein Plädoyer für technikoffene, klare und quantitativ weniger Regeln auch noch heute aktuell ist. Es kann angesichts dessen an das Resümee der Tagungsteilnehmerinnen und -teilnehmer von 1979 angeknüpft werden, das *Armin Dittmann* in seinem Tagungsbericht zur eingangs erwähnten Hamburger Tagung festgehalten hat: Dem Zentralanliegen des Datenschutzes Rechnung zu tragen, nämlich den Menschen vor seiner „Verobjektivierung“ in Gestalt von unkontrollierbaren Datenbeständen zu schützen, bedarf einer Besinnung auf die rechtsstaatlichen Grundprinzipien: auf die Menschenwürde, den Anspruch auf rechtliches Gehör und vor allem dem Verhältnismäßigkeitsgrundsatz,<sup>107</sup> der im Datenschutz sowohl im vertikalen, als auch im horizontalen Grundrechtsverhältnis längst den Siegeszug angetreten hat. Die Assistententagung wähnt sich in Habitus und Ablauf zwar als Hort der Traditionspflege, thematisch jedoch war sie im Rückblick immer auch Ort fortschrittlicher Gedanken und provokativer Thesen. Auch das „Reizthema“ Digitalisierung, Technik und Datenschutz im weiteren Sinne ging nicht an ihr vorbei, sondern wurde von ihr maßgeblich positiv mitgestaltet.

---

106 *Easterbrook*, University of Chicago Law Forum 1996 (Fn. 71), 207.

107 *Dittmann*, JZ 1979 (Fn. 10), 279.