3.3 Recht
Wenn Gerichte es im digitalen Zeitalter richten müssen

Ulf Buermeyer und Malte Spitz

Als im Mai 1949 das Grundgesetz der Bundesrepublik Deutschland verabschiedet wurde, sahen sich die Verfasser*innen einer Lebenswelt gegenüber, die mit der unsrigen kaum zu vergleichen ist. Computer im heutigen Sinne gab es nicht, das Internet sollte erst Jahrzehnte später erfunden werden. Trotzdem regelt das Grundgesetz, also die Verfassung der Bundesrepublik Deutschland, in seiner Auslegung durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) auch den digitalen Raum – und zwar im Grundsatz überzeugend: Das BVerfG hat es in bemerkenswerter Weise verstanden, die Grundrechte »entwicklungsoffen« zu interpretieren, ihnen wohldosiert neue Schutzdimensionen zu entnehmen und so einen im Kern rund achtzig Jahre alten Text fit für das digitale Zeitalter zu machen. Diese Entwicklung setzt sich inzwischen auch auf europäischer Ebene fort, wo der Europäische Gerichtshof auch die noch junge Charta der Grundrechte der Europäischen Union zu einem Maßstab der Digitalpolitik weiterentwickelt.

Im folgenden Beitrag werden wir zunächst die Entwicklung der höchstrichterlichen Rechtsprechung zu Fragen der Digitalisierung nachzeichnen. Im Ausgangspunkt wird es dabei um die informationelle Selbstbestimmung gehen, aber die betroffenen grundrechtlichen Konfliktlinien weisen längst weit über den Datenschutz hinaus. So werden wir auch Fragen der Meinungsfreiheit und der Informationsfreiheit behandeln und schließlich einen Ausblick wagen, welche Rechtsfragen der Digitalisierung in den nächsten Jahren zur Entscheidung anstehen.

I. Die Wurzeln der datenschutzrechtlichen Verfassungsjudikatur

In den frühen 1980er Jahren beschloss die Bundesregierung, das Leben in der Bundesrepublik statistisch präziser als zuvor zu erfassen. Im Rahmen einer sogenannten Volkszählung sollten die demografischen, wirtschaftlichen und sozialen Strukturen der Bundesrepublik ergründet werden. Gegen dieses Vorhaben und insbesondere die Auswertung und Speicherung der Daten durch Computer regte sich massiver öffentlicher Protest, der schließlich auch in Verfassungsbeschwerden gegen die Rechtsgrundlage des Zensus mündete, das Volkszählungsgesetz. Zwei Wochen vor Beginn der Zählung, im April 1983, stoppte das Bundesverfassungsgericht das Vorhaben in einer Eilentscheidung. Mit seinem im Dezember 1983 ergangenen »Volkszählungsurteil« legte das BVerfG schließlich den Grundstein für seine innovative Rechtsprechung im deutschen Datenschutzrecht: Dem Grundgesetz entnahm es ein neues Grundrecht – das Grundrecht auf informationelle Selbstbestimmung.

1. Das Volkszählungsurteil und das Recht auf informationelle Selbstbestimmung

Die informationelle Selbstbestimmung gewährleistet »die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«.[1] Es ist Ausdruck der Menschenwürde, dass jeder Mensch als frei denkendes und handelndes Individuum selbst entscheiden kann, welche persönlichen Daten er oder sie wem und wie überlässt.[2] Daneben leitete das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung auch aus dem Allgemeinen Persönlichkeitsrecht her, das sich wiederum aus dem im Grundgesetz verankerten Recht auf freie Persönlichkeitsentfaltung (Art. 2 Abs. 1 GG) und aus der Menschenwürdegarantie (Art. 1 Abs. 1 GG) ergibt.

Ausgangspunkt der Entscheidung war die Erkenntnis, dass die moderne automatisierte Datenverarbeitung eine unbegrenzte Speicher- und Abrufbarkeit von persönlichen Daten ermöglicht. Damit wird der Staat in die Lage versetzt, umfassende Persönlichkeitsbilder über einzelne Bürger*innen zu erstellen. Die damit einhergehenden Möglichkeiten, die eigene Bevölkerung genauestens zu kontrollieren, erkannte das BVerfG vorausschauend als große

1 BVerfGE 65, 1, 1. Leitsatz.

2 Vgl. BVerfGE 65, 1, 41f.

Gefahr für die tatsächliche Wahrnehmung von Freiheitsrechten – ein Phänomen, für das sich später die Bezeichnung *chilling effect* einbürgerte:

»Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung entsprechender Grundrechte (Art. 8, 9 GG) verzichten.«[3]

Das beeinträchtigt indes nicht nur die individuelle Freiheit, sondern die demokratische Kultur:

»Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.«[4]

Das Recht auf informationelle Selbstbestimmung entfaltet also eine doppelte Schutzwirkung: Zum einen schützt es Einzelne vor der ungewollten Preisgabe und Verarbeitung persönlicher Daten. Es ermächtigt Menschen im Grundsatz, frei über sie betreffende Daten zu verfügen. Bürger*innen sollen sich individuell und frei von psychischem Konformitätsdruck entfalten und von ihren grundgesetzlich verbrieften Freiheiten möglichst ungehemmt Gebrauch machen können.

Zum anderen aber schützt das Recht auf informationelle Selbstbestimmung damit die demokratische Kultur an sich, denn »Selbstbestimmung [ist die] elementare Funktion eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens«.[5] Das Recht auf informationelle Selbstbestimmung flankiert und erweitert so die grundrechtlich geschützte Verhaltensfreiheit und Privatheit, und zwar bereits auf der Ebene der bloßen Gefährdung.[6]

Das Urteil wirkte sich keineswegs nur auf die Volkszählung aus. Vielmehr entwickelte das Bundesverfassungsgericht an diesem Beispiel grundrechtli-

3 Ebd. Rn. 146.
4 Ebd. Rn. 146.
5 Ebd. Rn. 154
6 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 198.

che Garantien, die die Erhebung und Verarbeitung personenbezogener Daten begrenzen und die bis heute nachwirken – nicht zuletzt in der Datenschutzgrundverordnung der Europäischen Union, die maßgeblich auf der Dogmatik der informationellen Selbstbestimmung beruht. Demnach gilt jede staatliche Datenerhebung und -verarbeitung als Eingriff in das Grundrecht, der einer Rechtfertigung bedarf – entweder durch Einwilligung der Betroffenen oder durch eine hinreichend bestimmte gesetzliche Grundlage. Insbesondere muss ein solches Gesetz den Verwendungszweck der Daten begrenzen und verfahrensrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts- und Löschungspflichten der verarbeitenden Stelle vorschreiben.[7] Darüber hinaus etablierte das Urteil die Grundsätze der Datensparsamkeit und Zweckbindung, also der Beschränkung der Datenerhebung auf das für den gewünschten Zweck tatsächlich notwendige Maß. Spätestens seit dem Volkszählungsurteil gibt es kein »belangloses Datum« mehr.[8]

Mit seiner Entscheidung erfand das BVerfG zwar nicht den Datenschutz – die Sorge vor der »Verdatung« durch elektronische Datenverarbeitung lässt sich bis in die späten 1960er Jahre zurückverfolgen. Indes sensibilisierte das Gericht schon lange vor der Existenz sozialer Medien und ausschweifender Überwachungsprogramme eine breite Öffentlichkeit für die demokratische Relevanz des Datenschutzes. Im Volkszählungsurteil wurzeln bis heute wichtige Prinzipien des deutschen und europäischen Datenschutzrechts, die nicht zuletzt die Datenschutz-Grundverordnung maßgeblich prägen.

2. Die Entstehung des »Computer-Grundrechts«

Im Jahr 2008 verhandelte das Bundesverfassungsgericht über Verfassungsbeschwerden gegen das Nordrhein-Westfälische Landesverfassungsschutzgesetz. Dieses Gesetz erlaubte die sogenannte Online-Durchsuchung. Darunter versteht man den heimlichen Zugriff auf informationstechnische Systeme wie Computer, Smartphones oder Laptops mittels Infiltration durch staatliche Überwachungssoftware – sogenannte (Staats-)Trojaner.

Angesichts der digitalen Durchdringung aller Lebensbereiche erkannte das BVerfG das Gefahrenpotenzial einer Ausforschung von IT-Systemen wie insbesondere Smartphones: Die stetig zunehmende Masse immer persönlicherer Daten, die Menschen ihren Geräten anvertrauen, lässt detailliertes-

7 Vgl. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 154.
8 Vgl. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 150.

te Rückschlüsse auf deren persönliche Interessen, Neigungen, soziale, wirtschaftliche und nicht zuletzt physische wie psychische Situation zu.[9] Gleichzeitig wächst die Bedeutung solcher Informationssysteme für die individuelle Persönlichkeitsentfaltung.[10] Der im Gesetz vorgesehene heimliche Zugriff auf solche Daten geht laut BVerfG »in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen […] weit hinaus«.[11] Den bisherigen Schutz vor solchen Zugriffen im Rahmen des Rechts auf informationelle Selbstbestimmung erachtete das BVerfG daher als nicht mehr ausreichend: Komplexe Datensammlungen, wie sie etwa in einem Handy enthalten sind, lassen sich als »ausgelagertes Gehirn« der Menschen beschreiben, die das jeweilige System nutzen. Greifen Dritte auf ein solches Gerät zu, so verschaffen sie sich einen potenziell enorm weitreichenden und aussagekräftigen Datenbestand, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein.[12] Um trotz eines so umfassenden Zugriffs noch Verhaltensfreiheit und Privatheit zu garantieren, war daher der Schutz vor ungewolltem Zugriff auf IT-Systeme wie Laptops oder Smartphones insgesamt nötig – und nicht nur in Bezug auf einzelne Daten, wie sie im Fokus der informationellen Selbstbestimmung stehen.[13]

Um der besonderen Gefährlichkeit des Zugriffs auf IT-Systeme auch rechtlich gerecht zu werden, leitete das BVerfG daher aus dem Grundgesetz das neue »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« her, das auch als IT-Grundrecht oder Computer-Grundrecht bezeichnet wird. Dieses hat zwei Schutzrichtungen: Unter dem Aspekt der *Vertraulichkeit* schützt es das Interesse der an einem System Berechtigten, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben, dass also Dritte nicht Kenntnis nehmen können. Zum anderen schützt es unter dem Aspekt der *Integrität* die berechtigten Nutzer*innen eines Systems davor, dass im System gespeicherte Inhalte, Funktionen oder Leistungen durch Dritte genutzt und so ausgespäht, manipuliert oder überwacht werden können.[14]

---

9 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 178.
10 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –,Rn. 169ff.
11 BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 200.
12 Vgl. Conrad, Isabell in: Auer-Reinsdorff/Conrad (Hg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 34 Rn. 43.
13 Vgl. BVerfGE 120, 274, 313.
14 Vgl. BVerfGE 120, 274, 314.

Wie alle Grundrechte wirkt das Computer-Grundrecht jedoch nicht nur als Abwehrrecht gegen staatliche Eingriffe, in diesem Fall insbesondere durch Staatstrojaner. Vielmehr entfaltet es als Teil der Wertordnung des Grundgesetzes eine wesentlich breitere Wirkung:

Vor allem verpflichtet das Grundrecht den Gesetzgeber, die Rechtsordnung insgesamt so zu formen, dass Gefahren für die Integrität und Vertraulichkeit von IT-Systemen minimiert werden. Dieser Schutzpflicht kommt der Gesetzgeber indes bisher nur sehr eingeschränkt nach. So fehlt es an hinreichend wirksamen Anreizen – beispielsweise durch entsprechende Regelungen zur Produkthaftung –, um Hersteller von Hard- und Software zu motivieren, ihre Produkte so sicher wie eben möglich zu gestalten. Weist etwa eine verbreitete Software für E-Mail-Server eine Sicherheitslücke auf, durch die serienweise Unternehmensnetze infiltriert werden, dann verursacht das zwar bei den betroffenen Unternehmen schnell Schäden in Millionenhöhe, etwa für das »Reinigen« ihrer Infrastruktur. Für den Hersteller der schadhaften Software hat dies jedoch meist keine unmittelbaren finanziellen Folgen, vor allem weil in Allgemeinen Geschäftsbedingungen typischerweise jede Haftung für Programmierungsfehler ausgeschlossen wird. Insbesondere bei sehr verbreiteter Software sehen sich die Hersteller dann nicht veranlasst, solche Sicherheitslücken möglichst von vornherein zu vermeiden, da die hierfür notwendigen Investitionen – beispielsweise in unabhängige Sicherheits-Audits – sich bisher nicht lohnen. Müssten Software-Hersteller hingegen für die Folgen von Sicherheitslücken einstehen, so würde dies einen starken Anreiz bedeuten, mehr Wert auf Sicherheit zu legen.

Daneben entfaltet das IT-Grundrecht eine sogenannte mittelbare Drittwirkung auch in Rechtsverhältnissen zwischen Privaten. Das heißt, es verpflichtet etwa Arbeitgeber*innen zum Schutz der Daten von Arbeitnehmer*innen auf Firmenrechnern.[15]

II. Die europäische Strahlkraft des Bundesverfassungsgerichts

Neben den Garantien des Grundgesetzes stehen Rechte auf überstaatlicher Ebene, die den rechtlichen Diskurs zum Umgang mit der Digitalisierung prägen. Große Wirkung zeigen auch die Europäische Menschenrechtskonventi-

15 Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 34 Rn.46.

on (EMRK) und die EU-Grundrechtecharta (GRCh), die mit dem Inkrafttreten des Vertrages von Lissabon im Jahr 2009 geschaffen wurde.

1. Digitalisierung im Mehrebenensystem – Grundgesetz, Europäische Menschenrechtskonvention und Europäische Grundrechtecharta

Seit 1978 trifft der Europäische Gerichtshof für Menschenrechte (EGMR) wesentliche Leitentscheidungen für den Datenschutz.[16] Diese basieren vor allem auf Art. 8 der EMRK, die jedem Menschen den Schutz von Privatleben und Korrespondenz garantiert. Zwar gilt die EMRK in Deutschland nur im Rang eines einfachen Bundesgesetzes und hat keinen unmittelbaren Verfassungsrang.[17] Allerdings bettet das Grundgesetz die Bundesrepublik Deutschland in einen internationalen Verantwortungszusammenhang zur Wahrung der Menschenrechte.[18] Folgerichtig urteilte das BVerfG, dass die Entscheidungserwägungen des EGMR für deutsche Gerichte zu berücksichtigen und insofern bindend sind. Eine Abweichung von dessen Rechtsprechung muss besonders begründet werden.[19] Daher sind alle deutschen Gerichte angehalten, »solange im Rahmen geltender methodischer Standards Auslegungs- und Abwägungsspielräume eröffnet sind«[20], deutsches Recht im Einklang mit europäischem Recht auszulegen. Hierdurch entfalten die Entscheidungen des EGMR eine mittelbare Bindungswirkung. Daneben kann ein Urteil des EGMR, das eine Verletzung der Konvention feststellt, sogar die Rechtskraft einer bundesverfassungsrechtlichen Entscheidung durchbrechen und so zu dessen Revision führen.[21] So bildet auch die EMRK einen entscheidenden Maßstab für die Konkretisierung und Fortentwicklung der deutschen Grundrechte.[22]

Eine noch bedeutsamere Wirkung entfaltet die EMRK auf EU-Ebene. Denn die EU gab sich mit dem Inkrafttreten des Vertrages von Lissabon einen

16 Z.B. 1978 im Fall Klass u.a. gegen die Bundesrepublik Deutschland die durch Gesetzgeber und BVerfG bestimmten Schutzmaßnahmen, Kontrollen und Rechtsmittel bei geheimen Datenbearbeitungen bestätigt und ergänzt; Vgl. EGMR Urt. v. 6.9.1978, EuGRZ 1979, 278.

17 Herberth, Bethge in: Sachs (Hg.), GG-Kommentar, 8. Aufl., 2018, Art. 5 Rn. 6b.

18 Vgl. Art. 1 Abs. 2 GG.

19 BVerfGE 111, 307, 324.

20 BVerfGE 111, 307, 329.

21 Vgl. BVerfGE 128, 326, 36f.

22 Vgl. BVerfGE 74, 358, 370.

eigenen Grundrechtekatalog, die Europäische Grundrechtecharta (GRCh). Diese bindet alle Organe, Einrichtungen und sonstige Stellen der Union sowie Mitgliedstaaten, sobald sie Unionsrecht anwenden (Art. 51 Abs. 1 Satz 1 GRCh). Zudem gewährleistet die GRCh ein ausdifferenziertes europäisches Datenschutzgrundrecht (Art. 7, 8 GRCh).[23] Die EMRK verstärkt diesen unionsrechtlichen Datenschutz, indem sie einen Mindeststandard etabliert, der auch für die Anwendung der Unionsgrundrechte gilt (Art. 53 Abs. 3 Satz 1 GRCh).[24]

Die Rechtsprechung des BVerfG ist damit heute Teil eines Verfassungsverbundes, geprägt von nationalen Verfassungen, EMRK und Europäischer Grundrechtecharta. Die hieran von den jeweiligen Höchstgerichten entwickelten Maßstäbe bedingen und beeinflussen sich in einem judikativen Innovationsnetzwerk gegenseitig und garantieren so einen Mindeststandard. Einem datenschutzrechtlichen *race to the bottom*, also einer Entwicklung hin zu einem möglichst niedrigen Schutzniveau, wirkt die europäische Gerichtsstruktur so automatisch entgegen. Vielmehr entfalten die aufeinander bezogenen und jeweils für sich mit erheblichem Innovationspotenzial ausgestatteten Rechtsprechungen Synergieeffekte, die die Einhegung der Digitalisierung auf drei gerichtlichen Ebenen ermöglichen: durch mitgliedstaatliche Verfassungsgerichte, den EGMR und den Europäischen Gerichtshof (EuGH).

Die Rechtsprechung des BVerfG wird diesen Verfassungsverbund aber wohl auch in Zukunft erheblich beeinflussen. Denn die Europäische Grundrechtecharta (Art. 7, 8 GRCh) und die Europäische Menschenrechtskonvention (Art. 8 EMRK) knüpfen im Datenschutz an die Achtung des Privatlebens an, wohingegen das BVerfG die Datenhoheit als Voraussetzung zur individuellen Entfaltung sieht.[25] Hierdurch verlagert es den grundrechtlichen Datenschutz und damit die gerichtliche Kontrolle vor.

2. Der EuGH als Wächter der Europäischen Grundrechtecharta

Auch der EuGH war bisher vielfach mit datenschutzrechtlichen Fällen konfrontiert:

23 Vgl. Art. 8 Abs.1, Absatz 2 Satz 2, Absatz 3.
24 EuGH, Rechtssache C-528/15, Rn. 37.
25 BVerfGE 121, 1, 19.

a) Wächter im Inneren: Die Richtlinie zur Vorratsdatenspeicherung

2014 entschied der EuGH, dass die Richtlinie zur Vorratsdatenspeicherung von Verbindungsdaten (2006/24/EG) mit europäischem Recht nicht vereinbar ist. Die Richtlinie verlangte insbesondere von Telekommunikationsanbietern, anlasslos sämtliche Verbindungsdaten ihrer Kund*innen für sechs Monate bis zwei Jahre ab Zeitpunkt der Kommunikation zu speichern, vor allem Verkehrs- und Standortdaten.[26] In dieser Regelung sah der EuGH einen Eingriff »von großem Ausmaß« und von »besonders schwerwiegend[er]« Natur.[27] Dies stützte er auf vier Gesichtspunkte:

Erstens kritisierte der EuGH die personelle und kommunikationstechnische Streubreite der Normen, die sich »auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten […], ohne irgendeine Differenzierung« erstrecke sowie auf alle von ihr erfassten Daten, unabhängig davon, ob sie in irgendeinem Zusammenhang mit der öffentlichen Sicherheit stehen.[28] Zweitens enthalte die Richtlinie keine ausreichend konkreten, auf den Einzelfall bezogenen Kriterien und keine verfahrensrechtlichen Regelungen für den Zugang zu den Daten.[29] Drittens erfolge die Speicherung für mindestens sechs Monate unabhängig davon, ob die Daten tatsächlich so lange gebraucht würden.[30] Viertens würden keine ausreichenden Regelungen zur Sicherheit der gespeicherten Daten getroffen.[31]

Als besonders problematisch erachtete der EuGH die Möglichkeit, dass die Daten in Drittstaaten gespeichert werden, in denen das notwendige Schutzniveau nicht als gewährleistet angesehen werden könne[32] – ein deutlicher Verweis auf die bekannt gewordenen Enthüllungen Edward Snowdens und einen entsprechenden Datenaustausch zwischen der EU und US-Geheimdiensten. Kernthese war letztlich, dass sich eine derartige anlasslose Massenüberwachung auf das »absolut Notwendige« beschränken müsse.[33]

Das Urteil des EuGH war in mehrfacher Hinsicht revolutionär:

Inhaltlich übertrug der EuGH grundrechtliche Schutzpflichten auf den EU-Gesetzgeber. Diese Aufgabe hatte er bis dato den Mitgliedstaaten bei der

26 Vgl. Art. 5 RL 2006/24/EG.
27 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 37.
28 Ebd., Rn. 57ff., Zitat in Rn. 57.
29 Vgl. Ebd., Rn. 60ff.
30 Vgl. Ebd., Rn. 63ff.
31 Vgl. Ebd., Rn. 66ff.
32 Ebd., Rn. 68.
33 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 52.

Umsetzung der Richtlinien und damit den entsprechenden nationalen Verfassungsgerichten überlassen.[34] Infolgedessen spielt die Europäische Grundrechtecharta in der heutigen Gesetzgebungsarbeit von Kommission und Parlament eine größere Rolle. Methodisch arbeitete der EuGH wie ein selbstbewusstes nationales Verfassungsgericht. Mit der Grundrechtecharta mobilisierte er in klassisch verfassungsrechtlicher Art höherrangiges, dem einfachen Gesetzgeber nicht verfügbares »Verfassungsrecht« der EU gegen deren Sekundärrecht, also insbesondere gegen die auf Grundlage der EU-Verträge erlassenen Verordnungen und Richtlinien. Darüber hinaus gab er dem Gesetzgeber für eine rechtliche Neugestaltung konkrete legislative Instrumente vor.[35] So bekannte sich der Gerichtshof zu effektiver Grundrechtskontrolle.[36] Der EuGH bezog sich dabei erkennbar auf die Datenschutzrechtsprechung des BVerfG und des EGMR.[37]

b) Wächter nach außen: Das Privacy-Shield-Urteil 2020

Seit vielen Jahren findet ein transatlantischen Datenaustausch zwischen der EU und den USA statt – insbesondere durch US-Internetkonzerne wie Facebook und Co., aber auch durch die Datenverarbeitung zahlreicher deutscher Unternehmen, die ihre EDV zu großen Teilen in die »Cloud« verlagern, die oft durch US-Konzerne bereitgestellt wird. Bereits im eben angesprochenen Urteil zur Vorratsdatenspeicherung deutete der EuGH demgegenüber an, dass die Datenspeicherung europäischer Bürger*innen nur in Drittstaaten erfolgen könne, deren Datenschutzniveau dem europäischen entspreche.[38]

Rechtliche Grundlage dieses Datenaustausches war seit 2016 der sogenannte Privacy Shield, eine informelle Absprache zwischen der EU und den USA. Den Vorläufer »Safe Harbor« hatte der EuGH bereits 2015 für nichtig erklärt.

---

34 Vgl. Granger, Marie-Pierre/Irion, Kristina: https://www.ivir.nl/syscontent/pdfs/77.pdf vom 17.12.20, S. 24.

35 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 57-62.

36 Vgl. Classen, Clauss Dieter: »Datenschutz ja – aber wie?« in Europarecht 2014,. 441, 442.

37 Vgl. Ebd. EuR 2014, 441, 443. So decken sich die Entscheidungsgründe des EuGHs im Wesentlichen mit den Erwägungsgründen des BVerfG sowie jenen des EGMR zur Vorratsdatenspeicherung. Petri, Thomas, Urteilsanmerkung zu: »EuGH, Rechtssachen C-293/12 und C-594/12« in: Zeitschrift für Datenschutz 2014, 296, 300.

38 Vgl. EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 68. Dies verlangt auch Art. 44 DS-GVO.

Konkret stellte der EuGH fest, dass das Abkommen kein vergleichbares Schutzniveau gewährleiste. Zum einen bemängelte der EuGH einen zu weitreichenden und weitgehend unkontrollierten Zugriff der US-Behörden auf die übermittelten Daten, da im Abkommen den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der Vorrang gegenüber den Vorgaben zum Schutz der Betroffenen eingeräumt werde.[39] Konkret erlauben Section 702 des Foreign Intelligence Surveillance Act (FISA), eines US-Bundesgesetzes, sowie Executive Order 12333, ein Präsidialerlass aus der Amtszeit Ronald Reagans, den US-Geheimdiensten pauschale Überwachungsprogramme. Sie dürfen demnach auf sämtliche übermittelte Daten von Nicht-US-Bürger*innen zugreifen, die sich nicht in den USA aufhalten. Damit ist die komplette weltweite Datenverarbeitung in der »Cloud« dem Zugriff durch US-Geheimdienste ausgeliefert. Gleichzeitig ließen die Vorschriften in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung dieser Programme Einschränkungen bestehen.[40] Zum anderen kritisierte der EuGH, dass hinreichende Rechtsschutzmöglichkeiten zur Rüge und Verfolgung von Verstößen auch und gerade gegen die Vorgaben zum Grundrechtsschutz fehlen.[41]

Damit erweitert der EuGH die Rechtsschutzmöglichkeiten erheblich: Mit den Anforderungen an vertragliche Standardklauseln ordnet er wirtschaftliche Interessen klar datenschutzrechtlichen Bedenken unter und führt so seine Rolle als Wächter der Datenschutzgrundrechte in der Union fort.[42] Bemerkenswert ist auch, dass der EuGH den Privacy Shield im Urteil aufhebt, obwohl dies nicht zwingend entscheidungserheblich war.[43]

Der wohl wichtigste Aspekt dürfte aber sein, dass der EuGH zwar vordergründig nur Anforderungen an Unternehmen und Einzelpersonen in der EU definiert, damit der Sache nach aber auch über das Recht von Drittstaaten und dessen Vereinbarkeit mit europäischen Grundrechten urteilt. Hierdurch hebt der Gerichtshof den europäischen Datenschutzstandard faktisch auf eine internationale Ebene und macht ihn für alle Länder verbindlich, in die Daten aus der EU transferiert werden sollen. Mittelbar entfalten dadurch europäische Mindeststandards weltweite Wirkung. Daher ist zu erwarten,

39 Vgl. EuGH, Rechtssache C-362/14, Rn. 86ff.
40 EuGH, Rechtssache C-362/14, Rn 180ff.
41 EuGH, Rechtssache C-362/14, Rn. 89ff.
42 Vgl. verfassungsblog.de/a-groundhog-day-in-bruessels/ vom 17.12.2020.
43 Vgl. *Øe*, Schlussanträge v. 19.12.2019 – EUGH Rechtssache C-311/18, Rn. 161ff.

dass dies auch die rechtspolitische Debatte in anderen Rechtsräumen beeinflusst. Denn beispielsweise US-amerikanischen Wähler*innen dürfte kaum zu vermitteln sein, warum einheimische IT-Unternehmen die Daten von US-Bürger*innen weniger schützen müssen als jene der EU-Bürger*innen. Der öffentliche Diskurs über Datenschutz und den richtigen Umgang mit Digitalisierung wird so ein transnationaler.

Auch die Rechtssetzung durch die EU greift diese Tendenz in der Rechtsprechung des EuGH bereits auf: Kommission, Rat und insbesondere das Europäische Parlament werden den bewussten Export von grundrechtlichen Anforderungen absehbar fortsetzen und damit nicht nur EU-weit, sondern global den Rechtsrahmen für die Digitalisierung prägen. Die internationale Strahlkraft der europäischen Gesetzgebung wird sich beispielsweise auch auf Fragen der Regulierung großer Internetplattformen ausdehnen. Mit den anstehenden Gesetzesvorhaben des Digital Markets Act (DMA) und Digital Services Act (DSA) stehen bereits zwei Großprojekte in den Startlöchern, die ausdrücklich das Ziel verfolgen, einen verbindlichen Rechtsrahmen für alle Dienste zu setzen, die sich (auch) an Menschen in der Europäischen Union richten – also de facto so gut wie alle Internet-Dienste.

III. Aktuelle Herausforderungen der Gerichte und Ausblick

Auch 2020 trafen BVerfG und EuGH wegweisende Urteile.

1. Überwachung durch Geheimdienste – das BND-Urteil des BVerfG

Auch das im Mai 2020 ergangene BND-Urteil des BVerfG entfaltet internationale Wirkung. Auf Initiative der Gesellschaft für Freiheitsrechte e.V. (GFF) hatte ein Bündnis mehrerer Organisationen[44] gegen die 2016 verabschiedete Novelle des BND-Gesetzes Verfassungsbeschwerde erhoben. Das BND-Gesetz ermächtigte in der Fassung von 2016 den BND zur sogenannten strategischen Ausland-Ausland-Fernmeldeaufklärung. Darunter versteht man das anlasslose und massenweise Mitschneiden von Telekommunikationsverbindungen, beispielsweise via Glasfaserkabel oder Satellitenleitungen,

44 Neben der Gesellschaft für Freiheitsrechte waren dies der Deutsche Journalisten-Verband, die Deutsche Journalistinnen- und Journalisten-Union in ver.di, n-ost, das Netzwerk Recherche und Reporter ohne Grenzen.

und die Durchsuchung der so abgefischten Datenberge mittels sogenannter Selektoren. Der Geheimdienst nutzt Suchbegriffe, die angeblich auf Inhalte hinweisen, die für die Tätigkeit des Dienstes von Bedeutung sind. Für diese strategische Überwachung musste nach dem Gesetz weder ein konkreter Verdacht (daher führt die Bezeichnung »strategisch« in die Irre) noch eine richterliche Genehmigung vorliegen. Die BND-Überwachung konnte damit praktisch jede Person treffen.

Das BVerfG erklärte weite Teile des Gesetzes wegen Verstoßes gegen das grundrechtlich geschützte Fernmeldegeheimnis (Art. 10 Abs. 1 GG) und gegen die Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG) für verfassungswidrig. Zentrale Aussage und Errungenschaft des Urteils ist die unmissverständliche Klarstellung des BVerfG, dass Grundrechte auch für im Ausland lebende Menschen gelten und – jedenfalls soweit sie nicht explizit ausgenommen sind – auch für Ausländer*innen.[45] Weiterhin entschied das BVerfG, dass das grundgesetzliche Fernmeldegeheimnis auch Menschen schützt, die im Ausland für ausländische Personen tätig sind.[46]

Bemerkenswert umfangreich und detailliert gibt das BVerfG dem Bundesgesetzgeber Maßstäbe für eine Neuregelung des BND-Gesetzes mit. So fordert es Einschränkungen des Datenvolumens, die Sicherstellung der geografischen Begrenzung der Datensammlung[47], Regeln zur Aussortierung von Inlands- beziehungsweise Inlands-Auslandskommunikation[48], die Festschreibung konkreter und prüfbarer Überwachungszwecke[49] sowie den Schutz vertraulicher Beziehungen, beispielsweise zwischen Medien und ihren Quellen, durch eine gerichtsähnliche Ex-ante-Kontrolle.[50]

Weiterhin stellt das BVerfG klar, dass Daten nur unter hohen Auflagen an ausländische Stellen übermittelt werden dürfen. Voraussetzung ist eine Vergewisserung über deren rechtsstaatlichen Umgang mit den Daten.[51] Der BND muss sicherstellen, dass seine Informationen nicht genutzt werden, um gegen grundlegende Menschenrechte oder Völkerrecht zu verstoßen.[52] Eine automatisierte Datenweitergabe ist damit in der bisherigen Form nicht

45 BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 – 1 BvR 2835/17 –, 1. Leitsatz; Rn.94.
46 Ebd., 3. Leitsatz.
47 Ebd., Rn. 169.
48 Ebd., Rn. 170f.
49 Ebd., Rn. 175.
50 Ebd., Rn. 193f.
51 Ebd., Rn. 233ff.
52 Vgl. Ebd., Rn. 238.

mehr zulässig. Weiterer zentraler Aspekt der Entscheidung ist die umfangreiche[53] Forderung des BVerfG nach einer deutlich effektiveren Kontrolle des BND. Diese muss sich aus einer Art unabhängigem Geheimgericht und einer zusätzlichen unabhängigen Rechtskontrolle administrativen Charakters zusammensetzen.

Das BVerfG reagiert mit seinem Urteil auf das inhärente Potenzial, dass Auslandsnachrichtendienste innerstaatliche Bindungen zu umgehen versuchen.[54] Beeindruckend ist die Wirkung des Urteils: An die Stelle anlassloser weltweiter Überwachung tritt die weltweite Bindung der deutschen Staatsgewalt an Grund- und Menschenrechte. Damit setzt das Urteil neue Standards im internationalen Menschenrechtsschutz und für die Pressefreiheit. All diese Entscheidungen hätte das BVerfG nicht treffen müssen, da das Gesetz schon formell verfassungswidrig war. Es erklärte weiterhin, dass es nur »zentrale Defizite«[55] des Gesetzes festgestellt hätte, behält sich also weitere strenge Kontrollen vor. Die Entscheidung dürfte Vorbildcharakter für künftige Verfahren des EGMR haben.[56]

Das Verfahren legt so nicht nur den Grundstein für die Entwicklung einer umfassenden Nachrichtendienstkontrolle in Deutschland, sondern setzt auch einen Akzent für eine progressive, menschenrechtsfreundliche internationale Entwicklung in Richtung auf eine Verrechtlichung der Geheimdienstarbeit. Mittelfristig dürfte dies der Willkür im Geheimen arbeitender Behörden immer engere Grenzen setzen und so zugleich menschenrechtliche Standards stärken.

2. Predictive Policing – die Fluggastdatenrichtlinie vor dem EuGH

Derzeit liegt dem EuGH die Frage zur Entscheidung vor, ob die europäische Fluggastdatenrichtlinie 2016/681 mit der Grundrechtecharta vereinbar ist. Die 2016 erlassene Richtlinie verpflichtet Luftfahrtunternehmen, bei jedem Drittstaatenflug (außereuropäisch) sogenannte PNR (Passenger Name Records, Passagier-Namens-Datensätze) aller Fluggäste an die PNR-Zentralstellen der Mitgliedstaaten zu übermitteln, bei denen diese Daten automatisiert verarbeitet und dauerhaft gespeichert werden. Einen bestimmten Anlass braucht

53 Vgl. Ebd., Rn. 272ff.
54 Vgl. Ebd., Rn. 250
55 Ebd., Rn. 301
56 Vgl. Huber, Bertold: »Das BVerfG und die Auslands-Auslands-Fernmeldeaufklärung des BND« in: NvWZ-Beilage 2020, 3, 9.

es hierzu nicht. Die zu übermittelnden Datensätze umfassen neben den Namen und Adressen der Fluggäste und dem gesamten Reiseverlauf auch Angaben über ihr Gepäck, ihre Mitreisenden, alle Arten von Zahlungsinformationen sowie nicht näher definierte »allgemeine Hinweise« (ein Freitextfeld, das von der Fluggesellschaft auszufüllen ist). Die so erhobenen Daten werden sechs Monate personenbezogen und danach weitere 54 Monate pseudonymisiert gespeichert. Zusätzlich ermöglicht die Richtlinie über Umwege[57], diese Fluggastdaten an Drittstaaten für nahezu jeglichen Zweck zu übermitteln: zur Abwehr von irgendwelchen nicht näher bestimmten Gefahren, zur Geltendmachung irgendwelcher Rechtsansprüche und so weiter.

Die Verabschiedung dieser Richtlinie erscheint aus mehreren Gründen unverständlich. So bescheinigte ein EuGH-Gutachten bereits dem zum PNR-Abkommen zwischen der EU und Kanada die Grundrechtswidrigkeit. Grund hierfür waren das ebenfalls im Abkommen vorgesehene Freitextfeld,[58] der fehlende Schutz vor Weitergabe der PNR-Daten durch kanadische Behörden an Drittstaaten[59] und die vorgesehene fünfjährige Speicherdauer[60] – allesamt Bestimmungen, die die neue Richtlinie ungeachtet der klaren Vorgaben des EuGH wieder enthält.

Das deutsche Umsetzungsgesetz der Richtlinie, das Fluggastdatengesetz, geht nichtsdestotrotz sogar über die EU-Richtlinie hinaus. Es erfasst nicht nur Drittlandflüge, sondern auch unionsinterne. Darüber hinaus soll das Bundeskriminalamt die PNR-Daten mittels automatisierter Mustererkennung mit Polizeidatenbanken abgleichen und so verdächtige Flugbewegungen erkennen. Hier werden also erste Formen algorithmischer Verdachtsgewinnung, des sogenannten Predictive Policing, eingeführt. Diese Technik, bei der mit vorab festgelegten Kriterien Daten abgeglichen werden, soll die Gefährlichkeit von Menschen anhand von alltäglichen Daten beurteilen, die keinen Bezug zu einer konkreten Straftat haben. Die davon betroffenen Menschen werden allein durch algorithmische Berechnungen als

57 Vgl. Art. 11 Abs. 1 lit. a) Detaillierte Erläuterung: VG Wiesbaden, Beschluss vom 13.5.2020 – 6 K 805/19.WI, Rn. 96-98.

58 EuGH, Gutachten vom 26.7.2017 – Gutachten (Avis) 1/15, Rn. 160.

59 Ebd., Rn. 215.

60 Ebd., Rn. 206.

potenzielle Gefahrenquelle behandelt. Dies widerspricht grundlegend dem in der Europäischen Grundrechtecharta formulierten Menschenbild.[61]

Insgesamt sind die PNR-Richtlinie und deren deutsches Umsetzungsgesetz ein legislativer Frontalangriff auf die Grundrechte aller Unionsbürger*innen und auf die bisherige EuGH-Rechtsprechung. Es ist daher damit zu rechnen, dass der EuGH die Richtlinie für nichtig erklären wird, so wie er bereits das Abkommen mit Kanada kippte. Ein von der GFF initiiertes Verfahren gegen die Speicherung von PNR in Deutschland wurde bereits dem EuGH zur Vorabentscheidung vorgelegt. Besondere Aufmerksamkeit verdient nun, welche Ausführungen der EuGH zur algorithmischen Verdachtsgewinnung machen wird.

3. EUGH zu Uploadfilter

Auf eine Nichtigkeitsklage Polens gegen Bestimmungen der Urheberrechtsrichtlinie hin verhandelt der EuGH derzeit spannende Fragen im Konfliktfeld von Meinungs- und Informationsfreiheit einerseits und dem Schutz des geistigen Eigentums andererseits. Kern des Rechtsstreits sind dabei Verfahren zur technischen Filterung von Inhalten. Beispielsweise durch sogenannte Uploadfilter, die vermeintlich rechtswidrige hochgeladene Inhalte gar nicht erst online stellen, und die Frage, ob Überwachungspflichten für Betreiber von Online-Plattformen entstehen.

Der Europäische Gerichtshof (EuGH) prüft insbesondere die Vereinbarkeit einiger Bestimmungen des Artikels 17 der Urheberrechtsrichtlinie mit der EU-Grundrechtecharta.[62] Die polnische Regierung rügt, dass die angefochtenen Bestimmungen den Einsatz von Uploadfiltern vorschreiben. Dies verstoße gegen das in Art. 11 der EU-Grundrechtecharta verankerte Recht auf Meinungs- und Informationsfreiheit.

Der Prüfungsmaßstab des Gerichtshofs ist jedoch nicht auf die Prüfung der explizit gerügten Grundrechtverletzte beschränkt.[63] Es ist vielmehr damit

61 Vgl. http://freiheitsrechte.org/home/wp-content/uploads/2020/09/GFF-Stellungnahme-an-den-EuGH-zur-FluggastdatenspeicherungPNR-Richtlinie-2020.pdf vom 17.12.2020, S. 2.

62 Fall C-401/19 – Republik Polen v Europäisches Parlament und Rat der Europäischen Union.

63 Vgl. Reda, Julia/Selinger, Joschka/Servatius, Michael: Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment. Kapi-

zu rechnen, dass der Gerichtshof eine umfassende Abwägung aller betroffenen Grundrechte mit dem Recht auf geistiges Eigentum (Art. 17 Abs. 2 GRCh) vornehmen wird. In der mündlichen Verhandlung zu dem Verfahren im November 2020 hat der Gerichtshof insbesondere die Frage aufgeworfen, ob Artikel 17 zur Einführung allgemeiner Überwachungspflichten führt.[64] Solche Überwachungspflichten sind nach der Rechtsprechung des Gerichtshofs unzulässig, da sie neben dem Recht auf Meinungs- und Informationsfreiheit (Art. 11 GRCh) auch den Schutz personenbezogener Daten der Nutzer*innen (Art. 7 GRCh) sowie die unternehmerische Freiheit der Plattformunternehmen (Art. 16 GRCh) verletzen.

Der EuGH stellte in der mündlichen Verhandlung zudem darauf ab, ob der Europäische Gesetzgeber ausreichende verfahrensrechtliche Schutzvorkehrungen für den Eingriff in die Grundrechte in Artikel 17 vorgesehen hat. So enthält Artikel 17 die abstrakte Vorgabe, dass legale Inhalte nicht beeinträchtigt werden. Die EU-Institutionen argumentieren, diese Vorschrift stelle sicher, dass nur offensichtlich rechtswidrige Inhalte gesperrt werden. Tatsächlich gibt Artikel 17 aber keine Anhaltspunkte, wie die automatische Sperrung legaler Inhalte in der Praxis verhindert werden soll. Es ist also durchaus plausibel anzunehmen, dass die Regelung an der Unbestimmtheit ihrer grundrechtlichen Schutzvorkehrungen scheitern könnte.[65]

IV. Chancen und Grenzen des Rechts – warum Gerichte digitale Zukunft mitgestalten (müssen)

Wie die genannten Beispiele zeigen, sind Gerichte ein machtvolles Instrument, um Grundrechtsverletzungen im digitalen Raum effektiv zu begegnen, die insbesondere durch staatliche Massenüberwachung und das ungeregelte Sammeln von Daten entstehen. In der EU bieten dabei drei Ebenen rechtlichen Schutz: der EGMR auf völkerrechtlicher, der EuGH auf europarechtlicher und die Verfassungsgerichte auf nationaler Ebene. Diese Gerichte ha-

---

tel 2. https://freiheitsrechte.org/home/wp-content/uploads/2020/11/GFF_Article17_Fundamental_Rights.pdf

64 Vgl. Reda, Julia: In zwei Stunden von Luxemburg nach Brüssel spazieren: Der Europäische Gerichtshof wird über die Legalität von Uploadfiltern urteilen. Verfassungsblog. https://verfassungsblog.de/in-zwei-stunden-von-luxemburg-nach-brussel-spazieren/

65 Husovec, Martin: Over-Blocking: When is the EU Legislator Responsible? 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149

ben sich als innovative und im Grundsatz auch willige Verteidiger der Freiheitsrechte erwiesen, die in ihrer Rechtsprechung nicht nur aktuelle Gefahren einhegen, sondern auch vorausschauend Maßstäbe zur Unterbindung künftiger Grundrechtsverletzungen setzen und Rechtsschutzmöglichkeiten stärken. Dabei sind sie auch durchaus bereit, über den eigentlichen Fall hinaus Grundsatzfragen zu entscheiden – wie etwa das BVerfG im BND-Urteil oder der EuGH beim Privacy Shield. Die Gerichte greifen dabei wechselseitig auf die grundrechtlichen Erkenntnisse anderer Gerichte zurück und können daher die Gestaltung der Digitalisierung in grundrechtfreundlichere Richtungen weisen als es die Legislative mitunter vermag.

Zweifellos setzen Obergerichte dem Gesetzgeber und damit letztlich auch der Exekutive langfristig Grenzen. So heikel die mitunter drastischen Korrekturen gegenüber der Legislative aus einer demokratietheoretischen Perspektive sein mögen – der Fehler ist nicht in der Rechtsprechung zu suchen. Im Gegenteil, die systematische Unterbelichtung individueller Freiheiten seitens der Legislative im Namen strukturell nicht einzulösender Sicherheitsversprechen, zwingt die Judikative oft genug in eine aktivere Rolle, die sie dann wiederum konservativer Kritik aussetzt. In Wahrheit sind Gerichte in solchen Verfahren jedoch nur Lackmustest und zugleich Therapie legislativer Fehlsteuerungen, aber keineswegs selbst kritikwürdige Akteure oder gar *judicial activists*.

Dabei erstreckt sich der gerichtliche Schutz immer häufiger über das Unions- beziehungsweise Bundesgebiet hinaus. Insbesondere in dieser transnationalen Dimension europäischer Rechtsprechung liegt ein Potenzial, die Digitalisierung fair und grundrechtsfreundlich zu gestalten. Gesellschaftliche Debatten um Datenschutz können so von europäischen Gerichten ausgehend insbesondere in die USA getragen werden und beeinflussen damit zentrale Diskurse des 21. Jahrhunderts. Wenn sie Eingang in die Rechtsprechung des EGMR finden, gelten sie weit über die Grenzen der europäischen Union hinaus auch etwa in Russland, Georgien, Armenien, Aserbaidschan und anderen Ländern.

Die Gerichte können so einen wichtigen Beitrag dazu leisten, Freiheitsrechte in der digitalen Welt zu sichern und auszubauen. Hierfür müssen sie aber mit akribisch vorbereiteten strategischen Klagen mobilisiert werden. Dieser für die effektive Geltung von Grund- und Menschenrechten elementaren Aufgabe haben sich spezialisierte Nichtregierungsorganisationen unter dem Stichwort der strategischen Prozessführung verschrieben.

Gleichzeitig bleiben zentrale Fragen der rechtlichen Regelung der Digitalisierung bisher ungelöst und stellen sowohl die Legislative als auch die Rechtsprechung vor große Herausforderungen. So wird die Einwilligung, unter anderem bekannt als allgegenwärtige *Cookie-Banner*, als in der Theorie optimaler Ausdruck informationeller Selbstbestimmung zunehmend zur Fiktion: Viele Dienste, auf die die Menschen in der digitalen Gesellschaft nur unter großen sozialen oder beruflichen Kosten verzichten können, lassen sich Blankoschecks zum Umgang mit personenbezogenen Daten ausstellen – weil sie es können, und weil Einzelne jedenfalls subjektiv keine andere Wahl haben als zuzustimmen. Hier werden Gesetzgeber und Gerichte bestimmten »Einwilligungen« die rechtliche Anerkennung versagen müssen, so wie sich vor Jahrzehnten eine Rechtsprechung zur Inhaltskontrolle von Allgemeinen Geschäftsbedingungen (AGB) herausgebildet hat, die besonders krasse Klauseln im Kleingedruckten für unwirksam hält. Diese Regeln wiederum hat der Gesetzgeber schließlich erweitert, systematisiert und ins Bürgerliche Gesetzbuch übernommen. Eine ähnliche Form der »AGB-Kontrolle« wird auch im Bereich der Einwilligungen in die Datenverarbeitung erforderlich sein.

Strukturell ähnliche Probleme zeigen sich im Bereich der IT-Sicherheit, wo Einzelne meist nicht über die Marktmacht verfügen, mehr Investitionen von IT-Unternehmen in *security by default* (höchsten Sicherheitseinstellungen ab Werk) zu erzwingen. Gerichte und Gesetzgeber hingegen können die richtigen Anreize setzen, damit sich Investitionen in Sicherheit für Hersteller von Hard- und Software wirklich lohnen, indem sie Ansprüche auf Schadensersatz im Falle von Sicherheitsvorfällen deutlich erweitern. Und dies sind nur zwei der besonders heiklen Problemfelder.

Es ist nicht selbstverständlich, dass das Grundgesetz sowie die Grundrechtsquellen auf europäischer Ebene tatsächlich die Gefahren der Digitalisierung einhegen können. Wenn dies aber gelingt, so haben wir dies engagierten und innovativen Jurist*innen zu verdanken – bei den europäischen Gerichten, aber auch bei den Organisationen, die den Gerichten möglichst gut aufbereitete Rechtsfragen zur Entscheidung vorlegen.