

2. Kapitel: Ursachen und Hintergründe des Konflikts

A. Regulierung des Datenschutzes

Wesentliche Ursache für den Konflikt zwischen der Discovery und deutschem Datenschutzrecht ist das unterschiedliche Regulierungsverständnis Deutschlands und der USA auf dem Gebiet des Datenschutzes. In diesem Abschnitt werden die Datenschutzmodelle Deutschlands (I.) und der USA (II.) zunächst veranschaulicht und anschließend gegenübergestellt (III.).

I. Deutschland

1. Ausprägungen des allgemeinen Persönlichkeitsrechts

In Deutschland ist der Datenschutz verfassungsrechtlich verankert. Die meisten Bundesländer garantieren in ihren Verfassungen ausdrücklich ein Grundrecht auf Datenschutz.³⁴ Das Grundgesetz (GG) sieht kein eigenständiges Grundrecht auf Datenschutz vor. Allerdings leitete das BVerfG bereits 1969 im Mikrozensus-Beschluss aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein Selbstbestimmungsrecht des Einzelnen im Hinblick auf Informationen aus der Intimsphäre und solche mit Geheimnischarakter ab.³⁵ Im Volkszählungsurteil von 1983 formulierte das BVerfG schließlich grundsätzliche Vorgaben für den Datenschutz.³⁶ Das allgemeine Persönlichkeitsrecht beinhalte ein umfassendes Recht auf informationelle Selbstbestimmung. Danach sei der Betroffene befugt, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. In den Schutzbereich falle jedes personenbezogene Datum, da es unter den Bedingungen der automatisierten Datenverarbeitung kein „belangloses“ Datum gebe. Die automatisierte Datenverarbeitung ermögliche es, personenbezogene Daten zu einem Persönlichkeitsbild zusammenzufügen, ohne dass der Betroffene dessen Richtigkeit und Verwendung hinreichend kontrollieren könne. Zugleich wies das BVerfG aber darauf hin, dass das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet sei.³⁷ Der Betroffene müsse Einschränkungen im überwiegenden Allgemeininteresse hinnehmen.

Das BVerfG betont seit jeher die Entwicklungsoffenheit des allgemeinen Persönlichkeitsrechts in Bezug auf den technischen und gesellschaftlichen Fortschritt.³⁸ In seinem Urteil zur Online-Durchsuchung erkannte das BVerfG 2008 als weitere Ausprägung des allge-

³⁴ Berlin: Art. 33; Brandenburg: Art. 11; Bremen: Art. 12 Abs. 3; Mecklenburg-Vorpommern: Art. 6 Abs. 1; Nordrhein-Westfalen: Art. 4 Abs. 2; Rheinland-Pfalz: Art. 4a; Saarland: Art. 2 Satz 2; Sachsen: Art. 33; Sachsen-Anhalt: Art. 6 Abs. 1; Thüringen: Art. 6 Abs. 2.

³⁵ BVerfGE 27, 1, 6 ff.

³⁶ BVerfGE 65, 1, 41 ff.

³⁷ BVerfGE 65, 1, 43 ff.

³⁸ BVerfGE 54, 148, 153 f.; später auch: BVerfGE 72, 155, 170; 79, 256, 268.

meinen Persönlichkeitsrechts das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme an.³⁹ Der Schutzbereich erfasse Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten in einem Umfang und in einer Vielfalt enthalten können, sodass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“.⁴⁰ Als Beispiele nannte das BVerfG Computer, Mobiltelefone und elektronische Terminkalender.⁴¹

Direkte Wirkung entfalten die datenschutzrechtlichen Ausprägungen des allgemeinen Persönlichkeitsrechts lediglich gegenüber dem Staat.⁴² Dennoch werden sie zugleich bei der privaten Datenverarbeitung berücksichtigt. Aus dem allgemeinen Persönlichkeitsrecht folgen staatliche Schutzpflichten.⁴³ Der Gesetzgeber hat dafür zu sorgen, dass der Betroffene auch bei Eingriffen privater Datenverarbeiter geschützt ist.⁴⁴ Die Gerichte müssen das allgemeine Persönlichkeitsrecht bei der Anwendung zivilrechtlicher Normen im Sinne mittelbarer Drittwirkung als Auslegungsmaßstab beachten.⁴⁵ Überdies genießt das allgemeine Persönlichkeitsrecht deliktsrechtlichen Schutz nach § 823 Abs. 1 des Bürgerlichen Gesetzbuches (BGB).⁴⁶ Bei einem Eingriff kann der Betroffene mithin Schadensersatz- und Unterlassungsansprüche geltend machen.

2. *BDSG als allgemeines Datenschutzgesetz*

Deutschland reagierte auf die Gefahren der automatisierten Datenverarbeitung bereits früh mit Gesetzgebungsmaßnahmen. Am 30. September 1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz.⁴⁷ In den folgenden Jahren erließen die übrigen Bundesländer ebenfalls Datenschutzgesetze.⁴⁸ Am 1. Januar 1978 trat sodann das BDSG in Kraft.⁴⁹ Das

³⁹ BVerfGE 120, 274, 274 ff. Gegenstand der Verfassungsbeschwerden war § 5 Abs. 2 Nr. 11 des Verfassungsschutzgesetzes NRW, der das heimliche Beobachten des Internets und den heimlichen Zugriff auf informationstechnische Systeme gestattet. Dazu: Luch, MMR 2011, 75, 75 ff.; Kutscha, NJW 2008, 1042, 1042 ff.; Roßnagel/Schnabel, NJW 2008, 3534, 3534 ff.

⁴⁰ BVerfGE 120, 274, 314.

⁴¹ BVerfGE 120, 274, 314.

⁴² Vgl. Art. 1 Abs. 3 GG.

⁴³ BVerfGE 117, 202, 227; 96, 56, 62 ff.; Di Fabio in Maunz/Dürig, GG, Art. 2 Rn. 189; Buchner, Informationelle Selbstbestimmung, S. 51 ff.

⁴⁴ Masing, NJW 2012, 2307, 2307 f.

⁴⁵ BVerfGE 84, 192, 194 ff.; BAG, NJW 1986, 85, 86 f.; Di Fabio in Maunz/Dürig, GG, Art. 2 Rn. 191; Wente, NJW 1984, 1446, 1446 f.

⁴⁶ BGH, NJW 2004, 762, 765; DtZ 1994, 343, 344; Sprau in Palandt, BGB, § 823 Rn. 84 ff. Zum deliktsrechtlichen Schutz des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme: Roßnagel/Schnabel, NJW 2008, 3534, 3535 f.

⁴⁷ GVBl. I 1970, 625.

⁴⁸ Zu den Landesdatenschutzgesetzen: Simitis in Simitis, BDSG, Einleitung, Rn. 1; Gola, MDR 1980, 181, 181 ff.

BDSG wurde von Anfang an als allgemeines Datenschutzgesetz konzipiert, das sowohl die Datenverarbeitung durch öffentliche als auch durch nicht-öffentliche Stellen regelt. Das BDSG schützt den Einzelnen davor, dass er durch den Umgang mit personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.⁵⁰ Die geschützten Personen bezeichnet das BDSG als „Betroffene“.⁵¹ Zentrale Bedeutung kommt im BDSG dem Begriff der „personenbezogenen Daten“ zu. Darunter fallen nach § 3 Abs. 1 BDSG sämtliche Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person. Erhöhter Schutz gilt für besondere Arten personenbezogener Daten, sogenannte „sensible Daten“.⁵² Dies sind nach § 3 Abs. 9 BDSG Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Ausgangspunkt des Schutzkonzeptes ist das Verbot mit Erlaubnisvorbehalt in § 4 Abs. 1 BDSG. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene einwilligt. Die Zulässigkeitstatbestände des BDSG basieren auf dem Grundsatz der Zweckbindung.⁵³ Verantwortliche Stellen dürfen personenbezogene Daten grundsätzlich allein für den Zweck ihrer Erhebung verarbeiten. Dies soll verhindern, dass personenbezogene Daten beliebig in Datensammlungen zusammengeführt und ausgewertet werden.⁵⁴ Ergänzt wird der Grundsatz der Zweckbindung durch den Grundsatz der Erforderlichkeit.⁵⁵ Demgemäß ist die Datenverarbeitung nur zulässig, soweit es für den jeweiligen Zweck erforderlich ist. § 3a BDSG konkretisiert den Grundsatz der Erforderlichkeit durch die Grundsätze der Datenvermeidung und Datensparsamkeit. Demzufolge ist möglichst von Methoden zur Anonymisierung und Pseudonymisierung Gebrauch zu machen.⁵⁶ Das BDSG verlangt eine weitgehende Transparenz der Datenverarbeitung, indem es Informationspflichten der verantwortlichen Stelle und Auskunftsrechte des Betroffenen statuiert.⁵⁷ Darüber hinaus garantiert das BDSG dem Betroffenen die Rechte auf Widerspruch sowie Berichtigung, Löschung oder Sperrung seiner

⁴⁹ Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977, BGBl. I, S. 201; zuletzt geändert durch: Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl. I, S. 2814.

⁵⁰ § 1 Abs. 1 BDSG.

⁵¹ § 3 Abs. 1 BDSG.

⁵² Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 166; Schaffland/Wiltfang, BDSG, § 3 Rn. 107; Seifert in Simitis, BDSG, § 32 Rn. 63 und 70; Scholz/Sokol in Simitis, BDSG, § 13 Rn. 33. Teilweise wird auch der Begriff „sensitive Daten“ verwendet (so z.B. Simitis in Simitis, BDSG, § 3 Rn. 250 ff.).

⁵³ Siehe: §§ 14 Abs. 1, 28 Abs. 1 BDSG.

⁵⁴ Vgl. von Zezschwitz in Roßnagel, Handbuch Datenschutzrecht, Kap. 3.1 Rn. 1, S. 221.

⁵⁵ Siehe: §§ 14 Abs. 1, 15 Abs. 1, 16 Abs. 1 Nr. 1, 28 Abs. 1, Abs. 2, Abs. 3 Satz 2, Abs. 6, Abs. 7, Abs. 8 und Abs. 9 BDSG.

⁵⁶ § 3a Satz 2 BDSG.

⁵⁷ Siehe etwa: §§ 4 Abs. 3 Satz 1, 33 und 34 BDSG.

Daten.⁵⁸ Fügt die verantwortliche Stelle dem Betroffenen durch eine unzulässige Datenverarbeitung schuldhaft Schaden zu, ist sie nach § 7 Abs. 1 BDSG zum Schadensersatz verpflichtet.⁵⁹

Um die Einhaltung der Datenschutzvorschriften zu gewährleisten, sieht das BDSG ein doppeltes Kontrollsystem bestehend aus Selbst- und Fremdkontrolle vor. Die Selbstkontrolle wird von behördlichen bzw. betrieblichen Beauftragten für den Datenschutz ausgeübt.⁶⁰ Die Fremdkontrolle ist zwischen Bund und Ländern aufgeteilt. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert und berät Bundesbehörden, öffentliche Stellen des Bundes sowie Telekommunikations- und Postdienstunternehmen.⁶¹ Den Ländern obliegt die Aufsicht über nicht-öffentliche Stellen, Landesbehörden und sonstige Landesstellen. Die Aufsicht übernimmt entweder das Landesinnenministerium⁶² oder ein speziell ernannter Landesdatenschutzbeauftragter⁶³. Für die Durchsetzung des Datenschutzrechts stehen den Aufsichtsbehörden nach § 38 Abs. 5 BDSG Anordnungs- und Untersagungsbefugnisse zu. Verstöße können gemäß § 43 Abs. 3 Satz 1 BDSG als Ordnungswidrigkeit mit einem Bußgeld von bis zu 300.000,00 Euro oder nach § 44 Abs. 1 BDSG als Straftat mit einer Freiheitsstrafe von bis zu zwei Jahren sanktioniert werden. Übersteigt der wirtschaftliche Vorteil, den die verantwortliche Stelle aus der Ordnungswidrigkeit gezogen hat, die vorgesehenen Beträge, können nach § 43 Abs. 3 Satz 3 BDSG höhere Bußgelder verhängt werden. Hinzu kommen für die verantwortliche Stelle die mit Datenschutzskandalen verbundenen Reputationsschäden.⁶⁴

3. Harmonisierung durch die EG-Datenschutzrichtlinie

Anfang der 1990er Jahre verfügten in der Europäischen Union neben Deutschland auch Frankreich, Luxemburg, die Niederlande, Dänemark, Irland und das Vereinigte Königreich über Datenschutzgesetze. Die übrigen Mitgliedstaaten hatten noch keine Datenschutzgesetze erlassen. Das Schutzniveau war mithin in der Europäischen Union sehr unterschiedlich, worin ein Handelshemmnis gesehen wurde.⁶⁵ Aus diesem Grund schaltete sich der europäische Gesetzgeber ein. Am 24. Oktober 1995 verabschiedete die Europäische Kommission (EU-

⁵⁸ §§ 6 Abs. 1, 19, 20, 35 BDSG.

⁵⁹ Für öffentliche Stellen enthält § 8 Abs. 1 BDSG zusätzlich eine Gefährdungshaftung.

⁶⁰ § 4f BDSG.

⁶¹ § 24 BDSG, § 115 Abs. 4 TKG, § 42 Abs. 3 PostG.

⁶² So in Baden-Württemberg, Brandenburg, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Thüringen.

⁶³ So in Berlin, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein.

⁶⁴ Dazu: Scherer, MMR 2008, 433, 434; Bull, ZRP 2008, 233, 233; Kutscha, ZRP 2010, 112, 112.

⁶⁵ Wuermeling, Handelshemmnis Datenschutz, S. 6.

Kommission) die EG-Datenschutzrichtlinie (DSRL).⁶⁶ Die DSRL gilt für alle Mitgliedstaaten der Europäischen Union sowie für Island, Liechtenstein und Norwegen als Mitgliedstaaten des Europäischen Wirtschaftsraumes (EWR).⁶⁷ Die DSRL hat eine doppelte Schutzrichtung: Zunächst bezweckt sie den Schutz der Privatsphäre.⁶⁸ Zusätzlich soll sie die unterschiedlichen Datenschutzstandards in den Mitgliedstaaten ausgleichen und einen freien Datenverkehr im Binnenmarkt sicherstellen.⁶⁹ In der Folgezeit setzten alle Mitgliedstaaten die DSRL in nationales Recht um. Auch das BDSG wurde im Zuge der Umsetzung der DSRL novelliert⁷⁰ und ist deshalb richtlinienkonform auszulegen⁷¹.

Inhaltlich knüpft die DSRL an die Datenschutzkonvention des Europarates vom 1. Oktober 1981 an.⁷² Sämtliche Regelungen der DSRL gelten gleichermaßen für den öffentlichen und den nicht-öffentlichen Bereich. Art. 7 DSRL enthält ebenso wie § 4 Abs. 1 BDSG ein Verbot mit Erlaubnisvorbehalt. Die Mitgliedstaaten dürfen die Verarbeitung personenbezogener Daten nur dann gestatten, wenn der Betroffene gemäß Art. 7 a) DSRL einwilligt oder ein Zulässigkeitstatbestand nach Art. 7 b) bis f) DSRL eingreift. Die Verarbeitung sensibler Daten ist gemäß Art. 8 Abs. 1 DSRL grundsätzlich zu untersagen. Ausnahmen sind lediglich in den Fällen des Art. 8 Abs. 2 bis 5 DSRL zulässig. Zudem müssen die Mitgliedstaaten folgende in Art. 6 Abs. 1 DSRL geregelte Datenschutzgrundsätze gewährleisten: (1) die Datenverarbeitung nach Treu und Glauben, (2) den Grundsatz der Zweckbindung, (3) den Grundsatz der Datenverhältnismäßigkeit sowie (4) den Grundsatz der Datenqualität. Nach Art. 10 und 11 DSRL ist im Sinne der Transparenz sicherzustellen, dass die verantwortliche Stelle den Betroffenen über die Einzelheiten der Datenverarbeitung informiert. Ferner ist dem Betroffenen nach Art. 12 DSRL ein Auskunfts-, Berichtigungs- und Löschungsrecht sowie gemäß Art. 14 DSRL ein Widerspruchsrecht einzuräumen. Bei rechtswidrigen Datenverarbeitungen müssen die Mitgliedstaaten dem Betroffenen nach Art. 23 Abs. 1 DSRL außerdem ein Recht auf Schadensersatz gegenüber der verantwortlichen Stelle gewähren. Für

⁶⁶ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr vom 24. Oktober 1995, ABl. L 281, S. 31.

⁶⁷ Beschluss des Gemeinsamen EWR-Ausschusses Nr. 83/1999 zur Änderung des Protokolls 37 und des Anhangs IX zum EWR-Abkommen vom 25. Juni 1999, ABl. L 296, S. 41.

⁶⁸ Art. 1 Abs. 1 DSRL; Erwägungsgrund 10 DSRL.

⁶⁹ Art. 1 Abs. 2 DSRL; Erwägungsgründe 7 bis 9 DSRL.

⁷⁰ Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001, BGBl. I S. 904. Dazu: Tinnefeld, NJW 2001, 3078, 3078 ff.

⁷¹ Die Pflicht zur richtlinienkonformen Auslegung folgt aus dem Umsetzungsgebot des Art. 288 Abs. 3 AEUV und dem Grundsatz der loyalen Zusammenarbeit des Art. 4 Abs. 3 EUV. Vgl. EuGH, Rs. 14/83, Slg. 1984, 1891, Rn. 26 - von Colson und Kamann/Land Nordrhein-Westfalen; ebenso: EuGH, Rs. C-106/89, Slg. 1990, I-4135, Rn. 8 - Marleasing; Rs. C-91/92, Slg. 1994, I-3325, Rn. 26 - Faccini Dori. Dazu: Ruffert in Calliess/ Ruffert, EUV/AEUV, Art. 288 AEUV Rn. 77 ff.

⁷² Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, BGBl. 1985 II, S. 539.

Datenübermittlungen in Drittländer bestimmt die DSRL ein einheitliches Vorgehen: Nach Art. 25 Abs. 1 DSRL sind Datenübermittlungen zulässig, wenn das Drittland ein angemessenes Schutzniveau gewährleistet. Fehlt es daran, dürfen die Mitgliedstaaten Datenübermittlungen nur unter den engen Voraussetzungen der Ausnahmetatbestände des Art. 26 DSRL gestatten.

4. *Europäisches Grundrecht auf Datenschutz*

Bereits in der Vergangenheit erkannte der Europäische Gerichtshof (EuGH) das Grundrecht auf Datenschutz als Teil der ungeschriebenen allgemeinen Rechtsgrundsätze an.⁷³ Dazu zog er die Verfassungstraditionen der Mitgliedstaaten und das in Art. 8 Europäische Menschenrechtskonvention (EMRK) geregelte Recht auf Schutz des Privatlebens als Rechtserkenntnisquellen heran. Seit Inkrafttreten des Vertrages von Lissabon am 1. Dezember 2009 verfügt die Europäische Union mit der Grundrechte-Charta (GRCh) über einen geschriebenen Grundrechtskatalog.⁷⁴ Art. 8 Abs. 1 GRCh sieht ausdrücklich ein Grundrecht auf Datenschutz vor.⁷⁵ Danach hat jede Person das Recht auf Schutz sie betreffender personenbezogener Daten. Gemäß dem in Art. 8 Abs. 2 Satz 1 GRCh geregelten Verbot mit Erlaubnisvorbehalt dürfen personenbezogene Daten allein nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer gesetzlichen legitimen Grundlage verarbeitet werden. Nach Art. 8 Abs. 2 Satz 2 GRCh hat jede Person zudem das Recht, Auskunft über sie betreffende personenbezogene Daten zu erhalten und deren Berichtigung zu erwirken.

In erster Linie begründet Art. 8 GRCh ein Abwehrrecht gegenüber den Organen der Europäischen Union und den Mitgliedstaaten bei der Durchführung von Unionsrecht.⁷⁶ Auf private Datenverarbeiter ist Art. 8 GRCh nicht unmittelbar anwendbar.⁷⁷ Allerdings folgt aus Art. 8 GRCh eine Schutzpflicht des Unionsgesetzgebers zum Erlass entsprechenden Sekundärrechts.⁷⁸ Dieser Pflicht kam der Unionsgesetzgeber mit der DSRL nach. Die DSRL konkretisiert mithin das Grundrecht auf Datenschutz und ist im Lichte des Grundrechts auszulegen.⁷⁹ Der EuGH zieht das Grundrecht daher bei privatrechtlichen Sachverhalten zur

⁷³ EuGH, Rs. 29/69, Slg. 1969, 419 - Stauder; ebenso: EuGH, Rs. C-404/92 P, Slg. 1994, 4780, Rn. 17 - Aids-Test; Rs. C-369/98, Slg. 2000, I-6751, Rn. 32 ff. - Fisher; Rs. C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Rn. 39 ff. und 69 ff. - Österreichischer Rundfunk; Rs. C-101/01, Slg. 2003, I-12971, Rn. 86 ff. - Lindqvist.

⁷⁴ Charta der Grundrechte der Europäischen Union vom 14. Dezember 2007, ABl. C 303, S. 1.

⁷⁵ Zur Diskussion des Art. 8 GRCh im Grundrechtekonvent: Bernsdorff in Meyer, Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 5 ff.

⁷⁶ Vgl. Art. 51 Abs. 1 GRCh.

⁷⁷ Jarass, Charta der Grundrechte der Europäischen Union, Art. 8 Rn. 3.

⁷⁸ Streinz/Michl, EuZW 2011, 384, 386 f.

⁷⁹ EuGH, Rs. C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Rn. 68 ff. - Österreichischer Rundfunk. Die Mitgliedstaaten sind bei der Auslegung nationaler Umsetzungs Vorschriften ebenfalls an Art. 8 GRCh

Interpretation der DSRL heran.⁸⁰ Auf diese Weise entfaltet das Grundrecht zwischen Privaten mittelbare Drittwirkung.⁸¹

5. Reform des europäischen Datenschutzrechts

Aufgrund des schnellen technologischen Fortschritts und der daraus erwachsenden Herausforderungen für den Datenschutz plant die EU-Kommission gegenwärtig eine Reform des europäischen Datenschutzrechts.⁸² Ziel ist die Schaffung eines umfassenden und kohärenteren Konzepts für das Grundrecht auf Datenschutz. Am 25. Januar 2012 veröffentlichte die EU-Kommission als Teil der geplanten Reform einen Vorschlag für eine Datenschutz-Grundverordnung (DS-GVO), der die Grundsätze der DSRL konkretisiert und erweitert.⁸³ Die Vertreter der Mitgliedstaaten brachten in der Folgezeit zahlreiche Bedenken gegen den Vorschlag vor.⁸⁴ Am 21. Oktober 2013 nahm das Europäische Parlament im Innen- und Justizausschuss einen Standpunkt mit einem überarbeiteten Entwurf an und bestätigte diesen am 12. März 2014 im Plenum.⁸⁵ Die Justizminister der Mitgliedstaaten einigten sich sodann am 15. Juni 2015 auf eine Entwurfsfassung.⁸⁶ Im Anschluss begannen im Rahmen des Trilogs die Verhandlungen zwischen Rat, Parlament und EU-Kommission. Eine informell erzielte Einigung wurde schließlich am 17. Dezember 2015 vom Innen- und Rechtsausschuss des Europäischen Parlaments angenommen.⁸⁷ Das Plenum des Europäischen Parlaments wird hierüber voraussichtlich im Frühjahr 2016 abstimmen. Nach Inkrafttreten der DS-GVO haben die Mitgliedstaaten zwei Jahre Zeit für die Umsetzung. Die DS-GVO wird die DSRL ersetzen

gebunden. Das BVerfG beschränkt die Bindungswirkung deutscher Träger öffentlicher Gewalt aber auf zwingende Vorgaben des Unionsgrundrechts. Außerhalb dieses Bereichs seien die deutschen Grundrechte anwendbar, auch im Bereich von Umsetzungsspielräumen und Öffnungsklauseln im Sekundärrecht. So: BVerfGE 121, 1, 15. Dazu: Streinz/Michl, EuZW 2011, 384, 385 ff.

⁸⁰ EuGH, Rs. C-369/98, Slg. 2000, I-6751, Rn. 32 ff. - Fisher; Rs. C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Rn. 68 ff. - Österreichischer Rundfunk.

⁸¹ Streinz/Michl, EuZW 2011, 384, 387.

⁸² Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über ein Gesamtkonzept für den Datenschutz in der Europäischen Union vom 4. November 2010, KOM 2010/609 endg.

⁸³ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25. Januar 2012, KOM 2012/11 endg.

⁸⁴ Von deutscher Seite werden insbesondere verfassungsrechtliche Bedenken geltend gemacht. Die deutschen Grundrechte würden im Anwendungsbereich der DS-GVO ihre Geltung verlieren. Auf europäischer Ebene stünde den Bürgern kein der Verfassungsbeschwerde vergleichbarer Rechtsbehelf zur Verfügung. Für die Auslegung der DS-GVO wäre der EuGH zuständig, dessen Rechtsprechung zu den Grundrechten bislang weit hinter der ausdifferenzierten Dogmatik des BVerfG zurückbleibt. Dazu: Hornung, ZD 3/2012, 99, 100; Masing, Süddeutsche Zeitung, Ausgabe vom 9. Januar 2012, S. 10.

⁸⁵ Der Entwurf des Europäischen Parlaments ist abrufbar unter: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE>.

⁸⁶ Der Entwurf des Rates ist abrufbar unter: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf>.

⁸⁷ Die konsolidierte Fassung ist abrufbar unter: http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884.

und nach Art. 288 Abs. 2 AEUV für alle Mitgliedstaaten unmittelbare Wirkung entfalten. Die deutschen Gerichte, Behörden und Datenverarbeiter werden anstelle des BDSG und der Landesdatenschutzgesetze in ihrem inhaltlichen Geltungsbereich direkt die DS-GVO anwenden müssen. Da sich die hier relevanten Vorgaben der DSRL bezüglich der Gewährleistung eines angemessenen Schutzniveaus bei Datenübermittlungen in Drittländer auch in der DS-GVO wiederfinden⁸⁸, gelten die vorliegenden Ausführungen nach deren Inkrafttreten entsprechend.

II. USA

1. *Das verfassungsrechtliche Right to Privacy*

Das Datenschutzrecht der USA unterscheidet sich grundlegend von dem deutschen Modell. Der US Supreme Court erkennt lediglich für einzelne Bereiche ein Recht auf Privatsphäre (Right to Privacy) an.⁸⁹ In der Leitentscheidung *Katz v. United States* befand der US Supreme Court 1967, dass das polizeiliche Abhören eines öffentlichen Telefons gegen das Fourth Amendment verstoße.⁹⁰ Die Schutzgewährung sei jedoch davon abhängig, ob der Betroffene eine berechnete Erwartung am Schutz seiner Privatsphäre hat. Der Betroffene müsse den Schutz in der Situation tatsächlich erwartet haben und diese Erwartung müsse den allgemeinen gesellschaftlichen Vorstellungen entsprechen. Im Februar 1977 befasste sich der US Supreme Court in dem Verfahren *Whalen v. Roe* erstmals mit Datensammlungen.⁹¹ Die streitgegenständliche Vorschrift verpflichtete Ärzte zur Weitergabe von Rezepten für Arzneimittel einschließlich der darin enthaltenen Patientendaten an das US State Department of Health. Die Richter befanden, dass das Right to Privacy das Interesse an der Vermeidung der Offenlegung persönlicher Angelegenheiten umfasse. Das zweite bedeutende Urteil zu Datensammlungen verkündete der US Supreme Court im Juni 1977 in *Nixon v. Administrator of General Services*.⁹² In dieser Sache stellte sich die Frage nach der Rechtmäßigkeit des während der Watergate-Affäre erlassenen Presidential Recordings and Materials Preservation Act, der den Administrator of General Services zur Beschlagnahme von Unterlagen des ehe-

⁸⁸ Kapitel V, Artikel 40 bis 45 des Vorschlags für eine DS-GVO.

⁸⁹ Je nach Zusammenhang leitet der US Supreme Court das Right to Privacy aus dem First, Third, Fourth, Fifth, Ninth oder Fourteenth Amendment ab, vgl. *Griswold v. Connecticut*, 381 U.S. 479, 484 ff. (1965); *Rubenfeld*, 102 Harv. L. Rev. 737, 740 ff. (1989); *Solove*, 90 Cal. L. Rev. 1087, 1106 ff. (2002), jeweils m. w. N.

⁹⁰ *Katz v. United States*, 389 U.S. 347, 350 ff. (1967). Das Fourth Amendment der US Constitution lautet wie folgt: „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“. Zur Herleitung des Right to Privacy aus dem Fourth Amendment: *DeFilippis*, 115 Yale L. J. 1086, 1086 ff. (2006).

⁹¹ *Whalen v. Roe*, 429 U.S. 589, 591 ff. (1977).

⁹² *Nixon v. Administrator of General Services*, 433 U.S. 425, 429 ff. (1977).

maligen Präsidenten Richard Nixon berechnete. Die Richter entschieden, dass die Beschlagnahme von Unterlagen mit Bezug zur Präsidententätigkeit rechtmäßig sei, da sie der Aufklärung der Watergate-Affäre und dem öffentlichen Interesse diene. In rein privaten Angelegenheiten habe dagegen auch der ehemalige Präsident eine berechnete Erwartung am Schutz seines Right to Privacy.

Seit diesen Entscheidungen gehen die amerikanischen Gerichte überwiegend davon aus, dass das Recht auf informationelle Privatsphäre (Right to Information Privacy) als Unterfall des Right to Privacy verfassungsrechtlich geschützt sei.⁹³ Die genauen Konturen des Right to Information Privacy sind aber unklar. Zumeist erwähnen die Gerichte das Right to Information Privacy nicht gesondert, sondern sprechen allgemein von dem Right to Privacy.⁹⁴ Eine dem deutschen Volkszählungsurteil vergleichbare Entscheidung erließ der US Supreme Court bisher nicht.

Nach der amerikanischen State Action Doctrine ist das Right to Privacy in erster Linie ein Abwehrrecht gegenüber staatlichen Stellen.⁹⁵ Das Right to Privacy entfaltet weder Drittwirkung, noch begründet es Schutzpflichten des Staates hinsichtlich der Eingriffe durch Private.⁹⁶ Lediglich in Einzelfällen kommt es zu einer faktischen Wirkung des Right to Privacy im Verhältnis zwischen Privaten. So wird staatliches Handeln bei der Durchsetzung privater Rechte durch die Gerichte oder der Übernahme öffentlicher Funktionen durch Private angenommen.⁹⁷

2. *Das Common Law Right to Privacy*

Bereits Anfang des 20. Jahrhunderts erkannten die amerikanischen Gerichte das Right to Privacy als Common Law an und sprachen ihm deliktsrechtlichen Schutz zu.⁹⁸ Die von den Gerichten entwickelten Grundsätze veröffentlichte das American Law Institute in § 652 A bis

⁹³ NASA v. Nelson, 131 S.Ct. 746, 757 (2011); State v. Russo, 790 A.2d 1132, 1147 ff. (2002); Denius v. Dunlap, 209 F.3d 944, 955 ff. (7th Cir. 2000); Sterling v. Borough of Minersville, 232 F.3d 190, 194 ff. (3rd Cir. 2000); Chlapowski, 71 B.U.L. Rev. 133, 135 (1991) m. w. N.

⁹⁴ State v. Russo, 790 A.2d 1132, 1147 ff. (2002); Doe v. Attorney General, 941 F.2d 780, 796 (9th Cir. 1991); Doe v. Barrington, 729 F.Supp. 376, 382 ff. (D.N.J. 1990).

⁹⁵ Vgl. Houghton v. New Jersey Manufacturers Ins. Co., 615 F. Supp. 299, 306 (E.D. Pa. 1985); Miami Herald Pub. Co. v. Ferre, 636 F.Supp. 970, 975 f. (S.D. Fla. 1985); Giegerich, Privatwirkung der Grundrechte in den USA, S. 38 ff.; Buchner, Informationelle Selbstbestimmung, S. 9.

⁹⁶ Genz, Datenschutz in Europa und den USA, S. 49; Wuermeling, Handelshemmnis Datenschutz, S. 179; Wilske, CR 1993, 297, 299 und 304.

⁹⁷ Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 614 f. (1989); United States v. Jacobsen, 466 U.S. 109, 113 ff. (1984); Cooper, 36 Rutgers L. J. 775, 815 ff. (2005).

⁹⁸ Pavesich v. New England Life Ins. Co., 122 Ga. 190, 213 ff. (1905); Solove, 90 Cal. L. Rev. 1087, 1099 ff. (2002) m. w. N. Das Common Law Right to Privacy geht zurück auf den berühmten Artikel „The Right to Privacy“ von Samuel D. Warren und Louis D. Brandeis. Die Autoren beschrieben das Right to Privacy als „right to be let alone“, also das Recht, alleine gelassen zu werden, vgl. Warren/Brandeis, 4 Harv. L. Rev. 193 (1890).

E Restatement of the Law Second, Torts.⁹⁹ Danach muss derjenige, der das Right to Privacy eines anderen verletzt, diesem den entstandenen Schaden ersetzen. Im Einzelnen werden vier Tatbestände unterschieden: (1) Eindringen in den privaten Bereich, (2) unbefugter Gebrauch des Namens oder der Persönlichkeitsmerkmale zum eigenen Vorteil, (3) unbefugte Veröffentlichung privater Sachverhalte sowie (4) falsche oder entstellende Darstellung in der Öffentlichkeit.¹⁰⁰ Das Right to Information Privacy stellt kein selbstständiges Common Law dar. Bei Datenverarbeitungen wird deliktsrechtlicher Schutz allenfalls dann gewährt, wenn der jeweilige Fall einem der genannten Tatbestände zuzuordnen ist.¹⁰¹

3. *Einfachgesetzlicher Datenschutz im öffentlichen Bereich*

Die gesetzgeberischen Maßnahmen konzentrierten sich in den USA von Anfang an auf die staatliche Datenverarbeitung. Das wichtigste Gesetz ist der Federal Privacy Act von 1974, der für Datensammlungen von Bundesbehörden gilt.¹⁰² Der Federal Privacy Act bestimmt allgemeine Datenschutzprinzipien. Dazu zählen der Grundsatz persönliche Daten nur bei Einwilligung oder gesetzlicher Erlaubnis offenzulegen, die Pflicht zum Schutz gespeicherter Daten vor Verlust und Missbrauch sowie das Recht des Betroffenen auf Einsicht, Berichtigung und Schadensersatz.¹⁰³ Im Gegenzug enthält der Federal Privacy Act aber auch großzügige Erlaubnistatbestände.¹⁰⁴ Datenverarbeitungen sind zum Beispiel zulässig, soweit sie dem Routinegebrauch entsprechen und mit dem Zweck der ursprünglichen Datenerhebung übereinstimmen.¹⁰⁵

In der Folgezeit erließ der Bundesgesetzgeber weitere Vorschriften für spezielle Bereiche staatlicher Datenverarbeitung, so etwa den Right to Financial Privacy Act von 1978¹⁰⁶, den Privacy Protection Act von 1980¹⁰⁷ und den Drivers Privacy Protection Act von 1994¹⁰⁸. Über ein dem BDSG vergleichbares Datenschutzgesetz verfügen die USA nicht. Weder der Federal Privacy Act noch die sektoralen Gesetze sehen ein grundsätzliches Verbot der Datenverarbeitung vor. Im Anschluss an die Terrorangriffe vom 11. September 2001 erfuhr die Entwicklung des Datenschutzes in den USA eine Umkehrung, indem Datenverarbeitungen

⁹⁹ American Law Institute, Restatement of the Law Second, Torts, St. Paul, MN 1965.

¹⁰⁰ Zu den einzelnen Tatbeständen: Prosser, 48 Cal. L. Rev. 383, 389 ff. (1960); Wuermeling, Handelshemmnis Datenschutz, S. 185 ff.; Wilske, CR 1993, 297, 304 f.

¹⁰¹ Vgl. Elli Lake v. Wal-Mart Stores Inc., 582 N.W.2d. 231 (Minn. 1998); Shibley v. Time Inc., 45 Ohio App. 2d 69, 71 ff. (Ohio App. 1975).

¹⁰² 5 USC § 552a.

¹⁰³ 5 USC § 552a (b), (d), (e)(9) und (10), (g).

¹⁰⁴ 5 USC § 552a (b)(1) bis (10).

¹⁰⁵ 5 USC § 552a (b)(3).

¹⁰⁶ 12 USC §§ 3401 bis 3422.

¹⁰⁷ 42 USC § 2000aa.

¹⁰⁸ 18 USC §§ 2721 bis 2725.

durch staatliche Behörden in weitem Umfang für zulässig erklärt wurden. Vor allem der 2001 erlassene Patriot Act verleiht staatlichen Behörden extensive Datenverarbeitungsbefugnisse zur Prävention und Verfolgung terroristischer Straftaten.¹⁰⁹

4. Selbstregulierung und sektorale Datenschutzgesetze in der Privatwirtschaft

Seit den 1960er Jahren wurde in den USA der Datenschutz in der Privatwirtschaft erörtert.¹¹⁰ Allerdings befand eine vom Kongress eingesetzte Kommission 1977, dass die umfassende staatliche Regulierung nicht erforderlich sei, da die Konkurrenz in der Privatwirtschaft zu ausreichenden Datenschutzmaßnahmen führen würde.¹¹¹ Im privatwirtschaftlichen Bereich wird seither vorwiegend auf die Selbstregulierung vertraut.¹¹² Zahlreiche amerikanische Konzerne bestimmen in internen Richtlinien (Privacy Policies) Grundsätze für den Umgang mit personenbezogenen Daten.¹¹³ Inhaltlich orientieren sich die Instrumente der Selbstregulierung zumeist an den Vorgaben der OECD-Richtlinien von 1980^{114,115} Die Wirksamkeit der Instrumente ist aber von vornherein dadurch beschränkt, dass ihre Implementierung freiwillig ist und eine unabhängige Kontrolle fehlt.¹¹⁶

Der gesetzliche Schutz gegenüber Datenverarbeitungen der Privatwirtschaft beschränkt sich auf Bereiche, in denen besondere Risiken bestehen.¹¹⁷ Die Mehrzahl der Vorschriften betrifft den Finanzsektor.¹¹⁸ Hierzu zählt insbesondere der Fair Credit Reporting Act (FRCA) aus dem Jahr 1970.¹¹⁹ Der FRCA richtet sich an Kreditauskunfteien, Nutzer von Kreditauskünften sowie alle Stellen, die Daten an Kreditauskunfteien weitergeben. Der FRCA regelt die Voraussetzungen für die Übermittlung von Daten über die Kreditwürdigkeit, den Charakter, die allgemeine Reputation und die Lebensweise einer Person.¹²⁰ Den Betroffenen stehen

¹⁰⁹ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot Act) Act of 2001, Pub. L. 107-56, 115 Stat. 272, H. R. 3162.

¹¹⁰ Insbesondere Alan Westin leistete mit seinen Werken „Privacy and Freedom“ von 1967 und „Databanks in a Free Society“ von 1972 Pionierarbeit.

¹¹¹ Privacy Protection Study Commission, Personal Privacy in an Information Society, Ch. 13.

¹¹² Reidenberg, Privacy Protection and the Interdependence of Law, Technology and Self-Regulation, S. 1 ff.; Jacob in Büllesbach, Datenverkehr ohne Datenschutz?, S. 28; Genz, Datenschutz in Europa und den USA, S. 86 ff.

¹¹³ So etwa General Motors (https://media.gm.com/media/us/en/gm/account/privacy_policy.html) oder die Coca-Cola Company (<http://www.coca-colacompany.com/our-company/privacy-policy>).

¹¹⁴ OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980), Document C (89) 58 (Final) vom 23. September 1980. Die überarbeitete Fassung der Richtlinien von Juli 2013 ist abrufbar unter: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

¹¹⁵ Wellberry in Büllesbach, Datenverkehr ohne Datenschutz?, S. 172; Wuermeling, Handelshemmnis Datenschutz, S. 187.

¹¹⁶ Wuermeling, Handelshemmnis Datenschutz, S. 189.

¹¹⁷ Hoofnagle, Comparative Study on different approaches to new privacy challenges, USA, S. 1 ff. und 11 ff.

¹¹⁸ Zum Datenschutz im Finanzsektor: Genz, Datenschutz in Europa und den USA, S. 59 ff.

¹¹⁹ 15 USC § 1681.

¹²⁰ 15 USC § 1681a(d)(1).

Auskunftsrechte sowie Berichtigungs- und Schadensersatzansprüche zu.¹²¹ Wichtige Datenschutzbestimmungen enthält darüber hinaus der Gramm-Leach-Bliley-Act (GLBA) von 1999.¹²² Der GLBA gilt für Finanzinstitute, worunter neben Banken, Versicherungen und Investmentgesellschaften auch Aussteller von Kreditkarten und Anbieter von Leasingverträgen fallen. Nach dem GLBA sind Finanzinstitute dazu verpflichtet, Verbraucher über sie betreffende Datenverarbeitungen zu informieren.¹²³ Datenübermittlungen dürfen nur stattfinden, wenn ein Erlaubnistatbestand greift oder dem Verbraucher ein Widerspruchsrecht eingeräumt wird.¹²⁴

Für den Telekommunikationssektor bestehen ebenfalls Datenschutzgesetze. Der Electronic Communications Privacy Act von 1986 garantiert etwa die Vertraulichkeit von Kommunikationsvorgängen.¹²⁵ Er erstreckt sich auf sämtliche Formen der mündlichen, drahtgebundenen und elektronischen Kommunikation, wie Telefongespräche, E-Mails und Voice-Mails. Direkte Kommunikationsvorgänge werden vor unzulässigem Abhören und gespeicherte Kommunikationsvorgänge vor unbefugtem Zugriff geschützt.¹²⁶ In den Schutzbereich fallen ausschließlich die Inhalte der Kommunikationsvorgänge.¹²⁷ Der Telecommunications Act von 1996 indes schützt Sekundärinformationen wie Zeitpunkt, Dauer und Zielnummer von Telefongesprächen.¹²⁸ Diese Informationen dürfen erst nach gesetzlicher Anordnung oder zur Erfüllung eigener Leistungsverpflichtungen genutzt werden.¹²⁹ Das bedeutendste Datenschutzgesetz im Online-Bereich ist der Children's Online Privacy Act (COPPA) aus dem Jahr 1998.¹³⁰ Der COPPA regelt die Verarbeitung von Kinderdaten im Internet, wenn Betreiber ihr Angebot gezielt an Kinder richten oder Kenntnis erlangen, dass Daten von Kindern stammen.¹³¹ Die Betreiber sind verpflichtet, über die Verarbeitung der Kinderdaten zu informieren und das Einverständnis der Eltern einzuholen.¹³²

Im Gesundheitsbereich gewährleisten seit 2003 die auf Grundlage des Health Insurance Portability and Accountability Act (HIPAA) erlassenen Standards for Privacy of Individually Identifiable Health Information einen Mindestschutz für Gesundheitsdaten.¹³³ Die Regelungen

¹²¹ 15 USC §§ 1681g und 1681n ff.

¹²² 15 USC §§ 6801 bis 6809, §§ 6821 bis 6827.

¹²³ 15 USC §§ 6802(a) und 6803.

¹²⁴ 15 USC § 6802(b).

¹²⁵ 18 USC §§ 2510 bis 2522, §§ 2701 bis 2712 und §§ 3121 bis 3123.

¹²⁶ 18 USC §§ 2511 und 2701.

¹²⁷ 18 USC § 2510(8).

¹²⁸ 47 USC § 222.

¹²⁹ 47 USC § 222(c).

¹³⁰ 15 USC §§ 6501 bis 6506.

¹³¹ 15 USC § 6502(a)(1).

¹³² 15 USC § 6502(b)(1)(A)(i) und (ii).

¹³³ 45 C.F.R. §§ 160 und 164. Dazu: Oates, 30 Seattle U. L. Rev. 745, 745 ff. (2007).

richten sich an Krankenversicherungen, Clearingstellen und Anbieter von Gesundheitsleistungen, die elektronische Daten übermitteln.¹³⁴ Geschützt sind Daten, die den Gesundheitsstatus, die Krankenversicherung oder die Zahlung von Gesundheitsleistungen betreffen und einen Bezug zu einer bestimmten Person aufweisen.¹³⁵ Diese Daten dürfen einzig zur Durchführung und Zahlung von Gesundheitsleistungen oder zu ausdrücklich zugelassenen Zwecken verarbeitet werden.¹³⁶ In anderen Fällen bedarf es der Einwilligung des Betroffenen.¹³⁷

An dieser Stelle ist festzuhalten, dass in den USA auf Bundesebene zwar zahlreiche Gesetze die Datenverarbeitung in der Privatwirtschaft regeln, es aber an einer einheitlichen Systematik fehlt.¹³⁸ Die Gesetze haben einen engen Anwendungsbereich und behandeln Datenschutzfragen bloß anlassbezogen. Sie beruhen auf unterschiedlichen Ansätzen und beziehen sich zumeist auf bestimmte Datenarten und Verarbeitungsphasen. Für die Betroffenen ist oft nicht erkennbar, welche Rechte ihnen zustehen.¹³⁹

5. *Datenschutz in den Bundesstaaten*

Im Gegensatz zur US Constitution sehen die Verfassungen einiger Bundesstaaten ausdrücklich ein Right to Privacy vor.¹⁴⁰ Die meisten Regelungen schützen aber nur vor Eingriffen durch staatliche Stellen. Eine Ausnahme bildet Art. 1 Sec. 1 der kalifornischen Verfassung.¹⁴¹ Der California Supreme Court befand 1994 in der Sache *Hill v. National Collegiate Athletic Assn.*, dass die Vorschrift das Right to Privacy auch im Verhältnis zwischen Privaten gewährleiste.¹⁴² Es bedürfe jedoch einer schwerwiegenden Beeinträchtigung der Privatsphäre. Der Betroffene müsse ein rechtlich anerkanntes Interesse am Schutz des Right to Privacy und eine berechnete Schutzerwartung im Einzelfall darlegen. Die Anforderungen an die Schutzwährung sind somit hoch.

¹³⁴ 45 C.F.R. § 160.102.

¹³⁵ 45 C.F.R. § 160.103.

¹³⁶ 45 C.F.R. §§ 164.502 bis 164.506.

¹³⁷ 45 C.F.R. § 164.508.

¹³⁸ Hoofnagle, Comparative Study on different approaches to new privacy challenges, USA, S. 1 ff.; Reidenberg, 44 Fed. Comm. L. J. 195, 208 f. (1992); Schwartz, 52 Vand. L. Rev. 1607, 1632 ff. (1999); Solove, 53 Stan. L. Rev. 1393, 1444 (2001).

¹³⁹ Vgl. Hoofnagle, Comparative Study on different approaches to new privacy challenges, USA, S. 5.

¹⁴⁰ Alaska: Art. I Sec. 22; Arizona: Art. II Sec. 8; Florida: Art. I Sec. 23; Hawaii: Art. I Sec. 6 und 7; Illinois: Art. I Sec. 6; Kalifornien: Art. I Sec. 1; Louisiana: Art. I Sec. 5; Montana: Art. II Sec. 10; South Carolina: Art. I Sec. 10; Washington: Art. I Sec. 7.

¹⁴¹ Art. I Sec. 1 California Constitution lautet: „All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.“.

¹⁴² *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 20 ff. und 37 (1994). Ebenso: *Pioneer Electronics Inc. v. Superior Court*, 40 Cal. 4th 360, 370 ff. (2007); *Hernandez v. Hillsides Inc.*, 47 Cal. 4th 272, 295 ff. (2009).

Einige Bundesstaaten erließen zudem Datenschutzgesetze für den privaten Bereich.¹⁴³ Vor allem Kalifornien verfügt über eine Vielzahl von Gesetzen, die über das Schutzniveau der Bundesgesetze hinausgehen.¹⁴⁴ Das Gesetz zur Datensicherheit (Data Security Law) verpflichtet Unternehmen zum Beispiel zu Schutzmaßnahmen vor Zerstörung, Veränderung und Offenlegung persönlicher Informationen.¹⁴⁵ Über etwaige Verstöße müssen Unternehmen die Betroffenen in Kenntnis setzen.¹⁴⁶ Im Jahr 2001 richtete Kalifornien überdies beim Department of Consumer Affairs das Office for Privacy Protection ein.¹⁴⁷ Diese Behörde formuliert Richtlinien zum Datenschutz, informiert Verbraucher und setzt sich für deren Rechte ein. Gleichwohl fehlt es selbst in Bundesstaaten mit vergleichsweise umfänglichen Datenschutzregeln wie Kalifornien an einem einheitlichen Konzept.¹⁴⁸ Der Schutz ist zumeist auf Bewohner des Bundesstaates beschränkt. So ist das kalifornische Gesetz zur Datensicherheit ausschließlich auf Unternehmen anwendbar, die persönliche Informationen von Bewohnern Kaliforniens besitzen oder lizensieren.¹⁴⁹ Ausländer und Bewohner anderer Bundesstaaten sind nicht geschützt. Die Unternehmen können Daten ferner ungehindert in andere Bundesstaaten und das Ausland übermitteln.

III. Zusammenfassende Gegenüberstellung

1. *Unterschiedliche Regulierungsmodelle*

Die vorstehende Darstellung verdeutlicht die unterschiedlichen Regulierungsmodelle des deutschen und des amerikanischen Datenschutzrechts. Das deutsche Datenschutzrecht geht von einem einheitlichen Modell aus, das den öffentlichen und den nicht-öffentlichen Bereich erfasst.¹⁵⁰ Die Gefahren für das Persönlichkeitsrecht werden sowohl in der staatlichen als auch in der privaten Datenverarbeitung gesehen.¹⁵¹ Das Persönlichkeitsrecht ist daher nicht nur ein Abwehrrecht gegenüber staatlichen Stellen, sondern begründet zugleich die Pflicht des Staates, den Einzelnen vor Gefahren privater Datenverarbeiter zu schützen.

Anders als in Deutschland basiert das Datenschutzrecht in den USA auf einem zweigeteilten Modell, das zwischen der staatlichen und der privaten Datenverarbeitung differenziert.¹⁵² Die

¹⁴³ Schwartz, 118 Yale L. J. 902, 916 ff. (2009); Wilske, CR 1993, 297, 304 ff.

¹⁴⁴ Hoofnagle, Comparative Study on different approaches to new privacy challenges, USA, S. 15 ff.

¹⁴⁵ Cal. Civ. Code § 1798.81.5.

¹⁴⁶ Cal. Civ. Code § 1798.29.

¹⁴⁷ Die Homepage des Office for Privacy Protection ist abrufbar unter: <http://www.oag.ca.gov/privacy>.

¹⁴⁸ Genz, Datenschutz in Europa und den USA, S. 75.

¹⁴⁹ Cal. Civ. Code § 1798.81.5.

¹⁵⁰ Ausführlich zum einheitlichen Modell: Buchner, Informationelle Selbstbestimmung, S. 26 ff.

¹⁵¹ Vgl. Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung, BT-Drs. 7/1027 vom 21. September 1973, S. 14 und 17.

¹⁵² Ausführlich zum zweigeteilten Modell: Buchner, Informationelle Selbstbestimmung, S. 7 ff.

Gefahren für das Right to Privacy werden in erster Linie in der staatlichen Datenverarbeitung gesehen. Die Datenverarbeitung in der Privatwirtschaft bleibt vorrangig der Selbstregulierung überlassen. Die bereichsspezifischen Vorschriften schützen das Persönlichkeitsrecht nur bruchstückhaft vor Eingriffen.¹⁵³ Der unzureichende Datenschutz in der Privatwirtschaft wirkt sich vor allem deshalb deutlich aus, weil es an hinreichenden verfassungsrechtlichen Vorgaben fehlt.

2. Gründe für die umfassende Regulierung in Deutschland

Die umfassende Regulierung des Datenschutzes in Deutschland entspricht dem traditionellen kontinental-europäischen Staats- und Grundrechtsverständnis. Sowohl die französische Erklärung der Menschen- und Bürgerrechte von 1789 als auch die Vertreter des deutschen Vormärz forderten, dass der Staat nicht nur selbst Angriffe auf die bürgerlichen Freiheiten unterlässt, sondern, dass er daneben die Freiheitssphäre der Bürger gegen Leibeigenschaft, Grundlasten und Dienstpflichten sichert.¹⁵⁴ In Deutschland führte die ständische Ordnung zur Herausbildung eines paternalistischen Staates, in dem die Freiheit der Bürger von nachrangiger Bedeutung war.¹⁵⁵ Die Reformen unter Bismarck von 1883 und 1889 waren nicht der Erfolg einer Freiheitsbewegung der Bürger, sondern des reaktionären Staatsregimes.¹⁵⁶

Das BVerfG leitet in ständiger Rechtsprechung aus den Grundrechten staatliche Schutzpflichten ab.¹⁵⁷ Die besonderen Schutzpflichten des Staates auf dem Gebiet des Datenschutzes erklären sich durch die Nähe des allgemeinen Persönlichkeitsrechts zur Menschenwürde. In Abkehr von der nationalsozialistischen Vergangenheit formulierte der Parlamentarische Rat die Menschenwürde als Höchstwert des Grundgesetzes.¹⁵⁸ Das BVerfG betonte im Volkszählungsurteil die herausragende Bedeutung der Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt.¹⁵⁹ Ihrem Schutz diene das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht. Dabei hob das BVerfG die Wichtigkeit der Ausweitung des Grundrechtsschutzes hervor, wenn die Persönlichkeit wegen gesellschaftlicher oder technischer Entwicklung neuen Gefährdungen

¹⁵³ Genz, Datenschutz in Europa und den USA, S. 125 ff.

¹⁵⁴ Fröhlich in Beiträge Nürnberger Menschenrechtszentrum, S. 10.

¹⁵⁵ Huber, Transnationale Modellregeln, S. 346.

¹⁵⁶ Huber, Transnationale Modellregeln, S. 346 f.; Wahl in Isensee/Kirchhof, Handbuch des Staatsrechts, Band I, § 2 Rn. 14 f.

¹⁵⁷ BVerfGE 56, 54, 71 ff.; 46, 160, 164 f.; 39, 1, 41 f.; Isensee in Isensee/Kirchhof, Handbuch des Staatsrechts, Band IX, § 191 Rn. 33 ff.; Fröhlich in Beiträge Nürnberger Menschenrechtszentrum, S. 12; Klein, NJW 1989, 1633, 1633 ff.

¹⁵⁸ Herdegen in Maunz/Dürig, GG, Art. 1 Rn. 4, 16 und 21.

¹⁵⁹ BVerfGE 65, 1, 41.

ausgesetzt wird.¹⁶⁰ Der Gesetzgeber müsse Normen erlassen, die den Schutz des Persönlichkeitsrechts unter den jeweiligen Bedingungen bestmöglich gewährleisten.

3. Gründe für die restriktive Regulierung in den USA

Das Staats- und Grundrechtsverständnis der USA unterscheidet sich grundlegend von dem Deutschlands. Die reservierte Haltung des amerikanischen Bundesgesetzgebers bei der Normierung des Datenschutzes in der Privatwirtschaft geht zurück auf die ausgeprägt liberale Regulierungsphilosophie.¹⁶¹ Im Zuge der Loslösung von den europäischen Heimatstaaten entwickelte sich in den USA ein allgemeiner Freiheitsgedanke.¹⁶² Während in Kontinentaleuropa der Staat gesellschaftliche Zusammenhänge umfassend regelte, stellten die USA die Begrenzung des Staates in den Vordergrund.¹⁶³ Die US Constitution von 1789 basiert auf der Überzeugung, dass dem Menschen unveräußerliche Freiheitsrechte zustehen.¹⁶⁴ Der Staat soll sich auf die Gewähr der individuellen Freiheit und den Schutz des Privateigentums beschränken.¹⁶⁵

Die amerikanischen Grundrechte sind primär Abwehrrechte gegenüber dem Staat.¹⁶⁶ Dem Gesetzgeber kommt im Bereich der privaten Datenverarbeitung kein allgemeiner Schutzauftrag zu. Das Right to Privacy steht auch nicht in direktem Zusammenhang mit der Menschenwürde. Anders als das deutsche Grundgesetz gibt die US Constitution die Menschenwürde nicht als materielles Staatsziel vor.¹⁶⁷ Die US Constitution betont vielmehr die Rede- und Pressefreiheit des First Amendment, die den freien Informationsaustausch beinhaltet.¹⁶⁸ Der US Supreme Court ordnet das Right to Privacy daher regelmäßig als nachrangig gegenüber der Rede- und Pressefreiheit ein.¹⁶⁹ Eine umfassende Regulierung der Datenverarbeitung zwischen Privaten wäre nicht mit dem First Amendment vereinbar, da sie den freien Informationsaustausch einschränken würde.¹⁷⁰

¹⁶⁰ BVerfGE 65, 1, 41 ff.

¹⁶¹ Wuermeling, Handelshemmnis Datenschutz, S. 177.

¹⁶² Huber, Transnationale Modellregeln, S. 343.

¹⁶³ Hess, American Social and Political Thought, S. 37 ff.; Fink, Datenschutz zwischen Staat und Markt, S. 43 f.

¹⁶⁴ Huber, Transnationale Modellregeln, S. 343.

¹⁶⁵ Huber, Transnationale Modellregeln, S. 343.

¹⁶⁶ Fröhlich in Beiträge Nürnberger Menschenrechtszentrum, S. 9 f.

¹⁶⁷ Vöneky, Recht, Moral und Ethik, S. 483; Brugger, JZ 2008, 773, 774; ders., Demokratie, Freiheit und Gleichheit, S. 37 ff.; Kommers, Der Staat 37 (1998), 335, 338.

¹⁶⁸ Froomkin, 52 Stan. L. Rev. 1461, 1506 ff. (2000); Wellbery in Büllesbach, Datenverkehr ohne Datenschutz?, S. 170; Buchner, Informationelle Selbstbestimmung, S. 20 ff.

¹⁶⁹ Bartnicki v. Vopper, 532 U.S. 514, 527 ff. (2001); Florida Star v. B. J. F., 491 U.S. 524, 533 (1989); Smith v. Daily Mail Publishing Co., 443 U.S. 97, 1032 f. (1979).

¹⁷⁰ Volokh, 52 Stan. L. Rev. 1049, 1049 ff. (2000).

Die bereichsspezifischen Datenschutzgesetze spiegeln zugleich die amerikanische Tradition einer fallbezogenen Gesetzgebung wider, die darauf ausgerichtet ist, einzelne Rechte als Reaktion auf spezielle Probleme zu begründen.¹⁷¹ Gesetze dienen traditionell lediglich der Ergänzung des Common Law.¹⁷² Die staatliche Regulierung privater Aktivitäten wird gemeinhin als Gefahr für die Freiheiten der Bürger angesehen.¹⁷³ Diese abwehrende Haltung behindert die Gesetzgebung auf dem Gebiet des Datenschutzes. Trotz einer Hinwendung zu mehr Gesetzgebungsmaßnahmen unter der Präsidentschaft von Barack Obama wird die Selbstregulierung in den USA nach wie vor als bevorzugte Regelungsmethode angesehen.¹⁷⁴

B. Sachverhaltsaufklärung im Zivilprozess

Die zweite Hauptursache für den Konflikt zwischen der Discovery und deutschem Datenschutzrecht ist die unterschiedliche Auffassung von der Sachverhaltsaufklärung im Zivilprozess. Sowohl der deutsche als auch der amerikanische Zivilprozess basieren auf dem Beibringungsgrundsatz.¹⁷⁵ Danach ist es Sache der Parteien, die relevanten Tatsachen vorzutragen und einschlägige Beweismittel beizubringen. Allerdings geschieht dies in Deutschland und den USA auf ganz unterschiedliche Weise. Nachfolgend wird das Verfahren zur Sachverhaltsaufklärung in Deutschland (I.) und den USA (II.) erläutert und gegenübergestellt (III.).

I. Deutschland

1. Aktive Prozessleitung durch das Gericht

In Deutschland begleitet das Gericht den Zivilprozess von Anfang an und gewährleistet einen gesetzmäßigen Ablauf. Die formelle Prozessleitung umfasst den äußeren Ablauf des Verfahrens.¹⁷⁶ Dem Gericht obliegen insbesondere die Zustellung, die Fristsetzung, die Terminierung, die Ladung und die Festlegung der Verfahrensweise.¹⁷⁷ Im Rahmen der materiellen Prozessleitung sorgt das Gericht für eine sachangemessene Verhandlung des Falles.¹⁷⁸ Es legt fest, welche Streitpunkte entscheidungserheblich sind und worüber Beweis zu erheben ist.

¹⁷¹ Buchner, Informationelle Selbstbestimmung, S. 15.

¹⁷² Miedbrodt in Freundesgabe Büllersbach, S. 276; Lepsius, Verwaltungsrecht unter dem Common Law, S. 37 ff.

¹⁷³ Reidenberg, 52 Stan. L. Rev. 1315, 1342 f. (2000); ders., 80 Iowa L. Rev. 497, 501 (1995).

¹⁷⁴ The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Februar 2012, S. 1 ff. Danach sollen Unternehmen die Datenschutzrechte der Verbraucher vor allem durch Verhaltensregeln (Codes of Conduct) umsetzen.

¹⁷⁵ Krapfl, Dokumentenvorlage, S. 122; Gerber, 34 Am. J. Comp. L. 745, 767 f. (1986); Langbein, 52 U. Chi. L. Rev. 823, 827 ff. (1985); Stürner in FS Stiefel, 763, 763 ff.

¹⁷⁶ Prütting in Prütting/Gehrlein, ZPO, § 136 Rn. 2; Stadler in Musielak, ZPO, § 136 Rn. 2; Stürner in FS Stiefel, 763, 767.

¹⁷⁷ §§ 136 Abs. 1, 2 und 4, 166 bis 190, 214, 216, 227, 270, 272 ZPO.

¹⁷⁸ §§ 136 Abs. 3, 139 ZPO; Prütting in Prütting/Gehrlein, ZPO, § 136 Rn. 5.

Das Gericht ist verpflichtet, den Streitstand in rechtlicher und tatsächlicher Hinsicht aktiv mit den Parteien zu erörtern.¹⁷⁹ Es weist die Parteien auf fehlenden Tatsachenvortrag hin und regt Beweisangebote an.¹⁸⁰ Das Gericht führt auch die Beweiserhebung durch, indem es Augenschein einnimmt, Zeugen und Parteien hört, Sachverständige hinzuzieht und Urkunden einsieht.¹⁸¹ Bis auf den Zeugenbeweis darf das Gericht alle Beweismittel von Amts wegen erheben.¹⁸² Der Zivilprozess kann aus mehreren Terminen zur mündlichen Hauptverhandlung und zur Beweiserhebung bestehen. Die Parteien müssen nicht sämtliche Tatsachen und Beweismittel bei Verfahrensbeginn präsentieren, sondern können diese, soweit keine Verspätung vorliegt, bis zum Schluss der mündlichen Hauptverhandlung ergänzen. Anders als in den USA gibt es im deutschen Zivilprozess keine aus juristischen Laien bestehende Jury. Das Gericht ist vornehmlich mit Berufsrichtern besetzt.¹⁸³

2. Aufklärung des rechtserheblichen Sachverhalts

Die Sachverhaltsaufklärung ist im deutschen Zivilprozess auf rechtserhebliche Tatsachen begrenzt.¹⁸⁴ Der Kläger muss bereits in der Klageschrift den maßgeblichen Lebenssachverhalt schildern und einen bestimmten Klageantrag stellen.¹⁸⁵ Beabsichtigt der Beklagte eine Verteidigung, hat er in der Klageerwidern seine Verteidigungsmittel vorzubringen.¹⁸⁶ Das Gericht prüft im Zuge der Schlüssigkeitskontrolle, ob das Vorbringen des Klägers seinen Klageantrag rechtfertigt. Ist dies zu verneinen, kann das Gericht die Klage ohne Prüfung der Verteidigungsmittel des Beklagten abweisen. Ist das Vorbringen des Klägers hingegen schlüssig, kontrolliert das Gericht im zweiten Schritt, ob das Vorbringen des Beklagten für die Entscheidung rechtlich von Bedeutung ist. Allein hinsichtlich der zwischen den Parteien streitigen und rechtserheblichen Tatsachen nimmt das Gericht eine Beweiserhebung vor.

Bei der Aufklärung des rechtserheblichen Sachverhalts ist die beweisbelastete Partei zunächst auf solche Beweismittel beschränkt, über die sie selbst verfügt. Die Gegenseite ist grundsätzlich nicht prozessual zur Aufklärung verpflichtet.¹⁸⁷ Von dieser Grundregel sieht die Zivilprozessordnung (ZPO) wenige Ausnahmen vor. So kann eine Partei nach § 421 ZPO den Beweis antreten, indem sie bei Gericht beantragt, dem Gegner die Vorlage einer Urkunde aufzu-

¹⁷⁹ § 139 Abs. 1 Satz 1 ZPO; Prütting in Prütting/Gehrlein, ZPO, § 139 Rn. 1 ff.

¹⁸⁰ § 139 Abs. 1 Satz 2 ZPO.

¹⁸¹ §§ 284, 355 bis 484 ZPO.

¹⁸² §§ 142, 144, 293, 448 ZPO.

¹⁸³ Ehrenamtliche Richter werden in der Zivilgerichtsbarkeit lediglich in den Kammern für Handelssachen eingesetzt, vgl. § 105 Abs. 1 GVG.

¹⁸⁴ BGH, NJW 1990, 3151, 3151; Stürner in FS Stiefel, 763, 765 f.

¹⁸⁵ § 253 Abs. 2 Nr. 2 ZPO.

¹⁸⁶ § 277 Abs. 1 Satz 1 ZPO.

¹⁸⁷ BGH, NJW 1992, 1817, 1819; NJW 1990, 3151, 3151; OLG Hamm, NJW 1998, 3358, 3358; Leipold in Stein/Jonas, ZPO, § 138 Rn. 25 ff.; a. A. Stürner, Aufklärungspflicht, S. 56 ff., 92 ff. und 134 ff.

geben.¹⁸⁸ Voraussetzung dafür ist, dass den Gegner eine Vorlagepflicht nach den §§ 422, 423 ZPO trifft. Gemäß § 423 ZPO ist der Gegner zur Vorlage verpflichtet, wenn er im Prozess selbst auf die Urkunde Bezug genommen hat. Nach § 422 ZPO ist der Gegner zur Vorlage verpflichtet, wenn die beweisbelastete Partei einen materiell-rechtlichen Anspruch auf Herausgabe oder Vorlage hat. In Betracht kommen zum Beispiel die Ansprüche auf Herausgabe der §§ 371, 402, 985, 1144 BGB oder auf Einsichtnahme und Rechnungslegung der §§ 666, 716, 810 BGB sowie der §§ 118, 157 Abs. 3, 166, 233 HGB. Außerhalb des Beweisverfahrens kann die beweisbelastete Partei materiell-rechtliche Vorlageansprüche nur in einer Stufenklage oder einem gesonderten Prozess geltend machen.¹⁸⁹

Besitzt ein Dritter die Urkunde und überlässt er diese nicht freiwillig, muss die beweisbelastete Partei nach § 428 Alt. 1 ZPO bei Gericht eine Fristsetzung beantragen. Die Fristsetzung bewirkt die Unterbrechung des Verfahrens und ermöglicht der Partei, die Vorlage der Urkunde außerhalb des Verfahrens, soweit erforderlich auf dem Klageweg, durchzusetzen.¹⁹⁰ Nach § 429 ZPO ist der Dritte unter den gleichen Voraussetzungen wie der Beweisgegner zur Urkundenvorlage verpflichtet.¹⁹¹

Daneben ist die beweisbelastete Partei berechtigt, die Urkundenvorlage gemäß § 142 Abs. 1 ZPO anzuregen.¹⁹² Nach dieser im Rahmen der ZPO-Reform von 2001 neu gefassten Vorschrift kann das Gericht Parteien und Dritte auffordern, in ihrem Besitz befindliche Urkunden und sonstige Unterlagen vorzulegen, auf die sich eine Partei bezogen hat.¹⁹³ Die Entscheidung über die Anordnung steht im pflichtgemäßen Ermessen des Gerichts. Die Anordnung ist unabhängig von materiell-rechtlichen Ansprüchen und der Beweislast. Voraussetzung ist aber, dass neben der Bezugnahme ein schlüssiger Parteivortrag vorliegt.¹⁹⁴ § 142 Abs. 1 ZPO begründet somit keine allgemeine Aufklärungspflicht und ist nicht mit der amerikanischen Discovery vergleichbar.¹⁹⁵

¹⁸⁸ Auf elektronische Dokumente und andere Augenscheinsobjekte sind die §§ 421 ff. ZPO nach § 371 Abs. 2 Satz 2 ZPO entsprechend anwendbar.

¹⁸⁹ Foerste in Musielak, ZPO, § 254 Rn. 1 ff. (zur Stufenklage); Krapfl, Dokumentenvorlage, S. 10 ff.

¹⁹⁰ Preuß in Prütting/Gehrlein, ZPO, § 428 Rn. 4.

¹⁹¹ Eine Vorlagepflicht nach §§ 429, 422 ZPO wegen Bezugnahme auf die Urkunde kommt in Betracht, wenn der Dritte als Streithelfer am Prozess beteiligt ist oder früher Partei war, vgl. Preuß in Prütting/Gehrlein, ZPO, § 429 Rn. 2; Leipold in Stein/Jonas, ZPO, § 429 Rn. 1.

¹⁹² Für elektronische Dokumente und andere Augenscheinsobjekte enthält § 144 ZPO die entsprechende Regelung.

¹⁹³ Zuvor war § 142 Abs. 1 ZPO auf Urkunden einer Partei beschränkt, auf die sich *diese* Partei bezogen hat. Bei der Reform von 2001 wurde § 142 Abs. 1 ZPO insofern erweitert, als dass Parteien und Dritte nunmehr Urkunden vorlegen müssen, wenn sich *eine* Partei auf sie bezogen hat.

¹⁹⁴ Krapfl, Dokumentenvorlage, S. 26 f. und 31 ff.

¹⁹⁵ Beschlussempfehlung und Bericht des Rechtsausschusses des Deutschen Bundestags, BT-Drs. 14/6036 vom 15. Mai 2001, S. 120 f.; Zekoll/Bolt, NJW 2002, 3129, 3133 f.

In all diesen Fällen ist die Beweiserhebung im deutschen Zivilprozess durch das Ausforschungsverbot beschränkt.¹⁹⁶ Besteht die Gefahr einer Ausforschung, lehnt das Gericht den Beweis Antrag als unzulässig ab. Von der Gefahr einer Ausforschung ist in folgenden drei Fallgruppen auszugehen: Die erste Gruppe bilden Beweis Anträge, bei denen eine Partei die unter Beweis gestellten Tatsachen so ungenau angibt, dass das Gericht ihre Erheblichkeit nicht beurteilen kann.¹⁹⁷ Die zweite Gruppe erfasst Behauptungen, die eine Partei ohne konkreten Anhaltspunkt, also „ins Blaue hinein“, aufstellt.¹⁹⁸ Bei der dritten Gruppe handelt es sich um Beweis Anträge ohne Angabe beweisbedürftiger Behauptungen, mit denen Hinweise auf prozessrelevante Tatsachen erst in Erfahrung gebracht werden sollen.¹⁹⁹

3. *Berücksichtigung des allgemeinen Persönlichkeitsrechts*

Im deutschen Zivilprozess erfolgt die Vorlage von personenbezogenen Daten unter Beteiligung des Gerichts, welches den Prozessbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenübertritt. Nach Art. 1 Abs. 3 GG ist das Gericht an die Grundrechte und somit auch an die datenschutzrechtlichen Ausprägungen des allgemeinen Persönlichkeitsrechts gebunden. Zwar begründet das allgemeine Persönlichkeitsrecht kein Zeugnisverweigerungsrecht, gleichwohl berücksichtigt es das Gericht bei der Ermessensausübung.²⁰⁰ Die Verwendung personenbezogener Daten ohne Einwilligung des Betroffenen bedeutet einen Eingriff in dessen Persönlichkeitsrecht. Das Gericht prüft im Einzelfall, ob der Eingriff gerechtfertigt ist. Nach Art. 2 Abs. 1 GG wird das allgemeine Persönlichkeitsrecht unter anderem durch die verfassungsmäßige Ordnung beschränkt. Zur verfassungsmäßigen Ordnung zählt der aus dem Rechtsstaatsprinzip folgende Anspruch der Parteien auf eine faire Handhabung des Beweisrechts.²⁰¹ Danach ist das Gericht gehalten, von den Parteien angebotene Beweismittel zu berücksichtigen. Dies gilt aber nur insoweit, als eine Behauptung rechtserheblich und beweisbedürftig ist. Daher besteht im Regelfall lediglich für eine

¹⁹⁶ Laumen in Prütting/Gehrlein, ZPO, § 284 Rn. 24 f.; Beckhaus, Die Bewältigung von Informationsdefiziten, S. 247 ff.

¹⁹⁷ BGH, NJW 2005, 2710, 2711; NJW 1991, 2707, 2709; NJW-RR 1996, 183, 184; NJW 1974, 1710, 1711; Prütting in MüKo-ZPO, § 284 Rn. 79; Beckhaus, Die Bewältigung von Informationsdefiziten, S. 247.

¹⁹⁸ BGH, NJW-RR 2011, 1350, 1351; NJW 2005, 2710, 2711; NJW 1995, 2111, 2112; Foerste in Musielak, ZPO, § 284 Rn. 18; Prütting in MüKo-ZPO, § 284 Rn. 79; Beckhaus, Die Bewältigung von Informationsdefiziten, S. 247.

¹⁹⁹ BGH, NJW-RR 1986, 480, 482; NJW 1979, 1832, 1832 f.; NJW 1964, 1179, 1179; Beckhaus, Die Bewältigung von Informationsdefiziten, S. 247.

²⁰⁰ BVerfGE 117, 202, 240; 106, 28, 48; 52, 203, 207; BGHZ 27, 284, 291; BAG, NZA 2011, 571, 573 f.; NZA 2008, 1008, 1011 f.; OLG Braunschweig, Urteil vom 5. November 2006, 1 W 64/08, juris; OLG München, Urteil vom 9. November 2001, 1 U 2742/06, juris; OLG Hamm, Urteil vom 30. Juni 1992, 4 U 321/91, juris; Dauster/Braun, NJW 2000, 313, 316 ff.; Konrad, NJW 2004, 710, 711; Wagner, JZ 2007, 706, 715; ders. ZJP 108 (1995), 193, 213 ff; Werner, NJW 1988, 993, 997 ff.

²⁰¹ BVerfGE 117, 202, 240; 106, 28, 48; 52, 131, 145; BAG, NZA 2011, 571, 573; NZA 2008, 1008, 1010; Prütting in MüKo-ZPO, § 284 Rn. 18; Habscheid, ZJP 96 (1983), 306, 307 f.; Dauster/Braun, NJW 2000, 313, 319; Werner, NJW 1988, 993, 998.

überschaubare Anzahl von personenbezogenen Daten eine Vorlagepflicht. Das Gericht prüft, ob und in welchem Umfang die Offenlegung der personenbezogenen Daten tatsächlich für die Beweisführung erforderlich ist. In Bezug auf die erforderlichen personenbezogenen Daten wägt das Gericht das Persönlichkeitsrecht des Betroffenen gegen das Beweisführungsinteresse der Partei nach den Grundsätzen der praktischen Konkordanz ab. Entscheidende Bedeutung kommt der Art der personenbezogenen Daten zu.²⁰² Je sensibler und intimer die personenbezogenen Daten sind, desto mehr ist der Abwägungsspielraum des Gerichts eingeschränkt. Auf Seiten des Beweisführers ist zu berücksichtigen, ob andere Beweismittel zur Verfügung stehen.²⁰³ Das Interesse an der Sicherung eines Beweismittels allein rechtfertigt nicht den Eingriff in das Persönlichkeitsrecht.²⁰⁴ Vielmehr muss den personenbezogenen Daten eine besondere Bedeutung für die Rechtsdurchsetzung der Partei zukommen.²⁰⁵

II. USA

1. Zivilprozess als Zweikampf der Parteien

Die Rollenverteilung des amerikanischen Zivilprozesses unterscheidet sich grundlegend von der des deutschen Zivilprozesses. Nach dem Adversary System wird das Verfahren in erster Linie von den Parteien und ihren Anwälten gestaltet.²⁰⁶ Dem liegt die Vorstellung zugrunde, dass der Zweikampf der Parteien die beste Methode zur Herstellung von Gerechtigkeit sei (Sporting Theory of Justice).²⁰⁷ Im Pretrial besprechen die Parteien ohne Beteiligung des Gerichts den Ablauf des Verfahrens und formulieren einen Plan für die Discovery, aus dem sich deren Fristen und Maßnahmen ergeben.²⁰⁸ Das Gericht kann die Parteien zu einer Pretrial Conference laden und Verfahrensanordnungen erlassen.²⁰⁹ Weitere formelle Prozessleitungsmaßnahmen sind nicht ausgeschlossen, allerdings handelt das Gericht selten von sich aus. Im Regelfall nimmt das Gericht eine passive Rolle ein. Zustellungen und Mitteilungen erfolgen grundsätzlich im Parteibetrieb.²¹⁰ Materielle Prozessleitungsmaßnahmen des Gerichts sind ebenfalls ungewöhnlich. Gerichtliche Hinweis- und Aufklärungspflichten entsprechend der ZPO kennt der amerikanische Zivilprozess nicht.²¹¹ Die Parteien gestalten die Discovery und

²⁰² Vgl. BVerfGE 80, 367, 374; 34, 238, 248.

²⁰³ OLG Braunschweig, Urteil vom 5. November 2006, 1 W 64/08, juris; OLG Hamm, Urteil vom 30. Juni 1992, 4 U 321/91, juris.

²⁰⁴ BVerfGE 117, 202, 240; 106, 28, 48 f.

²⁰⁵ BVerfGE 106, 28, 48.

²⁰⁶ Junker, Discovery, S. 78 ff.; Gerber, 34 Am. J. Comp. L., 745, 767 ff. (1986); Frankel, 123 U. Pa. L. Rev. 1031, 1031 ff. (1975).

²⁰⁷ Stürmer in FS Stiefel, 763, 777; Frankel, 123 U. Pa. L. Rev. 1031, 1033 (1975).

²⁰⁸ FRCP 26(f)(1) bis (3).

²⁰⁹ FRCP 16(a), (c) und (d); Peckham, 69 Cal. L. Rev. 770, 770 ff. (1990).

²¹⁰ FRCP 4(c) und 5.

²¹¹ Junker, Discovery, S. 80.

entscheiden, welche Beweise zu erheben sind. Sie können ohne gerichtliche Anordnung Auskünfte und Dokumente von der Gegenseite und Dritten anfordern.²¹² Bei Streitigkeiten bestimmen die Parteien, ob sie das Gericht einschalten. Das Gericht befindet sodann ausschließlich über die Zulässigkeit der streitigen Maßnahme.

Für die mündliche Hauptverhandlung ist zumeist ein einziger Termin anberaumt. Die sorgfältige und umfassende Vorbereitung im Pretrial ist daher entscheidend für den Prozessausgang. Die Anwälte sind die zentralen Akteure der Hauptverhandlung. Überwiegend findet die Hauptverhandlung unter Beteiligung einer Jury statt, der die Anwälte ihre Version des Rechtsstreits und die von ihnen für relevant befundenen Beweismittel präsentieren.²¹³ Der Richter überwacht diesen Vorgang lediglich. Theoretisch kann der Richter einen aktiven Verhandlungsstil wählen und zum Beispiel von Amts wegen Zeugen und Sachverständige laden.²¹⁴ In der Praxis kommt dies so gut wie nicht vor.²¹⁵ Die Richter stammen vorwiegend aus der Anwaltschaft und sind es gewohnt, den Prozess aus Sicht des Anwalts zu sehen.²¹⁶

2. *Aufklärung des historischen Gesamtsachverhalts*

Anders als in Deutschland müssen die Parteien im amerikanischen Zivilprozess ihr Vorbringen dem Gericht nicht umfänglich in Schriftsätzen unterbreiten. Das Gericht unterzieht die Klage im Pretrial keiner Schlüssigkeitskontrolle. Die Klageschrift dient allein der Benachrichtigung des Gegners (Notice Pleading).²¹⁷ Sie enthält regelmäßig keinen ausführlichen Sachverhaltsvortrag oder gar Beweisangebote.²¹⁸ Der Kläger kann die Klage ohne Kenntnis der genauen Gründe erheben und diese erst in der Discovery auffindig machen. Die Jury beurteilt den Rechtsstreit primär nach dem tatsächlichen Geschehen und weniger nach rechtlichen Vorgaben.²¹⁹ Deshalb erfolgt die Sachverhaltsaufklärung in der Discovery weitgehend unabhängig von rechtlichen Anspruchsgrundlagen. Angestrebt wird die Aufklärung des historischen Gesamtsachverhalts.²²⁰ So befand auch der US Supreme Court bereits

²¹² Bis zur Reform der FRCP von 1970 mussten die Anwälte die Dokumentenvorlage bei Gericht beantragen und dafür einen vernünftigen Grund angeben. Dazu: Junker, Discovery, S. 166 f.

²¹³ Junker, Discovery, S. 75.

²¹⁴ FRE 614(a) und 706(a).

²¹⁵ Osthaus, Informationszugang, S. 55; Langbein, 52 U. Chi. L. Rev., 823, 840 (1985).

²¹⁶ Stürner in FS Stiefel, 763, 778; Frankel, 123 U. Pa. L. Rev. 1031, 1033 (1975).

²¹⁷ Osthaus, Informationszugang, S. 84; Marcus, 86 Colum. L. Rev. 433, 451 ff. (1986).

²¹⁸ Osthaus, Informationszugang, S. 84.

²¹⁹ Stürner in FS Stiefel, 763, 764.

²²⁰ Krapfl, Dokumentenvorlage, S. 123; Frankel, 123 U. Pa. L. Rev. 1031, 1036 (1975); Stürner in FS Stiefel, 763, 766.

1947 in der Leitentscheidung *Hickman v. Taylor*, dass die Discovery den Parteien größtmögliche Kenntnis der Tatsachen und Streitfragen vermitteln solle.²²¹

Aufgrund dieser Zielsetzung verfügen die Parteien über weitreichende Befugnisse zur Sachverhaltsaufklärung. Die Discovery kann sich auf alle Informationen erstrecken, die für ein Angriffs- oder Verteidigungsmittel einer Partei relevant sind und keinem Weigerungsrecht unterliegen.²²² Es muss sich nicht um Informationen handeln, die als Beweismittel für die mündliche Hauptverhandlung in Betracht kommen.²²³ Vielmehr ist ausreichend, wenn die Informationen zur Aufdeckung zulässiger Beweismittel geeignet erscheinen. Der Prozessausgang soll nicht vom bloßen Informationsvorsprung einer Seite abhängen.²²⁴ Für die umfassende Sachverhaltsaufklärung stehen den Parteien folgende Instrumente zur Verfügung:

- (1) Der Austausch von schriftlichen Fragen (Interrogatories) und Antworten zwischen Parteien²²⁵;
- (2) die Aufforderung von Parteien und Dritten zur Vorlage von Dokumenten, elektronisch gespeicherten Informationen und körperlichen Gegenständen (Production of Documents, Electronically Stored Information and Tangible Things)²²⁶;
- (3) die Vernehmung von Parteien und Dritten unter Eid (Depositions)²²⁷;
- (4) die Aufforderung von Parteien und Dritten zur Gestattung des Zutritts zu Grundstücken und anderem Besitztum (Entry onto Land or other Property)²²⁸;
- (5) die körperliche und geistige Untersuchung (Physical and Mental Examination) von Parteien²²⁹ sowie
- (6) die Aufforderung von Parteien zum Geständnis (Request for Admission)²³⁰.

Die Kehrseite der umfassenden Sachverhaltsaufklärung ist die Gefahr von Beweisfischzügen (Fishing Expeditions) und einer Ausforschung der Gegenseite.²³¹ Anders als in Deutschland wird dies in den USA im Interesse der Wahrheitsfindung bewusst in Kauf genommen.²³²

²²¹ *Hickman v. Taylor*, 329 U.S. 495, 501 (1947).

²²² FRCP 26(b)(1) Satz 1.

²²³ FRCP 26(b)(1) Satz 3.

²²⁴ *Hickman v. Taylor*, 329 U.S. 495, 507 (1947).

²²⁵ FRCP 33.

²²⁶ FRCP 34(a)(1).

²²⁷ FRCP 30 und 31.

²²⁸ FRCP 34(a)(2).

²²⁹ FRCP 35.

²³⁰ FRCP 36.

²³¹ Mössle, Extraterritoriale Beweisbeschaffung, S. 104 ff.; Lorenz, ZZP 111 (1998), 35, 49 f.; Reimann, IPRax 1994, 152, 152.

²³² *Hickman v. Taylor*, 329 US 495, 507 f. (1947).

Spätestens mit Abschluss der Discovery können die Parteien ihre eigene und die gegnerische Position einschätzen. Die Mehrzahl der Verfahren wird vor der Hauptverhandlung durch Vergleich beendet.²³³ Aus diesem Grund wird der Discovery eine vergleichsfördernde Wirkung zugesprochen.²³⁴ Zum Teil sind Beklagte auch nur zur Vermeidung hoher Discovery-Kosten bereit, einen unbegründeten Anspruch vergleichsweise zu befriedigen.²³⁵ Denn die Discovery-Kosten trägt grundsätzlich jede Partei selbst.²³⁶ Für Kläger ist das anfängliche Kostenrisiko gering, da die Gerichtsgebühren niedrig sind und viele Klägeranwälte auf der Basis von Erfolgshonoraren (Contingency Fees) tätig werden.²³⁷

3. Berücksichtigung des Right to Privacy

Die Gerichte haben dem Right to Privacy bislang nicht den Schutz eines Weigerungsrechts zuerkannt, sodass personenbezogene Daten in der Discovery prinzipiell offenzulegen sind. Anders als in Deutschland greift das Gericht in den USA nicht von sich aus in das Verfahren ein, um das Right to Privacy zu schützen. Die Discovery ist ein Parteiverfahren. Die Parteien bestimmen den Umfang der Discovery und die Schutzwürdigkeit von Informationen. Das Gericht berücksichtigt das Right to Privacy erst auf Antrag einer Partei oder des Betroffenen. Dazu muss der Antragsteller eine berechtigte Erwartung am Schutz des Right to Privacy darlegen.²³⁸ Für die Schutzwürdigkeit stellen die Gerichte in erster Linie auf die Art der Daten ab.²³⁹ Die Schutzerwartung ist besonders hoch bei Informationen über intime Beziehungen des Betroffenen zu anderen Personen²⁴⁰, Namen und Adressen von Patienten einer Arztpraxis²⁴¹ sowie Gesundheitsdaten²⁴². Geringer Schutz kommt demgegenüber Namen und Adressen außerhalb des Gesundheitskontexts sowie Angaben über den Familienstand und das Arbeitsverhältnis zu.²⁴³ Darüber hinaus stellen die Gerichte darauf ab, wessen Daten betroffen

²³³ Zu einer Hauptverhandlung kommt es in weniger als zehn Prozent der eingeleiteten Verfahren, vgl. Higginbotham, 6-26 Moore's Federal Practice - Civil § 26.101[1].

²³⁴ Higginbotham, 6-26 Moore's Federal Practice - Civil § 26.02; Lange/Black, Der Zivilprozess in den Vereinigten Staaten, S. 62; Zekoll, 50 Am. J. Comp. L. 121, 149 f. (2002).

²³⁵ Junker, Discovery, 91 f.; Schack, Einführung in das US-amerikanische Zivilprozessrecht, S. 46.

²³⁶ Dies entspricht der im amerikanischen Zivilprozess geltenden „American Rule“, wonach eine Partei grundsätzlich keine Kostenersatzung von der Gegenseite verlangen kann. Dazu: Breyer, Kostenorientierte Steuerung des Zivilprozesses, S. 108 ff.

²³⁷ Junker, Discovery, S. 90 f. Die Gebühr für die Klageeinreichung bei den Bundesgerichten beträgt lediglich 350 USD (siehe: <http://www.uscourts.gov/FormsAndFees/Fees/USCortOfFederalClaimsFeeSchedule.aspx>)

²³⁸ Hill v. National Collegiate Athletic Assn., 7 Cal. 4th 1, 36 f. (1994).

²³⁹ Adelman v. BSA, 276 F.R.D. 681, 694 ff. (S.D. Fla. 2011); Schnabel v. Superior Court, 5 Cal. 4th 704, 714 (1993).

²⁴⁰ Fults v. Superior Court, 88 Cal. App. 3d 899, 902 (Cal. App. 1st Dist. 1979); Martinelli v. District Court of Denver, 199 Colo. 163, 174 (1980); Byron & Assocs. Inc. v. State, 360 So.2d 83, 95 (Fla. 1st DCA 1978).

²⁴¹ Colonial Medical Spec. v. United Diagnostic Lab., 674 So.2d 923, 923 f. (Fla. 4th DCA 1996).

²⁴² Pagano v. Oroville Hosp., 145 F.R.D. 683, 697 (E.D. Cal. 1993); Heda v. Superior Court, 225 Cal. App. 3d 525, 527 (Cal. App. 1st Dist. 1990).

²⁴³ ACLU v. Whitman, 159 P.3d 707, 710 (Colo. App. 2006).

sind. Bei Daten des Klägers gehen die Gerichte regelmäßig von einer eingeschränkten Schutzwürdigkeit aus, da er den Rechtsstreit und damit die Discovery eingeleitet hat.²⁴⁴ Bei Daten des Beklagten hängt die Schutzwürdigkeit davon ab, ob er den Rechtsstreit provoziert hat. Am ehesten schützen die Gerichte Daten unbeteiligter Dritter.²⁴⁵

Bei Vorliegen einer berechtigten Schutzerwartung des Antragstellers prüft das Gericht im nächsten Schritt, ob der Vorlageersuchende ein überwiegendes Interesse an der Offenlegung der Daten hat. Dies ist der Fall, wenn die Informationen für den Vorlageersuchenden von wesentlicher Bedeutung sind und er sie nicht auf anderem zumutbaren Wege erlangen kann.²⁴⁶ Die Gerichte gehen überwiegend davon aus, dass dem Right to Privacy durch eine Schutzanordnung (Protective Order) genüge getan wird.²⁴⁷ Daher ordnen sie tendenziell eher die Dokumentenvorlage unter Schutzmaßnahmen an, anstatt sie zu versagen. Hat die Öffentlichkeit ein besonderes Interesse an den Informationen, ordnen die Gerichte zumeist die ungeschützte Vorlage an.²⁴⁸

III. Zusammenfassende Gegenüberstellung

1. *Unterschiedliche Reichweite der Sachverhaltsaufklärung*

In Deutschland leitet das Gericht den Zivilprozess aktiv und nimmt die Beweiserhebung vor. In den USA hingegen ist der Zivilprozess ein Zweikampf der Parteien, bei dem das Gericht eine passive Rolle einnimmt. Den Parteien obliegt die Sachverhaltsaufklärung in der Discovery. Dabei müssen die Gegenseite und Dritte sämtliche Informationen offenlegen, die für den Rechtsstreit potentiell relevant sein können. Im deutschen Zivilprozess ist die Sachverhaltsaufklärung indessen auf rechtserhebliche Tatsachen beschränkt. Die Gegenseite und Dritte sind grundsätzlich nicht prozessual zur Sachverhaltsaufklärung verpflichtet. Während eine Ausforschung der Gegenseite und Dritter in Deutschland verhindert werden soll, ist sie in den USA gerade Zweck der Discovery. Die Anzahl der im Zivilprozess vorzulegenden personenbezogenen Daten ist demzufolge in Deutschland von vornherein weitaus geringer als in den USA. Im Übrigen sichert die Grundrechtsbindung der deutschen Gerichte

²⁴⁴ Vassiliades v. Israely, 714 F.Supp. 604, 616 (D. Conn. 1989).

²⁴⁵ American Friends Service Committee v. City & County of Denver, 2004 U.S. Dist. LEXIS 18474 (D. Colo. 2004); Planned Parenthood Golden Gate v. Superior Court, 83 Cal. App. 4th 347, 358 (Cal. App. 1st Dist. 2000).

²⁴⁶ Pagano v. Oroville Hosp., 145 F.R.D. 683, 698 f. (E.D. Cal. 1993); Schnabel v. Superior Court, 5 Cal. 4th 704, 717 (1993); Vinson v. Superior Court 43 Cal. 3d 833, 842 (1987); Planned Parenthood Golden Gate v. Superior Court, 83 Cal. App. 4th 347, 367 (Cal. App. 1st Dist. 2000).

²⁴⁷ Kahn v. Superior Court, 188 Cal. App. 3d 752, 766 (Cal. App. 6th Dist. 1987); Board of Trustees v. Superior Court, 119 Cal. App. 3d 516, 532 (Cal. App. 1st Dist. 1981).

²⁴⁸ In re Roman Catholic Archbishop, 661 F.3d 417, 428 (9th Cir. 2011); Public Citizen v. Liggett Group Inc., 858 F.2d 775, 780 und 787 (1st Cir. 1988); In re Agent Orange Product Liability Litigation, 98 F.R.D. 539, 547 (E.D.N.Y. 1983).

ein verfassungsgemäßes Verfahren. Kommen personenbezogene Daten als Beweismittel in Betracht, wägt das Gericht das allgemeine Persönlichkeitsrecht des Betroffenen gegen das Beweisführungsinteresse der Partei ab. Anders verhält es sich in den USA. Die Discovery ist nur durch wenige eng gefasste Weigerungsrechte begrenzt. Das Right to Privacy begründet kein Weigerungsrecht, weshalb personenbezogene Daten grundsätzlich offenzulegen sind.

2. Gründe für die restriktive Sachverhaltsaufklärung in Deutschland

Die restriktive Sachverhaltsaufklärung im deutschen Zivilprozess geht historisch auf das Aktionendenken des römischen Rechts zurück.²⁴⁹ Im römischen Formularprozess legte der Prätor vor der Verhandlung die zwischen den Parteien streitigen Fragen fest.²⁵⁰ Diese ergaben sich aus dem Antrag des Klägers auf Erteilung einer bestimmten „actio“ und der Einlassung des Beklagten.²⁵¹ Der Richter entschied ausschließlich die vom Prätor für erheblich befundenen Streitfragen. In Deutschland wurde die rechtsgebundene Sachverhaltsaufklärung des römischen Rechts während der Rezeption im 14. und 15. Jahrhundert übernommen und 1879 in die ZPO eingeführt.²⁵² Den Prozessbetrieb überließ die ZPO zunächst noch den Parteien, während dem Richter eine passive Position zukam. Dies änderte sich Anfang des 20. Jahrhunderts mit dem Aufkommen der Idee des sozialen Zivilprozesses. Der Zivilprozess sei eine soziale Massenerscheinung, für die der Staat eine Wohlfahrtseinrichtung zur Verfügung zu stellen habe.²⁵³ Dementsprechend führte die ZPO-Novelle von 1909 vor den deutschen Amtsgerichten den Amtsbetrieb ein, der die Grundlage für die Stärkung der Richtermacht bildete.²⁵⁴ Fortan wurde die Rechtsprechung nicht als Akt bürgerlicher Selbstverwaltung, sondern als staatliche Daseinsvorsorge betrachtet.²⁵⁵

In seinen Grundzügen ist der deutsche Zivilprozess auch heute noch hoheitlich geprägt.²⁵⁶ Der Verfahrensablauf ist durch die ZPO vorgegeben und stark formalisiert. Das Gericht überwacht den Prozess und wirkt durch Hinweise auf die Klärung des Sachverhalts hin. Vorrangig dient der deutsche Zivilprozess dem Individualrechtsschutz.²⁵⁷ Generalpräventive Zwecke und der Schutz von Allgemeininteressen spielen eine nachrangige Rolle. Aufgrund der eingeschränk-

²⁴⁹ Huber, Transnationale Modellregeln, S. 107 f.; Stürner in FS Stiefel, 763, 775.

²⁵⁰ Kaser/Hackl, Das römische Zivilprozessrecht, S. 69 ff. und 151 ff.; Hausmaninger/Selb, Römisches Privatrecht, S. 374 f. und 382; Nakamura, ZZZ 99 (1986), 1, 4.

²⁵¹ Kaser/Hackl, Das römische Zivilprozessrecht, S. 231 ff. und 256 ff.; Nakamura, ZZZ 99 (1986), 1, 6.

²⁵² Vgl. Prütting in Prütting/Gehrlein, ZPO, Einleitung Rn. 5; Nakamura, ZZZ 99 (1986), 1, 6.

²⁵³ Zur Idee des sozialen Zivilprozesses: Rechberger, R.L.R. 25 (2008), 101, 101 ff.

²⁵⁴ Brehm in Stein/Jonas, ZPO, vor § 1 Rn. 150; Rechberger, R.L.R. 25 (2008), 101, 105.

²⁵⁵ Stürner in FS Stiefel, 763, 781 f.

²⁵⁶ Krapfl, Dokumentenvorlage, S. 124 f.

²⁵⁷ Brehm in Stein/Jonas, ZPO, vor § 1 Rn. 9; Prütting in Prütting/Gehrlein, ZPO, Einleitung Rn. 3; Stürner, Aufklärungspflicht, S. 49 f.; ders. in FS Stiefel, 763, 783.

ten Mitwirkungspflichten und der Grundrechtsbindung des Gerichts ist die Eingriffswirkung des Zivilprozesses für nicht beweisbelastete Parteien und Dritte gering.²⁵⁸

3. Gründe für die umfassende Sachverhaltsaufklärung in den USA

Die umfassende Sachverhaltsaufklärung in der Discovery hat ihren Ursprung im germanischen Prozess, der unter normannischem Einfluss das englische Recht beeinflusste.²⁵⁹ Im germanischen Prozess bewerteten die Schöffen unter Anleitung des Richters den Sachverhalt aufgrund des tatsächlichen Parteivortrags ohne feste Rechtsregeln.²⁶⁰ Das englische Common Law sah im Mittelalter noch das Verbot des Parteizeugnisses vor, wonach Parteien grundsätzlich weder für- noch gegeneinander aussagen konnten.²⁶¹ Zur Vermeidung von Beweisnotständen gestattete das Equity-Verfahren den Parteien, die Gegenseite zur schriftlichen Beantwortung von Fragen und zur Vorlage einzelner Dokumente aufzufordern.²⁶² Die Fragen und Vorlageverlangen mussten sich auf Tatsachen beziehen, für welche die ersuchende Partei beweispflichtig war (Own Case Rule).²⁶³ Zudem durften nur solche Beweismittel verlangt werden, die in den Prozess eingeführt und nicht anderweitig erlangt werden konnten (Admissibility).²⁶⁴ Die USA übernahmen im 18. Jahrhundert das englische System in seinen Grundzügen. Allerdings erweiterten die FRCP von 1938 die Discovery auf erhebliche Weise.²⁶⁵ Die FRCP vereinheitlichten die Verfahren des Common Law und der Equity.²⁶⁶ Gleichzeitig gaben die FRCP die Own Case Rule und die Beschränkung auf unmittelbar prozessrelevante Beweismittel auf.²⁶⁷

Für die Erweiterung der Discovery bestand aus amerikanischer Sicht eine allgemeine Notwendigkeit. Während Europa dem gesellschaftlichen Wandel des 20. Jahrhunderts mit Maßnahmen der Gesetzgebung begegnete, geschah dies in den USA verstärkt durch die Rechtsprechung.²⁶⁸ Wichtige regulatorische Aufgaben, die in Deutschland das Straf- und

²⁵⁸ Vgl. Gerber, 34 Am. J. Comp. L. 745, 769 (1986); Stürner in FS Stiefel, 763, 782.

²⁵⁹ Stürner in FS Stiefel, 763, 775.

²⁶⁰ Stürner in FS Stiefel, 763, 775; Nakamura, ZJP 99 (1986), 1, 6.

²⁶¹ Stadler, Unternehmensgeheimnis, S. 68; Subrin, 39 B. C. L. Rev. 691, 695 (1998).

²⁶² Hazard/Tait/Fletcher/Bundy, Pleading and Procedure, S. 26; Junker, Discovery, S. 46; Stadler, Unternehmensgeheimnis, S. 68.

²⁶³ Junker, Discovery, S. 46.

²⁶⁴ Junker, Discovery, S. 46; Stadler, Unternehmensgeheimnis, S. 68.

²⁶⁵ Hazard/Tait/Fletcher/Bundy, Pleading and Procedure, S. 822; Junker, Discovery, S. 52 ff.

²⁶⁶ Hazard/Tait/Fletcher/Bundy, Pleading and Procedure, S. 28 f.; Junker, Discovery, S. 52; Main, 78 Wash. L. Rev. 429, 431 (2003).

²⁶⁷ Huber, Transnationale Modellregeln, S. 155 f.; Junker in Heldrich/Kono, Herausforderungen des internationalen Zivilverfahrensrechts, S. 103, 106.

²⁶⁸ Maultzsch, Streitentscheidung und Normbildung durch den Zivilprozess, S. 188 f.

Verwaltungsrecht und seine Behörden erfüllen, werden in den USA Privaten überlassen.²⁶⁹ So kommt der Klage auf Strafschadensersatz (Punitive Damages) im Bereich der Produzentenhaftung die Funktion der Gewerbeaufsicht zu.²⁷⁰ Im Kartellrecht dient die Klage auf dreifachen Schadensersatz (Treble Damages) der Disziplinierung.²⁷¹ Die Discovery ermöglicht es den Parteien, die Wahrheit ähnlich einer staatlichen Behörde zu erforschen.²⁷² Die hohe Parteiverantwortung und die umfassende Sachverhaltsaufklärung in der Discovery sind Ausdruck des amerikanischen Freiheitsdenkens.²⁷³ Schutzmaßnahmen vor Privaten, die eigenverantwortlich ihr Recht verteidigen, werden für nicht erforderlich erachtet.²⁷⁴ Entsprechend lax sind die gerichtlichen Kontrollen und die Schutzvorkehrungen für das Right to Privacy.

²⁶⁹ Maultzsch, Streitentscheidung und Normbildung durch den Zivilprozess, S. 189; Hess, AG 2005, 897, 898. Das Kostenrecht verwendet insofern den Begriff des privaten Staatsanwalts (Private Attorney General), vgl. Junker, Discovery, S. 96; Buxbaum, 26 Yale J. Int'l L. 219, 220 ff. (2001); Rubenstein, 57 Vand. L. Rev., 2129, 2130 ff. (2004).

²⁷⁰ Junker, Discovery, S. 96.

²⁷¹ Junker, Discovery, S. 96.

²⁷² Huber, Transnationale Modellregeln, S. 344.

²⁷³ Stürner in FS Stiefel, 763, 781.

²⁷⁴ Stürner in FS Stiefel, 763, 782 f.

US-amerikanische Discovery und deutsches
Datenschutzrecht

Der Konflikt im Falle der Dokumentenvorlage

Posdziech, M.

2017, XXXI, 262 S., Softcover

ISBN: 978-3-658-14409-8