Teil 4: Rechtsvergleichung

A. Der verfassungsrechtliche Datenschutz in den einzelnen Rechtsordnungen

I. Deutschland

1. Privatsphären- und Datenschutz

a) Privatsphärenschutz

In der deutschen Verfassung lässt sich das Recht auf Privatsphärenschutz nicht ausdrücklich vorfinden. Trotzdem werden die verschiedenen Aspekte und Bereiche, die in der privaten Lebensführung eine wichtige Rolle spielen, spezifisch und subsidiär umfassend geschützt. Dazu gehört das Recht auf die Unverletzlichkeit der Wohnung aus Art. 13 GG, das Recht auf das Brief-, Post- sowie Fernmeldegeheimnis aus Art. 10 GG und das allgemeine Persönlichkeitsrecht aus Art. 2. Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Mit diesen Grundrechten werden die konkreten Aspekte der Privatsphäre des Einzelnen einschließlich der Wohnung und des Fernmeldegeheimnisses geschützt.

Zum Schutz vor dem Eingriff in die Privatsphäre der Bürger als einen der wesentlichen Bestandteile des verfassungsrechtlichen Persönlichkeitsschutzes hat der Bundesgerichtshof in der Leserbrief-Entscheidung im Rahmen der Zivilrechtsprechung erstmals das allgemeine Persönlichkeitsrecht als ein verfassungsmäßig gewährleistetes Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 anerkannt. Damit wird dem Einzelnen ein räumlich und thematisch bestimmter Bereich garantiert, der grundsätzlich frei von unerwünschter staatlicher Einsichtnahme bleiben soll. Aus dem allgemeinen Persönlichkeitsrecht hat die Rechtsprechung die verschiedenen Ausprägungen der Privatsphäre entwickelt: das Recht auf sexuelle Selbstbestimmung, das Recht auf individuelle Selbstbestimmung, das Recht auf wirtschaftliche Selbstbestimmung, das Recht am eigenen Wort, das Recht auf Selbstdarstellung, das Recht an der eigenen Wohnung und das Recht an den eigenen Daten. Außerdem hat die Rechtsprechung eine Möglichkeit eröffnet, um den Einzelnen auch gegen neuartige Gefährdungen der freien Persönlichkeitsentfaltung zu schützen, indem sie den Schutzbereich des allgemeinen Persönlichkeitsrechts nicht abschließend definiert hat.

b) Die Bedeutung des Datenschutzes für den Privatsphärenschutz

In der deutschen Verfassung ist auch das Recht auf Datenschutz nicht ausdrücklich genannt. Der Privatsphärenschutz sieht sich jedoch aufgrund des modernen technischen Fortschritts mit neuen Herausforderungen konfrontiert. Die automatisierte Datenverarbeitung eröffnet die Möglichkeit, personenbezogene Daten schnell miteinander zu verknüpfen, zu übermitteln und in neue Zusammenhänge zu bringen. Der moderne Fortschritt der Datenverarbeitung erfordert ferner – über den Schutz von Wohnung und Fernmeldegeheimnis und das allgemeine Persönlichkeitsrecht hinaus, das von der Rechtsprechung entwickelt und konkretisiert wird – den Schutz der selbstständigen Herrschaft über personenbezogene Daten. Einen neuen Horizont für den Umgang mit der neuen Rechtsmaterie des Datenschutzes hat das Volkszählungsurteil des Bundesverfassungsgerichts gesetzt. In diesem Urteil hat das Bundesverfassungsgericht die Grundrechtsberührung der Informationsverarbeitung anerkannt, das Grundrecht auf informationelle Selbstbestimmung als einen weiteren spezifischen Aspekt der Privatsphäre aus Art 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und einige wichtige Schlüsse daraus gezogen.

Das Bundesverfassungsgericht erkennt das Potenzial der Gefährdung der freien Persönlichkeitsentfaltung, das den Möglichkeiten der modernen Datenverarbeitung innewohnt, wobei es das Recht auf informationelle Selbstbestimmung als eine Ausprägung des allgemeinen Persönlichkeitsrechts wahrgenommen hat, das den Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten schützt. Das heißt, das Bundesverfassungsgericht erkennt die Notwendigkeit des Datenschutzes als einen weiteren Aspekt des Privatsphärenschutzes an und präzisiert nicht nur das allgemeine Persönlichkeitsrecht aus der Perspektive des Datenschutzes, sondern arbeitet daraus auch das Recht auf informationelle Selbstbestimmung heraus. Außerdem entwickelt das Bundesverfassungsgericht das Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme.

c) Der verfassungsrechtliche Datenschutz

Das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht unter dem Aspekt des Datenschutzes aus dem allgemeinen Persönlichkeitsrecht abgeleitet hat, gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personen-

bezogenen Daten zu bestimmen.[593] Das Gericht erkennt damit die Notwendigkeit des Schutzes dieser Befugnis unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung an. Diese Anerkennung beruht auf den folgenden Erkenntnissen:

1. Die freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten voraus.
2. Die Bürger sind mit den Einzelheiten der Datenverarbeitungsvorgänge unter den modernen Datenverarbeitungsbedingungen nicht vertraut. Die automatische Datenverarbeitung ermöglicht es, personenbezogene Daten unbegrenzt zu speichern und jederzeit in Sekundenschnelle abzurufen. Außerdem können die personenbezogenen Daten mit anderen Datensammlungen zu einem teilweisen oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden.
3. Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum, da ein im Grunde belangloses Datum durch die der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten einen neuen Stellenwert erhalten kann.
4. Die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung kann die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen oder zu entscheiden, wesentlich einschränken.

Das Bundesverfassungsgericht entschied, den neuen Gefährdungen der Privatsphäre durch die automatisierte Datenverarbeitung mit Hilfe des Rechts auf informationelle Selbstbestimmung wirksam entgegenzutreten. In diesem Zusammenhang hat das Bundesverfassungsgericht einige Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung gestellt: Gesetzesvorbehalt, Normenklarheitsgebot, Verhältnismäßigkeitsgrundsatz, Zweckbindungsgrundsatz sowie Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung. Damit wurden einheitliche Grundsätze als ein Prüfungsstab für jeden Eingriff in personenbezogene Daten geschaffen.

Neben dem Datenschutz durch das Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht mit seinem Online-Durchsuchungsurteil auch durch ein verfassungsrechtlich neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine weitere Ausprägung des allgemeinen Persönlich-

593 BVerfGE 120, 274 (312); BVerfGE 65, 1 (43).

keitsrechts auf den Datenschutz gezielt. Mit diesem IT-Grundrecht wird seitens des Bundesverfassungsgerichts der Versuch unternommen, die Lücken im Datenschutz zu schließen. Diese bestehen bezüglich der möglichen Infiltration gesamter informationstechnischer Systeme, die sich außerhalb einer Wohnung befinden, und bezüglich solcher Daten, die nach Anschluss eines Kommunikationsprozesses nicht mehr von Art. 10 GG gedeckt sind und mangels einzelner, punktueller Datenerhebungen auch nicht oder nicht ausreichend dem Recht auf informationelle Selbstbestimmung unterliegen. Abgesehen von der Frage, ob das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um den besonderen Schutz der Freiheit der Bürger willen erforderlich oder effektiv ist, lässt sich aus der Ableitung dieses Rechts von der Rechtsprechung feststellen, dass deutsche Recht das ausgeprägte Persönlichkeitsgefährdungspotenzial der modernen Datenverarbeitung wahrnimmt und gegen dieses Potenzial einen noch wirksameren Schutz der personenbezogenen Daten zu gewähren beabsichtigt. Die Position der Rechtsprechung gewinnt eine größere Bedeutung in Deutschland, wo sich unter der generellen Idee der Schutzpflicht des Staates auch eine Pflicht des Staates abzeichnet, aktive Maßnahmen zum Schutz der Privatsphäre von Individuen zu ergreifen.

2. Das einfachgesetzliche Datenschutzsystem

Im Sinne eines einheitlichen und umfassenden Datenschutzes erließ der Gesetzgeber in Deutschland im Jahr 1977 das Bundesdatenschutzgesetz, das sowohl in der Bundesrepublik als auch in den einzelnen Ländern Anwendung findet. Das BDSG regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden. Jede Datenverarbeitung – Datenerhebung, -verarbeitung und -nutzung – im öffentlichen und nichtöffentlichen Sektor wird in diesem Gesetz geregelt, jedoch auf unterschiedliche Weise. In der deutschen Rechtsordnung ist die Verarbeitung personenbezogener Daten grundsätzlich verboten und daher nur auf Basis eines Erlaubnistatbestandes zulässig.

II. USA

1. Privacy Protection und Datenschutz

a) Privacy Protection

Das Recht auf *privacy* wird von der US-amerikanischen Rechtsprechung anerkannt und erweitert. Der Begriff „privacy" wird in der US-amerikanischen Verfassung jedoch nicht genannt. Vor allem im Hinblick auf die Vagheit der Bedeutung von *privacy* gab es vielfältige Versuche, den Begriff zu definieren. Den verfassungsrechtlichen Schutz des Rechts auf *privacy* anerkannte der Supreme Court aber erst mit der *Griswold*-Entscheidung. Anfangs wurde der verfassungsrechtliche Schutz dieses Rechts hauptsächlich im Kontext des vierten Verfassungszusatzes diskutiert. Ursprünglich wurde das Recht auf *privacy* nur gegen das materielle Betreten eines verfassungsrechtlich geschützten Raums verfassungsrechtlich geschützt.[594] Dementsprechend wurde kein verfassungsrechtlicher Schutz gegen die Überwachung von Telefonleitungen gewährt, solange kein physisches Betreten der Wohnung erfolgte.

Der technische Fortschritt und die ausdrückliche Anerkennung des Rechts auf *privacy* veranlassten den Supreme Court später jedoch dazu, seine Ansicht zu ändern. In der *Katz*-Entscheidung ersetzte der Supreme Court hinsichtlich des Schutzes des Rechts auf *privacy* das Kriterium des materiellen Betretens eines verfassungsrechtlich geschützten Raums durch das Kriterium einer begründeten Erwartung auf *privacy*. Gemäß der *Katz*-Prüfung wird im Rahmen der subjektiven Prüfung (*personal agency*) geprüft, ob der Einzelne eine Erwartung auf *privacy* hat, während im Rahmen der objektiven Prüfung herauszufinden ist, ob diese Erwartung gesellschaftlich als begründet anerkannt werden kann. Damit ist ein staatliches Handeln auch ohne physisches Betreten als ein Eingriff in das Recht auf *privacy* anzusehen, wenn eine begründete Erwartung auf *privacy* anerkannt wird. Jede Person genießt somit den verfassungsrechtlichen Schutz ihrer *privacy*, mit einigen Ausnahmen, wenn sie eine begründete Erwartung auf *privacy* hat. Für die Durchsuchung durch die Strafverfolgungsbehörden ist ein *warrant* erforderlich, der durch einen *probable cause* gestützt wird.

Angesichts des technischen Fortschritts stellt sich jedoch eine weitere Frage, und zwar, ob der Einzelne eine bestimmte Tätigkeit, die eine Erwartung auf *privacy* hat, ausüben kann, auch wenn er die eingesetzte neuartige

---

594 Olmstead v. United States, 277 U. S. 438 (457 f.).

Technologie nicht kennt. In diesem Zusammenhang hat der Supreme Court der *Katz*-Prüfung ein weiteres Kriterium hinzugefügt, nämlich die Gewöhnlichkeit der eingesetzten Technologie im Hinblick auf *personal agency*.

b) Die Bedeutung des Datenschutzes für die Privacy Protection

Aus den zahlreichen Versuchen, den Begriff der *privacy* zu definieren, können die informationelle Privatheit, die Privatheit der Kommunikation und die körperliche Privatheit als die Hauptelemente extrahiert werden. Allerdings lässt sich feststellen, dass das Recht auf *privacy* nicht abschließend bestimmt werden kann. Es besteht daher die Möglichkeit, dass den Begriffen „Privacy Protection" und „Datenschutz" in der US-amerikanischen Rechtsordnung mehr oder minder dieselbe Bedeutung zukommt. Zur vollständigen und sinnvollen Rechtsvergleichung wäre es daher erforderlich, den weiten Begriff der Privacy Protection auf die Unterkategorie des Datenschutzes zu reduzieren und diesen zu untersuchen. Dadurch soll der Schutz der informationellen Privatheit im Vordergrund stehen.

c) Der verfassungsrechtliche Datenschutz

Auch mit Bezug auf die informationelle Privatheit wendet der Supreme Court die Katz-Prüfung an. Wird eine begründete Erwartung auf *privacy* anerkannt, stellt ein staatliches Handeln einen Eingriff in die informationelle Privatheit dar.

Hiermit wurde u. a. das Recht anerkannt, Mitgliederlisten vor einer staatlichen Stelle geheim zu halten. Der Supreme Court hat den vierten Verfassungszusatz über lange Zeit hinweg sowohl im Hinblick auf personenbezogene Daten unter der Herrschaft Dritter oder auf Daten ohne Inhalt – z. B. Telefonnummern –[595] als auch im Hinblick auf Daten beschämender Natur[596] als unanwendbar angesehen. In Anlehnung an den Fall *Roe v. Wade* hat der Supreme Court jedoch Leitlinien zu den verfassungsrechtlich geschützten Informationen vorgelegt:

595 Smith v. Maryland, 442 U. S. 735 (742).
596 Paul v. Davis, 424 U. S. 693 (713).

1. Der Einzelne hat das Recht, die Offenlegung von persönlichen Angelegenheiten durch staatliche Akteure zu verhindern.
2. Mit diesem Recht ist eine Pflicht auf Seiten des Staates verbunden, die Informationen zu schützen, zu deren Preisgabe dieser den Einzelnen zwingt.
3. Informationen, die eng mit den *fundamental areas* verbunden sind, werden durch das Selbstbestimmungsrecht geschützt und rechtfertigen einen stärkeren Schutz des verfassungsrechtlichen Rechts auf informationelle Privatheit.

In einer grundsätzlichen Entscheidung im Hinblick auf das Recht auf informationelle Privatheit[597] hat der Supreme Court im Jahr 1965 festgestellt, dass das Recht auf *privacy* als „das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten" zu verstehen sei. Damit wurde das Recht auf informationelle Privatheit und dessen verfassungsrechtlicher Schutz anerkannt. Dem entspricht die Nixon-Entscheidung. Trotz dieser Auslegung erhielt der Supreme Court die in den beiden Fällen jeweils angegriffene Verordnung und Regelung aufgrund einer Interessenabwägung aufrecht.

Nach der Bewertung der Circuit Courts haben die Entscheidungen des Supreme Courts zwar das Interesse des Einzelnen an einer Vermeidung der Offenlegung seiner persönlichen Angelegenheiten zum einen und zum anderen das Interesse an der Selbstbestimmung bei wichtigen Entscheidungen klar festgestellt, der Supreme Court habe jedoch keine nachvollziehbare Leitlinie vorgelegt, die auf Fälle anwendbar ist, welche die informationelle Privatheit betreffen. Die Circuit Courts entwickelten daher ihrerseits eine nützliche Abwägungsgleichung. Mit Hilfe dieser Abwägungsgleichung war die Vielzahl der Fälle bezüglich der informationellen Privatheit im Rahmen des Circuit Court entschieden.

Der Supreme Court beschäftigte sich in NASA v. Nelson im Jahr 2011 wieder mit dem Recht auf informationelle Privatheit. Er hat hier den verfassungsrechtlichen Schutz des Rechts auf informationelle Privatheit nur implizit anerkannt und aufgrund einer Abwägung festgestellt, dass die Hintergrundprüfung von der NASA das implizit anerkannte Recht nicht verletzt hat.

Daraus werden die folgenden Schwächen in der US-amerikanischen verfassungsrechtlichen Rechtsprechung zum Datenschutz ersichtlich:

---

597 Whalen v. Roe, 429 U. S. 589.

1. Das Recht auf *privacy* umfasst das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten. Der Supreme Court gewährt lediglich vor der öffentlichen Bekanntgabe Schutz, jedoch nicht vor der unbegrenzten Datenerhebung, -speicherung, -nutzung und internen Übermittlung personenbezogener Daten innerhalb öffentlicher Stellen.
2. Der verfassungsrechtliche Schutz des Rechts auf informationelle Privatheit wird nur implizit, aber nicht ausdrücklich anerkannt.
3. Angesichts der Abwägungsgleichung der Circuit Courts werden die personenbezogenen Daten unterschiedlich, nämlich je nach Art ihrer Sensibilität, geschützt.
4. In der verfassungsrechtlichen Nachprüfung stellt sich lediglich die Frage, ob Sicherungsmaßnahmen vorgesehen sind, aber nicht, ob sie hinreichend sind, um die personenbezogenen Daten vor der unbegrenzten Erhebung, Speicherung, Nutzung und Weitergabe zu schützen.

Diese Schwächen werden insofern noch hervorgehoben, als es nach US-amerikanischer Dogmatik keine Vorstellung von einer Schutzpflicht des Staates gibt, aktive Maßnahmen zum Schutz der *privacy* von Individuen zu ergreifen, und weil daher die aus der US-Verfassung ableitbaren Rechte ausschließlich als Abwehrrechte gegenüber dem Staat zu verstehen sind.

2. Das einfachgesetzliche Datenschutzsystem

Es fehlt in den USA an einem umfassenden Auffangdatenschutzgesetz. Es gibt lediglich bereichsspezifische Gesetze, die nur bestimmte Fälle einer Datenverarbeitung regeln. Demnach stützen sich die USA im Rahmen des Datenschutzes auf einen Flickenteppich eng fokussierter sektoraler Gesetze und freiwilliger Selbstregulierung. Die Datenschutzgesetze können je nach Normadressaten in zwei Kategorien aufgeteilt werden: zum einen Datenschutz im öffentlichen Sektor, zum anderen Datenschutz im privaten Sektor.

Diesem bereichsspezifischen Regelungsansatz gemäß ist die Verarbeitung von personenbezogenen Daten grundsätzlich zulässig, sofern keine rechtliche Grundlage für das Verbot einer Verarbeitung oder kein bereichsspezifisches Gesetz, das die Verarbeitung einschränkt, besteht.[598]

598 *Schwartz*, Zur Architektonik des Datenschutzes in den USA, in: *Stern/Pfeifer/Hain*, Datenschutz im digitalen Zeitalter, S. 110.

Aufgrund der schieren Menge der einschlägigen Gesetze ist es unmöglich, diese alle übersichtlich darzustellen. Unter diesen Gesetzen besonders zu beachten ist jedoch der Privacy Act. Der Privacy Act[599] schützt als direkte gesetzgeberische Folge der sog. Watergate-Affäre die Privaten gegen hoheitliche Eingriffe in deren Privatsphäre. Der wesentliche Grundsatz des Privacy Act besteht darin, die Datensammlung soweit möglich bei der betroffenen Person durchzuführen.[600] Außerdem wird betroffenen Personen ein Recht auf Einsichtnahme und gegebenenfalls auf Berichtigung der über sie gesammelten Daten gewährt.[601] Der Privacy Act ist deshalb von so großer Bedeutung, weil er das erste gesamtstaatliche Gesetz zum Schutz Privater gegen hoheitliche Eingriffe in deren Privatsphäre war. Er findet allerdings nur bei Regierungsstellen der Bundesbehörden, nicht bei Regierungsstellen der einzelnen föderalen Staaten Anwendung.

Neben dem Schutz der Privatsphäre vor hoheitlichen Eingriffen dienen verschiedene weitere Normen zum Datenschutz für den privaten Bereich, etwa der Fair Credit Reporting Act und der Gramm-Leach-Billey-Act für Finanzdienstleister sowie der Electronic Communications Privacy Act und der Children's Online Privacy Protection Act im Bereich der Telekommunikation und der neuen Medien.

Wie bereits erwähnt, fehlt ein allgemeines und bereichsübergreifendes Gesetz zum Schutz personenbezogener Daten sowohl für den öffentlichen als auch für den privaten Sektor. Auch wenn es im öffentlichen Sektor ein gesamtstaatliches Gesetz gibt, ist dieser Schutz begrenzt.

III. Vergleich

1. Privatsphärenschutz

In den beiden Rechtsordnungen wird ein Recht auf Privatsphäre nicht ausdrücklich genannt. Während die Bedeutung der Privatsphäre in der deutschen Rechtsdogmatik relativ einheitlich zu verstehen ist, ist der Begriff der *privacy* in den USA je nach Kontext sehr unterschiedlich zu verstehen.

Zum Zweck des Privatsphärenschutzes werden in Deutschland verschiedene Aspekte und Bereiche, die eine bedeutungstragende Rolle im Privatsphärenschutz spielen, verfassungsrechtlich geschützt. Dem Schutz der

599 5 U. S. C. A. § 552a von 1974.
600 5 U. S. C. A. § 552a (e).
601 5 U. S. C. A. § 552a (d).

Privatsphäre dient neben den Freiheitsrechten aus Art. 13 und Art. 10 vor allem das allgemeine Persönlichkeitsrecht. Dieses Recht verpflichtet alle staatliche Gewalt, die private Sphäre der Grundrechtsträger als individuelle Handlungssphäre und Sphäre der Intimität zu schützen.[602] Mit diesem Recht werden vielfältige Ausprägungen der Privatsphäre geschützt. Die Reaktionen auf neuartige Herausforderungen der freien Persönlichkeitsentfaltung sind dadurch möglich, dass das allgemeine Persönlichkeitsrecht nicht abschließend definiert ist.

In den USA hingegen wurde das Recht auf *privacy* von der Rechtsprechung aus *penumbras* und *emanations* mehrerer Verfassungszusätze gefasst und hauptsächlich im Kontext des vierten Verfassungszusatzes diskutiert. Die *privacy protection* konzentrierte sich daher auf den verfassungsrechtlich geschützten Raum und das physische Betreten desselben. Verfassungsrechtlich nicht geschützter Raum oder der Einsatz von Technik ohne physisches Betreten des privaten Raums im buchstäblichen Sinne genoss hingegen keinen verfassungsrechtlichen Schutz im Sinne der *privacy*. Dieses relativ enge Verständnis der *privacy protection* erfuhr mit dem neuen Kriterium einer begründeten Erwartung auf *privacy* nach der *Katz*-Entscheidung eine erhebliche Erweiterung. Weist der Einzelne eine Erwartung auf *privacy* auf und kann die Erwartung als gesellschaftlich betrachtet begründet angesehen werden, wird das Recht auf *privacy* anerkannt. Dadurch wurde die Entscheidung für die *privacy protection* mit Hilfe des Raums und des physischen Betretens aufgehoben. Der technische Fortschritt stellt jedoch eine neue Herausforderung bezüglich der Frage dar, ob der Einzelne eine Erwartung auf *privacy* aufweist. Der Supreme Court musste dabei die Schwierigkeit berücksichtigen, dass der Einzelne eine Erwartung auf *privacy* schafft, wenn die eingesetzte neuartige Technik allgemein nicht gewöhnlich ist. Die *privacy protection* in der US-amerikanischen Rechtsordnung wird somit durch die *Katz*-Prüfung und zusätzlich die Gewöhnlichkeit der eingesetzten Technik gewährt. Daraus lässt sich folgern, dass die US-Verfassung den Schutz des Privatlebens i. w. S. für einen engen, inneren und speziellen Bereich zumindest vor hoheitlichen Eingriffen garantiert. Damit wurde zwar der Rahmen festgelegt, der bestimmte Sphären von Privatheit garantiert, es sind dabei jedoch nur geringe Möglichkeiten gegeben, einen Schutz herbeizuführen, der alle Bereiche des Privatlebens umfasst.[603]

602 Vgl. *Kunig*, Grundgesetz-Kommentar, Art. 2 Rn. 32.
603 *Genz*, Datenschutz in Europa und den USA, S. 48.

2. Der verfassungsrechtliche Datenschutz

Durch zahlreiche Entscheidungen des Bundesverfassungsgerichts – z. B. seine Urteile zur Volkszählung, zur Vorratsdatenspeicherung und zur Online-Durchsuchung – ist in Deutschland ein starker verfassungsrechtlicher Datenschutz ohne Rücksicht auf die Sensibilität der Daten abgesichert. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil das allgemeine Persönlichkeitsrecht vor allem zu einem Recht auf informationelle Selbstbestimmung konkretisiert, damit der spezifische Datenschutz erfolgt. Im Zuge des Volkszählungsurteils hat das Bundesverfassungsgericht die Grundrechtsberührung der automatisierten Datenverarbeitung wahrgenommen und das Recht auf informationelle Selbstbestimmung entwickelt, um den Einzelnen gegen das der modernen Datenverarbeitung innewohnende Persönlichkeitsgefährdungspotenzial zu schützen. Das Recht ist als ein Anspruch des Einzelnen zu verstehen, die Bedingungen zu kontrollieren, unter denen personenbezogene Daten erlangt, übermittelt oder zur Nutzung gebraucht werden können. Durch dieses Verständnis des Rechts auf informationelle Selbstbestimmung wird der Schutz des Einzelnen vor der unbegrenzten Erhebung, Speicherung, Nutzung und Weitergabe seiner Daten unter den gegenwärtigen Datenverarbeitungsbedingungen garantiert. Neben der Ableitung dieses Rechts werden von der Rechtsprechung einige konkrete Anforderungen gestellt, um den materiellen Datenschutz zu verwirklichen. Zu diesen Anforderungen gehören der Gesetzesvorbehalt, das Normenklarheitsgebot, der Verhältnismäßigkeitsgrundsatz, der Zweckbindungsgrundsatz und die Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen. Außerdem legt das Recht auf informationelle Selbstbestimmung dem Staat auch Schutzpflichten gegenüber Privaten auf.

Demgegenüber wird der Datenschutz in den USA unter dem Begriff „privacy" subsumiert, der nicht abschließend definiert werden kann.[604] Der Rahmen, der die bestimmten Bereiche des Rechts auf *privacy* garantiert, wird von der Rechtsprechung festgelegt. In Bezug auf das Recht auf informationelle Privatheit unter dem Recht auf *privacy* wird das Interesse des Einzelnen, die Offenlegung seiner persönlichen Angelegenheiten zu vermeiden, von der Rechtsprechung anerkannt und auf der Ebene der Circuit Courts wurde eine Abwägungsgleichung entwickelt. Jedoch betrifft dieser Rahmen lediglich den Schutz vor der öffentlichen Bekanntgabe von personenbezogenen Daten und gibt keine Garantie eines umfassenden

604 Vgl. *Genz*, Datenschutz in Europa und den USA, S. 39 m. w. N.

Rechts zur Datenkontrolle. Ein Recht des Einzelnen, seine Daten eigenständig zu kontrollieren, sprich die unbefugte oder übermäßige Erhebung, Speicherung, Nutzung und Weitergabe seiner Daten zu verhindern und selbst darüber zu entscheiden, ob, wann, wie und in welchem Maße seine Daten öffentlich bekannt gemacht werden, wird noch nicht wahrgenommen. Außerdem geht selbst dieser von der Rechtsprechung herausgearbeitete Schutz der informationellen Privatheit noch nicht über den Einzelfall hinaus.[605] Es gibt also keinen umfassenden Datenschutz, der dem Schutz durch das Recht auf informationelle Selbstbestimmung entspricht. Einen allgemeingültigen und verlässlichen Datenschutz kann der Einzelne in diesem Fall nicht erwarten. Wegen dieses Mangels an verfassungsrechtlicher Absicherung im Hinblick auf das Recht auf informationelle Privatheit kann ein bereichsübergreifender Privatsphären- und Datenschutz nicht erreicht werden.

Während der Datenschutz in Deutschland bereits grundrechtlich verankert ist, dieser den höchstgerichtlichen Schutz erfahren hat und die konkreten Anforderungen zum materiellen Datenschutz von der Rechtsprechung entwickelt wurden, scheint der US-amerikanische Datenschutz angesichts des Umstands, dass ein Recht auf informationelle Privatheit verfassungsrechtlich noch nicht umfassend abgesichert ist, noch einen weiten Weg vor sich zu haben.

3. Datenschutzsystem

Der Unterschied zwischen dem deutschen und dem US-amerikanischen Datenschutzrechtssystem beruht vor allem auf dem Datenschutzansatz. In Deutschland fungiert das BDSG als ein umfassendes Datenschutzgesetz, unter dem jede Datenverarbeitung grundsätzlich verboten ist, wenn es keinen gesetzlichen Erlaubnistatbestand gibt. In den USA hingegen wurde es vermieden, allgemeine Datenschutzgesetze und -vorschriften aufzustellen. Für diesen Zweck wurde eine bereichsspezifische Sondergesetzgebung mit einer Unterstützung der Selbstregulierung ausgewählt. Hier ist jede Datenverarbeitung grundsätzlich zulässig, soweit es gesetzlich nicht anders bestimmt ist.

Die rasch gewachsenen Möglichkeiten der elektronischen Datenverarbeitung machen einen umfassenden gesetzlichen Datenschutz erforderlich. Denn der sektorale Ansatz hinterlässt notwendigerweise eine Vielzahl

605 Vgl. *Genz*, Datenschutz in Europa und den USA, S. 49 m. w. N.

von wesentlichen Bereichen, in denen ein Schutz der informationellen Privatheit bzw. personenbezogener Daten nicht sichergestellt ist. Lediglich grundlegende Schranken- und Steuerungsmechanismen der Datenverarbeitung durch bereichsübergreifende Vorgaben zum Datenschutz können einen sicheren Rechtsschutz im Rahmen des Umgangs mit personenbezogenen Daten versprechen.

Das unterschiedliche Datenschutzniveau zwischen der EU und den USA hat zu einer Vereinbarung über die Grundsätze des sog. „sicheren Hafens" zwischen der EU und dem Handelsministerium (Department of Commerce) der USA geführt.[606] Den Ausgangspunkt für diese Vereinbarung bildet die EU-Datenschutzrichtlinie,[607] die die Mindeststandards für den Datenschutz beschreibt, die in allen Mitgliedstaaten der EU durch nationale Gesetze sichergestellt werden müssen, um den freien Verkehr personenbezogener Daten innerhalb der EU durch die Schaffung eines gleichen Datenschutzniveaus in allen EU-Mitgliedstaaten zu erleichtern. Die Richtlinie legt die Verpflichtungen für die Verarbeiter von personenbezogenen Daten und die Rechte für die Betroffenen fest. Gemäß der Richtlinie ist ein Datentransfer in Drittstaaten, die über kein mit dem EU-Recht vergleichbares Datenschutzniveau verfügen, verboten. Es wurde festgestellt, dass die USA kein angemessenes Schutzniveau bieten, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Art. 25 Abs. 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland feststellen kann, sprich, dass sie darüber befinden kann, ob ein Drittland hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet oder nicht. In diesem Zusammenhang können sich Organisationen in den USA freiwillig darauf verständigen, die Safe-Harbor-Grundsätze

606 Safe Harbor, Kommissionsentscheidung 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.

607 Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Die Richtlinie wurde ab dem 25. Mai 2018 durch die Verordnung (EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) ersetzt.

einzuhalten, und diese Einhaltung öffentlich bestätigen. Dies führt zu der Annahme, dass diese Organisationen den Angemessenheitsstandard der EU-Richtlinie für den Datenschutz erfüllen. Infolgedessen kann der internationale Informationsaustausch zwischen Unternehmen in der EU und jenen Organisationen in den USA, die den Safe-Harbor-Bestimmungen entsprechen, stattfinden. Die Safe-Harbor-Vereinbarung enthält vor allem die folgenden Punkte: 1. Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über die Personen erhebt und verwendet und wie die Personen die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können; 2. An wen dürfen die Daten weitergegeben werden und welche Mittel sowie Wege sollten die Daten den Privatpersonen zur Verfügung stellen, damit die Verwendung und Weitergabe der Daten eingeschränkt werden können?

B. Datenschutz bei den konkreten Maßnahmen in den einzelnen Rechtsordnungen

I. Strafregister

Die Daten aus dem Strafregister spielen in jeder Phase des Strafverfahrens eine bedeutsame Rolle. Unter den Bedingungen der modernen Datenverarbeitung sollte der Schutz der im Strafregister gespeicherten Daten in Bezug auf den Schutz der Privatsphäre als eines Teils des Rechts auf Freiheit des Einzelnen jedoch ebenfalls im Vordergrund stehen. Denn die Speicherung strafrechtlich relevanter Daten ist zwar im Interesse der Öffentlichkeit, die Strafregistrierungen für den Zweck zukünftiger Verbrechensermittlungen und gerichtlicher Entscheidungsfindungen beizubehalten, greift aber in das informationelle Selbstbestimmungsrecht des Betroffenen ein. Ein ehemaliger Verurteilter hat das Recht, sein Leben ohne das Stigma von Strafregistrierungen zu führen.

Im Folgenden sollen die Ausgestaltungen des Strafregistersystems in Deutschland und den USA übersichtlich dargestellt und die beiden Systeme im Hinblick auf die Organisationsstruktur, die Erhebung, die Speicherung, die Übermittlung und die Weitergabe von Daten unter dem Aspekt von Einschränkungen zum Zweck des Datenschutzes miteinander verglichen werden.

1. Deutschland

a) Organisationsstruktur

Das deutsche Strafregistersystem besteht aus dem BZR als einem einheitlichen Strafregister und dem ZStV. Die Einrichtung und die Führung der beiden Register werden vor allem durch §§ 474–495 StPO ermächtigt. Entscheidungen gegen Jugendliche werden gesondert in das Erziehungsregister eingetragen, das in das BZR integriert ist. Damit wird den Besonderheiten des Jugendstrafrechts und seinen vorwiegend auf erzieherische Wirkungen abstellenden Maßnahmen Rechnung getragen. Bezüglich der Organisationsstruktur sollen das Erhebungs-, Speicherungs- und Übermittlungsverfahren von Daten in den Registern übersichtlich vorgestellt werden.

Bei einem Erhebungsvorgang beim BZR übermittelt eine mitteilungspflichtige Stelle der Registerbehörde mittels Fernübertragung die in das Register einzutragenden Inhalte. Die mitteilungspflichtigen Stellen schreibt § 1 Abs. 1 BZRGVwV im Einzelnen vor, die in das Register einzutragenden Inhalte § 3 BZRG. Damit das Register aktuell gehalten wird, ist die Mitteilungspflicht mit obligatorischen Mitteilungsfristen verbunden. Die Übermittlung soll bei Entscheidungen binnen eines Monats nach Eintritt der Vollziehbarkeit, Unanfechtbarkeit oder Rechtskraft mitgeteilt werden. Die mitgeteilten Daten erfahren elektronisch zahlreiche Plausibilitätsprüfungen und eine Identitätsfeststellung und werden danach eingeordnet. Die Speicherung erfolgt erst zu diesem Zeitpunkt. Die im Register gespeicherten Daten werden mittels Datenübertragung angefragt und daraufhin übermittelt (Auskunftserteilung). Die Auskunftserteilung aus dem Register durch die Registerbehörde erfolgt entweder im Weg eines Führungszeugnisses oder einer unbeschränkten Auskunft. Bei dieser Stufe muss gewährleistet werden, dass ein unbefugter Zugriff Dritter auf die Daten wirksam abgewehrt wird und dass die dem jeweiligen Stand der Technik entsprechenden Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit – z. B. Verschlüsselungsverfahren im Falle der Nutzung allgemein zugänglicher Netze – getroffen werden.

Beim ZStV, das mit umfassenden und schnell verfügbaren Informationen über die bundesweit gegen einen Beschuldigten geführten Ermittlungs- und Strafverfahren der Staatsanwaltschaft zur Erleichterung der sachgerechten Führung eines Ermittlungsverfahrens eingerichtet wurde, lehnen sich die Erhebungs-, Speicherungs- und Übermittlungsverfahren teilweise an das Verfahren beim BZR an. Die Staatsanwaltschaften teilen

die einzutragenden Daten der Registerbehörde zu dem in § 492 Abs. 2 Satz 2 StPO genannten Zweck im Weg der Datenfernübertragung mit. Die einzutragenden Daten werden in § 492 Abs. 2 Satz 1 StPO und § 4 ZStVBetrV aufgeführt. Da dieser Regelungsbereich zum unmittelbaren Vorfeld des gerichtlichen Verfahrens gehört, wird die entsprechende Eintragung im ZStV automatisch gelöscht, wenn eine solche Entscheidung in das BZR eingetragen wird.[608] Eine Frist hierfür wird nicht festgelegt, auch wenn die ZStVBetrV vorschreibt, dass die Mitteilung erfolgen muss, sobald ein Strafverfahren anhängig wird. Mit diesen Informationen wird eine Vollspeicherung im Register erreicht. Die Datenübermittlung zur Anfrage und Auskunftserteilung erfolgt normalerweise per Datenfernübertragung. Die ZStVBetrV schränkt die Stellen ein, die eine Auskunft aus dem ZStV erhalten dürfen (ZStVBetrV § 6 Abs. 1 und 2).

b) Inhalt des Registers

Im BZRG werden die im BZR einzutragenden Daten ausführlich geregelt. Danach ist neben strafgerichtlichen Verurteilungen auch Weiteres im BZR zu speichern: strafgerichtliche Verurteilungen, Entscheidungen von Verwaltungsbehörden und Gerichten, Vermerke über Schuldunfähigkeit, gerichtliche Feststellungen nach § 17 Abs. 2, § 18 BZRG, nachträgliche Entscheidungen und Tatsachen und sogar strafgerichtliche Verurteilungen ausländischer Gerichte. Die Registeraufgabe wurde damit erheblich erweitert.[609] Das Eintragen von Entscheidungen und Anordnungen gegen Jugendliche regelt § 60 BZRG.

Die in das ZStV einzutragenden Daten regeln § 492 Abs. 2 StPO und § 4 ZStVBetrV. Danach sind nur die Personendaten der beschuldigten Person, die Daten zur Straftat, die Vorgangsdaten wie etwa die mitteilende Stelle, die sachbearbeitende Stelle der Polizei sowie die Aktenzeichen und die Daten zum Verfahrensstand zu speichern. Die Speicherung hängt nicht vom Gewicht der vorgeworfenen Taten ab, sondern es werden die Ermittlungsverfahrensdaten bezüglich aller beschuldigten Personen gespeichert.

608 *Gieg*, KK-StPO, § 494 Rn. 4.

609 In Bezug auf die erweiterte Aufgabe hat sich die Bezeichnung zutreffend von *Strafregister* zu *Bundeszentralregister* geändert (vgl. dazu oben Fn. 174).

c) Verwendung der Daten aus dem Register

Um die informationelle Selbstbestimmung des Einzelnen zu schützen, hat das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983[610] einige Anforderungen gestellt. Sie gelten auch für die Daten im Strafregister. Da bei der Verwendung der Daten aus dem Register stets die Gefahr besteht, dass hochsensible Daten wie etwa eine Verurteilung oder eine sonst eintragungspflichtige Tatsache gegen den Willen des Bestraften bekannt werden und diesem dadurch Nachteile entstehen, wird bei der Verwendung der Daten aus dem Register besondere Sorgfalt gefordert. Die Verwendung von Daten aus dem Strafregister wird deswegen unter verschiedenen Aspekten eingeschränkt.

Diejenigen, die Anfragen stellen und gegebenenfalls eine Auskunft aus dem Register erhalten dürfen, sind beim BZR nur der Betroffene – ausnahmsweise auch sein Vertreter oder auch die Behörde, wenn das Führungszeugnis zur Vorlage bei ihr vorgelegt wird – und die in § 41 BZRG genannten Stellen; beim ZStV sind es nur die in § 6 Abs. 1 und 2 ZStV-BetrV genannten Behörden. Das deutsche Strafregistersystem beschränkt also, wer Auskunft erhält.

Auskunft aus dem BZR kann entweder im Weg des Führungszeugnisses oder der unbeschränkten Auskunft erteilt werden. Je nach Auskunftsmöglichkeit gelten unterschiedliche Einschränkungen. Beim Führungszeugnis werden die Eintragungen im Register mit bestimmten Aufnahmenormen und -fristen verbunden. Die Aufnahmefristen richten sich nach der Höhe der Verurteilungen. Die Mitteilungspflicht an den Betroffenen wird in der Regel nicht vorgeschrieben, da ein Führungszeugnis grundsätzlich von ihm selbst beantragt wird. In das Führungszeugnis zur Vorlage bei einer Behörde hat die das Zeugnis erhaltende Behörde dem Antragsteller auf Verlangen Einsicht zu gewähren. Anders als beim Privatführungszeugnis unterliegt das Behördenführungszeugnis dem Zweckbindungsprinzip; es wird daher gefordert, dass die Behörde das Zeugnis zur Erledigung ihrer hoheitlichen Aufgaben benötigt (§ 31 Abs. 1 BZRG). Die Weitergabe von Führungszeugnissen hängt durchaus vom Willen des Betroffenen ab. Das Behördenführungszeugnis darf an eine andere Behörde weitergegeben werden, wenn der Betroffene damit einverstanden ist.

Die Situation ist eine andere, wenn es um unbeschränkte Auskünfte geht. In unbeschränkten Auskünften sind auch solche Eintragungen enthalten, die nicht in das Führungszeugnis aufgenommen werden. Die

610 BVerfGE 65, 1.

Eintragungen beeinflusst nur der Löschungsvorgang. Eine unbeschränkte Auskunft wird auf Ersuchen der berechtigten Stellen erteilt, ohne dass der Betroffene davon Kenntnis nimmt. Eine Person kann auf Antrag nur davon Kenntnis nehmen, welche Eintragungen über sie im Register enthalten sind. Man kann als Einzelner also nicht feststellen, ob irgendeine Behörde Auskunft über seine im Register gespeicherten Daten angefragt und danach erhalten hat. Die Zweckangabe wird bei einer Anfrage gesetzlich gefordert und die Zwecke werden je nach Behörde unterschiedlich aufgezählt, damit die Daten im Register vor dem übermäßigen Zugriff geschützt werden können – z. B. bei Anfragen von Gerichten, Gerichtsvorständen, Staatsanwaltschaften und Aufsichtsstellen für Zwecke der Rechtspflege. In einem Ersuchen muss also angegeben werden, aus welchem Grund eine Auskunft erforderlich ist, die dann auch ausschließlich zu dem genannten Zweck verwendet wird. Außerdem wird das Ersuchen grundsätzlich auf Einzelanfragen begrenzt. Unbeschränkte Auskünfte dürfen nur weitergegeben werden, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde. Darüber hinaus werden die Auskünfte nur den mit der Entgegennahme oder Bearbeitung betrauten Bediensteten erteilt. Dadurch soll dem Betroffenen die weitestgehende Geheimhaltung seiner Daten garantiert werden.

Die anfragenden und gegebenenfalls Auskunft aus dem ZStV erhaltenden Stellen sind gesetzlich auf die Strafverfolgungsbehörden eingeschränkt.[611] Die Daten im ZStV unterliegen dem Zweckbindungsprinzip. Die Daten dürfen also nur zum Zweck der Verwendung im Strafverfahren gespeichert, verändert und verwendet werden. Die im ZStV gespeicherten Daten werden zum Zweck der Strafrechtspflege verwendet, genauso wie bei unbeschränkten Auskünften, ohne dass der Betroffene davon Kenntnis nimmt. Außerdem flankieren die erforderlichen und angemessenen Maßnahmen die Verwendung personenbezogener Daten in diesem Bereich, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten sicherzustellen.

611 Ausnahmsweise darf auch den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst und dem Bundesnachrichtendienst Auskunft erteilt werden, sofern diesen Stellen ein Auskunftsrecht gegenüber den Strafverfolgungsbehörden zusteht. Das dient dazu, unnötigen Aufwand zu vermeiden.

d) Speicherdauer

Wie oben erwähnt, bleiben Eintragungen im BZR grundsätzlich nicht dauerhaft gespeichert. Das Gesetz eröffnet neben der Nichtaufnahme einer Eintragung in das Führungszeugnis die Möglichkeit der Tilgung, um das Rehabilitationsinteresse des Betroffenen in Rechnung zu stellen. Neben der vollständigen Entfernung von Eintragungen aus dem BZR gemäß §§ 16 Abs. 2, 24 und 63 BZRG erfolgt eine Tilgung aufgrund Fristablaufs oder aufgrund Anordnung der Registerbehörde. Die Anordnungsmöglichkeit der Tilgung dient der Einzelfallgerechtigkeit, die bei der fristgebundenen Tilgung nicht berücksichtigt wird; damit wird sie auf wenige Ausnahmefälle begrenzt. Die Tilgung aufgrund einer Anordnung erfolgt auf Antrag oder von Amts wegen nach der Entscheidung der Registerbehörde.

Das BZRG regelt die Tilgungsfristen je nach Höhe der Hauptstrafe. Nach einem Tilgungsfristablauf werden die Daten von einem besonderen Löschprogramm automatisch gelöscht. Die zu tilgenden oder schon getilgten Daten dürfen mit einigen Ausnahmen (§ 52 BZRG) nicht mehr verwertet werden (Verwertungsverbot, § 51 BZRG); daher genießt der Betroffene das Schweigerecht im Hinblick auf seine getilgten Daten. Auch wenn die Tilgungsfristen noch nicht abgelaufen sind, kann in besonderen Fällen die Tilgung aufgrund Anordnung der Registerbehörde vorkommen. Die Fälle sieht § 49 BZRG vor. Darüber hinaus dürfen Entscheidungen aus dem Register fristunabhängig entfernt werden, wenn sie in einem Wiederaufnahmeverfahren rechtskräftig aufgehoben wurden. § 24 BZRG regelt noch eine andere fristunabhängige Tilgungsmöglichkeit, um einem stetigen Anwachsen des Registers durch Belassen überholter Eintragungen entgegenzuwirken.[612] Amtsgerichte, Anstaltsleitungen oder amtliche Vertretungen der Bundesrepublik Deutschland müssen die Registerauszüge, die zur Einsichtnahme des Betroffenen gemäß § 42 BZRG herangezogen wurden, nach Einsichtnahme vernichten.

Die Speicherung bleibt grundsätzlich unberührt, bis die Eintragungen im ZStV in das BZR übernommen werden. § 494 StPO regelt die Ausnahmefälle: die versehentliche Eintragung der Daten, Doppelspeicherungen, den rechtskräftigen Freispruch, die unanfechtbare Ablehnung der Eröffnung des Hauptverfahrens, Verfahrenseinstellungen, die nicht nur vorläufig oder endgültig sind, und ein weiteres Verfahren zur Eintragung in das ZStV. Außerdem ist es gesetzlich vorgesehen, dass die ersuchende Stelle nach erfolgter Identifizierung alle übermittelten Daten, die sich nicht auf

612 *Tolzmann*, Bundeszentralregistergesetz, § 24 Rn. 4.

den Betroffenen beziehen, unverzüglich zu löschen hat; dies gilt auch bei einer unmöglichen Identifizierung.

Die im ZStV gespeicherten Daten werden nicht nur gelöscht, sondern unter bestimmten Umständen auch gesperrt. § 494 Abs. 3 i. V. m. § 489 Abs. 7 und 8 StPO führen die hierfür relevanten Umstände auf. Die Verwendung der gesperrten Daten beschränkt sich nur auf die Verwendung zu dem Zweck, für den die Löschung unterblieben ist, und auch soweit dies zur Behebung einer bestehenden Beweisnot unerlässlich ist.

2. USA

a) Organisationsstruktur

In den USA steht kein national zentralisiertes Strafregister, sondern das dezentralisierte III-System zur Verfügung, das ein zwischenstaatliches Computernetzwerk zum Datenaustausch zwischen dem Bund und den Einzelstaaten im Hinblick auf die Strafregistrierungen ist. Jeder Staat und auch das FBI (bezüglich bundesgesetzlicher Verbrechen) betreiben jeweils ihr eigenes Strafregister, die mittels des III-Systems durch einen Index-Pointer-Ansatz miteinander vernetzt sind. Das III-System wird vom NCIC beim FBI geführt. Das III-System gibt auf Ersuchen an, ob eine Person irgendwo im Land bereits registriert ist: falls ja, verweist der *Interstate Identification Index* die anfragende Behörde an das FBI und/oder an ein oder mehrere der staatlichen Register, die den ersuchten Datenbestand erhalten.

Die im Strafregister einzutragenden Daten werden zuerst im Strafregister desjenigen Staates erhoben und gespeichert, in dem ein Verbrechen strafverfolgend ermittelt und in dem gerichtliche Entscheidungen gegen den Betroffenen getroffen wurden. Der methodische Unterschied zwischen am NFF teilnehmenden Staaten und daran nicht teilnehmenden Staaten liegt innerhalb des III-Systems darin, die in eigenen Strafregistern gespeicherten Daten dem FBI mitzuteilen. Erstere senden dem FBI nur die ersten Registrierungsdaten (Fingerabdrücke und Identifikationsdaten) über jede Person, um den Index des III-Systems zu aktualisieren. Die Staaten speichern die anderen im Strafregister einzutragenden Daten immer wieder in ihrem eigenen Strafregister. Die Daten stehen für eventuelle Anfragen aus anderen Einzelstaaten oder aus zugelassenen Bundesbehörden zur Verfügung. Die nicht am NFF teilnehmenden Staaten leiten demgegenüber alle Strafregistrierungen an das FBI weiter. Mit allen mitgeteilten

Daten wird die Speicherung im NFF und zugleich die Aktualisierung des Index erreicht.

Die Regelungen des Zugangs zu den Daten und der Auskunftserteilung von Daten aus dem Register sind zwar von Staat zu Staat unterschiedlich, das Anfrage- und Auskunftsverfahren unter dem III-System läuft jedoch insgesamt ähnlich ab. Eine Anfrage über eine Person wird zunächst über das staatliche Telekommunikationsnetz an das staatliche Repository gestellt. Das staatliche Strafregister leitet die Anfrage dann über das NCIC-Netzwerk an den III-Computer weiter, der daraufhin die anfragende Behörde an das FBI und/oder an ein oder mehrere der staatlichen Strafregister verweist, von denen Strafregistrierungen über die Person erhalten werden. Das anfragende staatliche Strafregister kann die Daten mit Hilfe des NCIC-Netzwerks oder des *National Law Enforcement Telecommunications Systems* (NLETS-Netzwerk) direkt aus den angegebenen Quellen erhalten. Das Strafregister übermittelt die Antwort an die anfragende Behörde. Bei der Weitergabe, der Löschung sowie der Vernichtung der einmal angebotenen Antwort gilt keine Regelung oder Einschränkung.

b) Inhalt des Registers

Was in die staatlichen Strafregister eingetragen werden soll, ist nicht bundesgesetzlich geregelt. Über die in das Register einzutragenden Daten besteht keine Einigkeit zwischen den Einzelstaaten. Das führt dazu, dass Daten in einem Staat gespeichert, in einem anderen hingegen nicht gespeichert werden. Der Begriff der *criminal history records* umfasste ursprünglich nicht nur die strafgerichtlichen Verurteilungsdaten, sondern auch die Verhaftungsdaten, also auch die Strafverfahrensdaten ohne Verurteilung.

Unabhängig davon, was in einem staatlichen Strafregister registriert werden soll, ist der Datenaustausch unter dem III-System bundesgesetzlich geregelt. Zum einen erfolgt die Mitteilung der Strafregistrierung unter dem III-System nur für schwere und/oder erhebliche (*serious and/or significant*) Erwachsenen- und Jugendstraftaten.[613] Auch wenn auf staatlicher Ebene eine Datenspeicherung für minder schwere Straftaten erreicht wird, können die Daten nicht durch eine Suche des III-Systems herausgefunden werden. Zum anderen erfährt die Datenspeicherpraxis eine tendenziell allmähliche Erweiterung. Dies gilt insbesondere für Entscheidungen gegen Jugendliche. Die Daten für schwere Straftaten durch Jugendliche werden

613 28 C. F. R. § 20.32 (a).

deswegen nun in staatlichen Strafregistern gespeichert. Bei den *criminal history records* handelt es sich um Informationen, die von Strafverfolgungsbehörden über Personen gesammelt werden und die aus identifizierbaren Beschreibungen und Feststellungen von Verhaftungen, Festnahmen, Anklageschriften oder anderen formellen Strafanzeigen einschließlich daraus resultierender Freisprüche, Verurteilungen oder Strafvollzugskontrollen bestehen.[614] Dabei werden für Identifizierungsdaten normalerweise Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Geschlecht, Rasse, physikalische Eigenschaften wie Haar- und Augenfarbe, Größe, Gewicht und alle auffälligen Narben, Marken, Tattoos oder auch Fingerabdrücke und für Dispositionsdaten die Daten über alle Entscheidungen über Personen gespeichert.

c) Verwendung der Daten aus dem Register

Wer berechtigt ist, die Strafregistrierungen bei einer Registerbehörde zu ersuchen und daraus Auskunft zu erhalten, regelt 42 U. S. C. § 14616 IV (b) und 20 C. F. R. § 20.21 (b) und § 20.33 (a). Dort ist jede Auskunft zweckgebunden. Danach stehen die Strafregistrierungen sowohl den Strafverfolgungsbehörden als auch anderen Behörden für nichtstrafrechtliche Zwecke zur Verfügung, für die das Bundes-, Bundesordnungs- oder Staatsgesetz erlaubt, die nationalen Indexprüfungen zu verwenden. Darüber hinaus kann der Betroffene eine Kopie eines im Strafregister eingetragenen Datensatzes gegen eine Gebühr in Höhe von 18 USD erhalten, um es einzusehen oder inhaltlich zu ändern, korrigieren oder aktuell zu halten.[615] Diese Einschränkung der Personen, die zum Zugriff auf die Strafregistrierungen berechtigt sind, ist aus drei Gründen in der Wirksamkeit begrenzt. Erstens ist es in den USA zulässig, dass Arbeitgeber eine Hintergrundprüfung[616] über Arbeitsbewerber nur mit deren Zustimmung vornehmen.[617] Eine Studie der *Society for Human Resource Management* zeigte aber, dass

614 42 U. S. C. § 14616 *Overview* (b) (4) (A).

615 28 C. F. R. § 16.30 bis 34.

616 Eine Hintergrundprüfung umfasst eine Überprüfung der Geschäfts-, Straf-, Beschäftigungs- und/oder Finanzdaten einer Person.

617 Wenn Arbeitgeber unter der *third-party-doctrine* eine Hintergrundprüfung (einschließlich Kredit-, Straf- und Vergangenheitsarbeitgeberprüfungen) durchführen, wird diese durch den Fair Credit Reporting Act von 1970 (FCRA) abgedeckt. Ungefähr 30 Prozent der Arbeitgeber führen eine offizielle Hintergrundprüfung von Bewerbern durch und etwas weniger als die Hälfte aller Arbeitge-

in der Realität mehr als 80 Prozent der amerikanischen Arbeitgeber kriminalpolizeiliche Überprüfungen potenzieller Mitarbeiter durchführen.[618] Es gibt ferner private Informationsdienstunternehmen, die gegen eine geringe Gebühr eine Internetsuche nach Strafregistern zu den kriminalpolizeilichen Überprüfungen anbieten. Diese Unternehmen sind in gewissem Umfang durch den Fair Credit Reporting Act *(FCRA)* geregelt. Staatliche Gesetze regeln diese Unternehmen jedoch nicht direkt, sondern verbieten Arbeitgebern nur, Strafregistrierungen in Arbeitsentscheidungen zu verwenden.[619] Einen zweiten Grund bilden die bei den Gerichten gespeicherten und von diesen geführten Daten, die durch das E-Government-Gesetz von 2002 öffentlich leicht zugänglich geworden sind. Einen dritten Anlass zum Zweifel an der Wirksamkeit geben die sogenannten Megans Gesetze, die die Identitäten, Adressen und Straftaten von Sexualstraftätern über das Internet öffentlich zugänglich machen. Diese Gesetze führen dazu, dass jeder die Daten von Sexualstraftätern erhalten kann.

Das Anfrage- und Auskunftsverfahren läuft meist online über spezielle Computer-Terminals ab. Dabei wird gesetzlich gefordert, dass ein Verfahren verfügbar ist, das die Genauigkeit und die Vertraulichkeit der Daten schützt und das sicherstellt, dass die Daten nur von den Berechtigten für berechtigte Zwecke verwendet werden und dass die Abfragen grundsätzlich auf Einzelanfragen begrenzt sind.[620] Aber die Einzelheiten werden den einzelnen Staaten überlassen. Um einen unbefugten oder übermäßigen Zugriff auf Strafregistrierungen zu vermeiden, wird teilweise in den Gesetzen aller oder einiger Staaten vorausgesetzt, eine Übermittlung von Daten im Strafregister an bestimmte im Gesetz vorgeschriebene Zwecke zu binden – eine Weitergabe von Daten an eine andere als die anfragende Behörde ist zwar möglich, aber nur innerhalb des angefragten Zwecks. Im Falle der Übermittlung von *nonconviction data* oder der Übermittlung von Strafregistrierungen an eine andere Behörde als Strafverfolgungsbehörden sind bestimmte Schranken erforderlich. Außerdem müssen bei Datenanfragen Protokolle angefertigt werden oder es muss für eine entsprechende Ausbildung des Personals gesorgt werden, das am Strafregistersystem beteiligt ist. Die Übermittlung der Strafregistrierungen an eine Behörde setzt

---

ber überprüfen kriminelle Hintergrunddaten aus offiziellen Quellen (Vgl. *Pager*, The Mark of a Criminal Record, S. 953).

618 Siehe *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 6.

619 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 186 f. m. w. N.

620 42 U. S. C. § 14616 IV (c).

aber keine Möglichkeit der Betroffenen voraus, auf Verlangen Einsicht zu nehmen. Die Behörde ist auch nicht dazu verpflichtet, die Betroffenen darüber zu benachrichtigen. Bei der Verwendung des Strafregisters zur Strafrechtspflege scheint der Aspekt des Privacy-Schutzes, also des Datenschutzes, nicht genügend berücksichtigt zu werden. Die Verwendung ist ausschließlich mit gesetzlich vorgesehenen bestimmten Zwecken verbunden.

Die Politik konzentriert sich viel mehr auf die Versorgung mit genauen Daten als auf den Datenschutz. Dafür wurden einige gesetzliche Sicherungsvorkehrungen getroffen, damit sichergestellt wird, dass die staatlichen *criminal history records* vollständig, genau, für berechtigte Nutzer leicht zugänglich und vertrauensvoll sind. Zu diesen Vorkehrungen zählen u. a. die Mitteilungspflicht innerhalb von 90 Tagen nach den Verfügungen sowie der Prozess der systematischen Prüfung im Rahmen der Datenerhebung der -eintragung und der -speicherung.

d) Speicherdauer

Die bundesgesetzliche Regelung über die Speicherdauer von Daten im Strafregister existiert nur in Form von Ausnahmen. Die Datenspeicherung auf staatlicher Ebene ist jedem einzelnen Bundesstaat anvertraut. Die Strafregistrierungen werden in den meisten Fällen auf unbegrenzte Zeit bestehen.[621] Die Speicherdauer der Daten im Strafregister wird zwar einzelstaatlich auch nicht normiert, jeder einzelne Bundesstaat stellt jedoch die Begünstigungsmaßnahme der Tilgung[622] der Daten unter bestimmten Umständen[623] zur Verfügung. Die Voraussetzung zur Tilgung ist je nach Staat unterschiedlich. In einigen Staaten können nur die Verhaftungsdaten ohne Verurteilungen getilgt werden, in anderen auch die Verurteilungsdaten. Ob ein ehemaliger Straftäter die Tilgung seiner Strafregistrierung genießen kann, hängt davon ab, wo er angeklagt wurde. Aber es gibt Gemeinsamkeiten: Ein erstmaliges Vergehen insbesondere von einem Minderjährigen wird meist nach einer gewissen Zeit getilgt. In den meisten

621 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 393.

622 Hierbei wird unter *Tilgung* die Rechtsfolge verstanden, nach der die behördlichen Daten der Öffentlichkeit nicht zugänglich gemacht werden. Zu Einzelheiten siehe auch oben Fn. 469.

623 Zum Beispiel innerhalb eines bestimmten Zeitraums, in der Regel mehr als ein Jahr (Vgl. *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 393 m. w. N.).

Einzelstaaten ist es unmöglich, die Strafregistrierungen wegen sexueller Verbrechen zu löschen. Den Verhaftungsdaten ohne Verurteilungen ist in 36 Einzelstaaten die Möglichkeit der Tilgung gegeben.

Auch wenn eine Löschung landesgesetzlich vorgesehen ist, erfolgt sie nicht automatisch. In der Regel muss sich die die Löschung ersuchende Person bei einer zuständigen Behörde bewerben und von sich aus Unterlagen dafür vorlegen. Im US-amerikanischen System, in dem Strafregistrierungen nicht nur in den staatlichen Strafregistern, sondern auch in den Datenbanken aller Gerichte und kommerzieller Informationsanbieter zur Verfügung gestellt werden, kann die Löschung von Daten nur im Strafregister ihre praktische Bedeutung verlieren und damit das einheitliche Datenmanagement unmöglich machen. Entsprechendes gilt für das Versiegeln von Daten im Strafregister. Darüber hinaus besteht hier sogar ein Risiko, die versiegelten Daten absichtlich oder versehentlich offenzulegen. Ein weiteres Problem liegt zudem in der Wirksamkeit der Versiegelung von Daten unter modernen automatisierten Bedingungen. Der Versiegelung oder Löschung kann kaum Bedeutung zukommen, wenn bestimmte Daten für eine bestimmte Zeit auf einer Webseite veröffentlicht werden können. Diese Probleme sind deshalb ernst, weil ein Verwertungsverbot nach einer Löschung oder Sperrung gesetzlich nicht vorgesehen ist.

3. Vergleich

a) Organisationsstruktur

Die Strafregistersysteme in Deutschland und den USA zeigen vor allem einen konstruktiven Unterschied. In Deutschland wird das BZR abgesehen vom ZStV als ein einheitliches Strafregister geführt, das umfassende und schnell verfügbare Informationen über einen Beschuldigten in einem Ermittlungsverfahren bis vor deren Eintragung ins BZR zur Verfügung stellt.[624] Demgegenüber wird in den USA ein zentrales Strafregister mit Verweis auf dessen mangelnde Effektivität absichtlich vermieden[625] und stattdessen auf ein dezentrales Strafregistersystem gesetzt, in dem die

624 BT-Drs. 12/6853, S. 3; *Gieg*, KK-StPO, § 494 Rn. 4.

625 *Jacobs/Blitsa*, Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125 (2008) /Loyola of Los Angeles International and Comparative Law Review, Vol. 30, Issue 2 (Spring 2008), pp. 125–210 (130 f.).

jeweils von allen Bundesstaaten und dem FBI gesondert geführten Strafregister unter dem III-System (*Interstate Identification Index*) miteinander verbunden werden. In solchen dezentralen Strafregister werden alle strafrechtlich relevanten Daten, also nicht nur die Verurteilungsdaten, sondern auch die bloßen Verhaftungsdaten ohne Verurteilungen, gespeichert.

Unter der deutschen Strafprozessordnung flankieren einige gesetzliche Regelungen im Rahmen der Erhebung, der Speicherung, der Übermittlung und der Weitergabe von Daten das Strafregistersystem (BZR und ZStV), wodurch einem unbefugten oder übermäßigen Zugriff auf diese Daten vorgebeugt werden soll. Bei der Erhebung werden die mitteilungspflichtigen Stellen begrenzt und namentlich im Gesetz aufgeführt und die in das Register einzutragenden Inhalte, Erhebungs-, Anfrage- und Übermittlungsmethode und obligatorische Mitteilungsfristen sind ebenfalls konkret vorgesehen. Zur Speicherung im Strafregister müssen die Daten einige Prüfungen bestehen. Das Verfahren und die Methode der Übermittlung (die Auskunft auf Ersuchen) sind im Einzelnen beschrieben. Danach teilt eine mitteilungspflichtige Stelle der Registerbehörde die einzutragenden Inhalte innerhalb einer für die Daten bestimmten Mitteilungsfrist mittels Fernübertragung mit. Die Daten werden nach einigen Prüfungen für eventuelle Anfragen gespeichert. Eine berechtigte Stelle stellt nach festgelegten Verfahren eine Anfrage zu den in Gesetzen ermächtigten Zwecken. Die Registerbehörde prüft die Berechtigung der Stelle und des angegebenen Zweckes und erteilt dann der Stelle auf Anfrage eine Auskunft mittels Datenübertragung oder eines automatisierten Verfahrens (Abruf). Die Weitergabe der von der Registerbehörde erhaltenen Daten ist grundsätzlich verboten, aber ausnahmsweise zulässig, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde. Die übermittelten Daten sind nach ihrer Verwendung unverzüglich zu löschen. Die Daten im Strafregister werden nicht dauerhaft gespeichert, sondern nach vorher festgelegten Fristen vollends gelöscht.

Das US-amerikanische Strafregistersystem geht einen völlig anderen Weg. Die Bundesgesetze, auf denen das III-System basiert, regeln nur den Austausch von Daten unter dem III-System und die Erhebungs- und Speicherregelung im staatlichen Strafregistersystem ist jedem einzelnen Bundesstaat überlassen. Die Erhebung, Speicherung, Übermittlung und Weitergabe von Daten auf staatlicher Ebene werden also je nach Bundesstaat unterschiedlich geregelt. Das III-System verbindet einen ersuchenden Staat nur mit dem Staat, der die ersuchten Daten in seinem Strafregister

erhält, aber beeinflusst nicht die Führung des staatlichen Strafregisters. Jeder Staat besitzt damit verschiedene Regelungen über die mitteilungspflichtigen Stellen, die Mitteilungsmethoden sowie -fristen und die einzutragenden Daten. Die Mitteilung der Strafregistrierungen an das III-System variiert außerdem in Abhängigkeit davon, ob die einzelnen Bundesstaaten am NFF teilnehmen oder nicht. Abgesehen von den unterschiedlichen Regelungen über das Strafregistersystem unter allen Staaten teilen die am NFF teilnehmenden Staaten dem FBI alle ersten Registrierungsdaten mit, die nicht daran teilnehmenden Staaten hingegen alle Strafregistrierungen. Mit diesen Daten gewinnen das NFF und der Index Aktualität. Die ersuchende Stelle stellt ihre Anfrage über ihr staatliches Strafregister an das FBI. Der III-Computer verweist das staatliche Strafregister an das FBI und/oder an ein oder mehrere der staatlichen Strafregister, die die angefragten Daten erhalten. Die angegebenen Quellen schicken die Antwort, die dann vom staatlichen Strafregister zur anfragenden Behörde weitergeleitet wird. Drei Arten von Computernetzwerken stehen in diesem Prozess für eine Anfrage und Antwort zur Verfügung. Die Übermittlung von *conviction data*, die Weitergabe oder die Vernichtung der übermittelten Daten und die Löschung von in staatlichen Strafregistern gespeicherten Daten werden bundesgesetzlich nicht geregelt.

b) Inhalt des Registers

Ein Unterschied beim Strafregistersystem in den beiden Ländern liegt im Inhalt des Registers. Während in Deutschland die Verurteilungsdaten und die Strafverfahrensdaten nach unterschiedlichen Regeln separat gespeichert und verarbeitet werden, werden in den USA die beiden Datenarten zusammen in Strafregister eingetragen und gespeichert. Die Strafverfahrensdaten im ZStV werden also entweder ins BZR eingetragen und dann gelöscht oder bei Nichteintragung nach einer gewissen Zeit vollständig gelöscht. Demgegenüber bleiben neben den Verurteilungsdaten die bloßen Verhaftungsdaten im Strafregister gespeichert, was für den Betroffenen dauerhaft nachteilig sein kann.[626]

626 Eine nachteilige Verfügung kann auch nur aus der Verhaftung vor einer Verurteilung begründet werden. Zu einer näheren Betrachtung der Nachteile siehe oben Teil 3 B. I. 4. und Department of Housing and Urban Development v. Rucker, 535 U. S. 125.

Während in Deutschland die sowohl im BZR als auch im ZStV einzutragenden Daten bundesgesetzlich geregelt werden, gibt es in den USA nichts Entsprechendes. Das BZRG und § 492 Abs. 2 StPO als die Rechtsgrundlage des ZStV sehen die ausführlichen Kataloge vor. Unter dem deutschen Strafregistersystem werden neben strafgerichtlichen Verurteilungen noch weitere Daten gespeichert; daher wurde das System in *Bundeszentralregister* umbenannt. Unter dem US-amerikanischen III-System, das dem Austausch von Strafregistrierungsdaten zwischen dem Bund und den Einzelstaaten dient, ist nur vorgesehen, dass die Mitteilung der Strafregistrierungen unbeschadet der unterschiedlichen Praxis des Strafregisters in jedem Staat nur für schwere und/oder erhebliche Erwachsenen- und Jugendstraftaten erfolgen darf.

c) Verwendung der Daten aus dem Register

Beim Datenschutz ist der Schutz vor der unbefugten oder übermäßigen Verwendung und Weitergabe personenbezogener Daten genauso bedeutsam wie der Schutz vor der unbegrenzten Erhebung und Speicherung personenbezogener Daten. Dieser Schutz setzt voraus, dass die Möglichkeit zur Korrektur von Fehlinformationen durch die Falschverarbeitung dem Einzelnen offenstehen muss und dass die Betroffenen nachvollziehen können, welche ihrer Daten von wem in welchem Verwendungszusammenhang weiterverarbeitet werden. Dafür sind die präzise Normklarheit, die Zweckbestimmung und -bindung sowie die Mitteilung an die Betroffenen erforderlich. Hierbei soll das Strafregistersystem in den beiden Ländern unter Maßgabe des Kriteriums betrachtet werden, welche Sicherheitsmaßnahmen verfügbar sind, um den Einzelnen gegen die mögliche missbräuchliche Verwendung seiner personenbezogenen Daten zu schützen. Denn beim Strafregistersystem kommt der Abwägung der unterschiedlichen Interessen eine wichtige Bedeutung zu: zum einen das Interesse der Verurteilten an einer Resozialisierung, insbesondere an der Erlangung einer neuen Arbeitsstelle und zum anderen das Interesse Dritter, insbesondere der Arbeitgeber an der Kenntnis belastender, für eine Einstellung maßgebender Gesichtspunkte und das öffentliche Interesses an einer brauchbaren Grundlage für Verwaltungsentscheidungen.[627]

Von Eintragungen im deutschen BZR darf grundsätzlich nur der Betroffene und unter bestimmten Voraussetzungen auch bestimmte Behörden

627 *Tolzmann*, Bundeszentralregistergesetz, § 30 Rn. 7.

Kenntnis nehmen. Die Auskunftsmöglichkeiten haben je nach Empfängerkreis unterschiedliche Inhalte. Die Staatsanwaltschaft und das Strafgericht erhalten in bestimmten Fällen eine weitergehende Auskunft als die übrigen Auskunftsberechtigten.[628] In das Führungszeugnis für private Zwecke wird hingegen nur ein begrenzter Ausschnitt der tatsächlich möglichen Eintragungen – nur die strafrechtlichen Verurteilungen (§ 4 BZRG) mit Ausnahmen von §§ 32 bis 34, 39 BZRG – aufgenommen. Dies ist das Ergebnis einer sorgfältigen Abwägung widersprüchlicher Interessen. Das zielt darauf ab, dass die Wiedereingliederung der Bestraften in Beruf und Gesellschaft dadurch erleichtert wird, dass bestimmte Bestrafungen überhaupt nicht, andere nach Ablauf bestimmter Fristen nicht mehr in das Privatführungszeugnis aufgenommen werden. Damit die Möglichkeit der Aushändigung des Zeugnisses an Unbefugte ausgeschlossen wird, darf das Führungszeugnis grundsätzlich nur an die Antragstellenden geschickt werden, und die Meldebehörde ist dazu verpflichtet, die Identität der Antragstellenden und die Angaben zum Wohnsitz zu überprüfen. Aus dem gleichen Grund ist die Übersendung der zur Vorlage bei einer Behörde bestimmten Zeugnisse, also der Behördenführungszeugnisse, an die Antragstellenden gesetzlich verboten. Denn in diese Zeugnisse werden auch Eintragungen aufgenommen, die im Privatführungszeugnis nicht erscheinen. Dadurch wird die missbräuchliche Verwendung personenbezogener Daten verhindert: Schutzvorschriften könnten ansonsten z. B. dadurch umgangen werden, dass die Arbeitgeber die Betroffenen dazu veranlassen, ein angeblich zur Vorlage bei einer Behörde bestimmtes Zeugnis zu beantragen und dann ihnen zu zeigen.[629] Außer wenn die Auskunft unmittelbar dem Betroffenen oder ggf. seinem gesetzlichen Vertreter erteilt wird, ist der Auskunftsantrag gesetzlich an bestimmte Voraussetzungen gebunden, damit die Betroffenen gegen die missbräuchliche Verwendung ihrer personenbezogenen Daten effektiv geschützt werden können. Dazu gehört das Verbot der Übersendung des Behördenführungszeugnisses an die Antragstellenden. Darüber hinaus wird vorausgesetzt, dass das Führungszeugnis zur Erledigung der hoheitlichen Aufgaben der Behörden benötigt wird und eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß oder erfolglos bleibt. Die Weitergabe des Behördenführungszeugnisses an eine andere Behörde ist nur unter der Einwilligung der Betroffenen möglich.

628 Für eine Übersicht über den inhaltlichen Unterschied je nach Empfängerkreis siehe *Tolzmann*, Bundeszentralregistergesetz, § 3 Rn. 18.

629 *Tolzmann*, Bundeszentralregistergesetz, § 30 Rn. 33.

Bei unbeschränkter Auskunft nach § 41 BZRG, mit der der gesamte Inhalt des Registers lediglich einer eng begrenzten Zahl von Behörden im überwiegend öffentlichen Interesse an dem Schutz vor der Begehung weiterer Straftaten zur Kenntnis gebracht wird, sind zur Gewährleistung des Schutzes dieser hochsensiblen Daten und zur Verhinderung ihrer missbräuchlichen Verwendung Schranken eingebaut worden: die abschließende Aufzählung der auskunftsberechtigten Stellen, die Begrenzung auf Einzelfallanfragen und die Beschränkung der Auskunftserteilung auf bestimmte Zwecke. Die unbeschränkt auskunftsberechtigte Stelle muss also den Zweck der Anfrage angeben und die Registerbehörde muss prüfen, ob der angegebene Zweck ein Recht auf unbeschränkte Auskunft gibt. Die Auskunft darf nur für diesen Zweck verwertet werden. Damit wird die Weitergabe unbeschränkter Auskünfte grundsätzlich mit der Ausnahme der Weiterleitungsmöglichkeit nach § 43 BZRG verboten. Die Ausnahme dient aber dazu, den Umfang der Verwendung der Daten, die die obersten Bundes- und Landesbehörden gem. § 41 Abs. 1 BZRG ohne konkrete Zweckbeschränkung erhalten, einzugrenzen. Die Weitergabe darf nur an die der obersten Behörde unterstellten Behörden erfolgen, wenn dies zur Vermeidung von Nachteilen für Bund oder Land unerlässlich ist, weil die Erfüllung öffentlicher Aufgaben andernfalls erheblich gefährdet oder erschwert würde.

Für die Strafverfahrensdaten von Beschuldigten und Tatbeteiligten sind nur die Strafverfolgungsbehörden auskunftsberechtigt. Sie dürfen diese Daten – mit einigen Ausnahmen – aber ausschließlich für Strafverfahren speichern, verändern und verwenden. Die Strafverfahrensdaten ohne Verurteilung werden im BZR gespeichert und zugleich aus dem ZStV gelöscht. Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, werden die Strafverfahrensdaten hingegen nach Ablauf einer bestimmten Zeit aus dem ZStV gelöscht und damit von niemandem verwendet. Da die Verwendung der Strafverfahrensdaten an den Verwendungszweck gebunden ist, dürfen die Daten nur zu dem Zweck verwendet werden, für den sie übermittelt wurden. Eine Verwendung für andere Zwecke wird nur insoweit erlaubt, als die Daten dafür hätten übermittelt werden dürfen.

Da die Verwendung personenbezogener Daten sowohl aus dem BZR als auch aus dem ZStV nicht mit der Verpflichtung verbunden ist, die Betroffenen darüber zu unterrichten, werden diese Daten normalerweise ohne das Wissen der Betroffenen verwendet, außer wenn die Betroffenen ein Führungszeugnis zur Vorlage bei einer Behörde beantragen. Statt der Un-

terrichtungspflicht sind jedoch die Verwendungsberechtigten, der Verwendungszweck und die Weitergabe schon übermittelter Daten gesetzlich eng eingeschränkt, um den Einzelnen gegen eine unbefugte oder unbegrenzte Verwendung personenbezogener Daten zu schützen. Die Betroffenen sind außerdem dazu berechtigt, die Eintragungen im BZR und im ZStV einzusehen. Das Einsichtsrecht dient dazu, die Wahrscheinlichkeit falscher Informationen zu verringern. Auf das Einsichtsrecht sind die Antragstellenden von der Meldebehörde hinzuweisen. Darüber hinaus werden die erforderlichen und angemessenen Maßnahmen gesetzlich gefordert, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen.

Rechtliche Vorkehrungen zum Schutz eines Einzelnen vor unbefugter oder unbegrenzter Verwendung von Eintragungen aus dem Strafregister sollen in den USA jeweils getrennt auf bundesstaatlicher Ebene und auf einzelstaatlicher Ebene berücksichtigt werden. Die bundesgesetzlichen Einschränkungen der Datenverwendung unter dem III-System und FIRS, das dem zwischenstaatlichen Datenaustausch dient, sind in 28 C. F. R. § 20.33 geregelt. Hierbei sind die Auskunftsberechtigten in Verbindung mit bestimmten Verwendungszwecken genannt. Ebenso wie in Deutschland sind in den USA die Verwendungsberechtigten und der Verwendungszweck von Strafregistrierungen auf bundesstaatlicher Ebene eingeschränkt. Die Strafgerichte und Strafverfolgungsbehörden dürfen z. B. auf die Strafregistrierungen, die im III-System und FIRS enthalten sind, für Zwecke der Strafrechtspflege oder der Durchführung von Hintergrundkontrollen im Rahmen des *national instant criminal background check system* (NICS) zugreifen. Die Strafregistrierungen dürfen an gesetzlich berechtigte Bundesbehörden oder zur Verwendung im Zusammenhang mit der Lizenzierung oder Beschäftigung übermittelt werden. Die Verwendung der auf diese Weise übermittelten Daten beschränkt sich zweckgebunden auf die genannten Behörden und damit ist die Weitergabe der Daten an eine andere Behörde grundsätzlich verboten (28 C. F. R. § 20.33 (b)). Außerdem können die Betroffenen ihre Daten vom FBI erhalten, um die Gefahr von Fehlinformation zu reduzieren. Der *Code of Federal Regulations* fordert, dass geeignete Maßnahmen getroffen werden, um die Vollständigkeit, Genauigkeit und Sicherheit von Strafregistrierungen zu gewährleisten.

Die Verwendung von Eintragungen auf einzelstaatlicher Ebene regelt zuerst bundesgesetzlich 28 C. F. R. § 20.21 (b) und (c). Die Vorschrift beschränkt nur die Verwendung von *nonconviction data*. Diese Daten

dürfen nur an Strafgerichte und Strafverfolgungsbehörden für Zwecke der Strafrechtspflege und an Einzelpersonen und Behörden für jeden Zweck, der durch Gesetze, Verordnungen, Verfügungen oder Gerichtsurteile, -entscheidungen oder -ordnungen genehmigt wurde, aufgrund einer spezifischen Vereinbarung mit einer Strafverfolgungsbehörde oder für den ausdrücklichen Zweck der Forschung, Evaluation oder Statistik im Rahmen einer Vereinbarung mit einer Strafverfolgungsbehörde übermittelt werden. Diese Regelung bestimmt außerdem, dass die Verwendung von Strafregistrierungen, die an eine andere als die justizielle Behörde übermittelt wurden, auf den Zweck beschränkt ist, für den sie erteilt wurden (Zweckbindung), und dass die Übermittlung von Daten über Verfahren in Bezug auf die Entscheidung eines Jugendlichen an eine andere als die justizielle Behörde verboten ist. Auf Grundlage dieses Bundesgesetzes regelt jeder Einzelstaat auf staatlicher Ebene abhängig von der Datenart – *conviction data*, *nonconviction data* und *arrest data* – unterschiedliche Einschränkungen.[630] Maryland kennt Ermächtigungsgrundlagen, auf denen jede Art von Daten jeweils an die justiziellen Behörden, die anderen Behörden oder zum privaten Sektor übermittelt werden darf. Dazu gehören Normen, die eine Hintergrundprüfung in bestimmten Bereichen erlauben oder sogar beauftragen. Während in Maryland kein Übermittlungsverbot dieser drei Datenarten vorgesehen ist, verbietet Kalifornien eine Datenübermittlung in bestimmten Bereichen.[631]

Werden die Gesetzgebungen über die Verwendung von Strafregistrierungen zusammengefasst, lässt sich Folgendes feststellen: Die Verwendung von *conviction data* ist im Bundesgesetz grundsätzlich unbeschränkt und jeder Staat verfügt demnach über Ermächtigungsnormen, die es ermöglichen, Daten an die strafjustiziellen sowie die anderen Behörden oder den privaten Sektor zu übermitteln. Die Übermittlung von *nonconviction data* an eine Strafjustizbehörde, die anderen Behörden oder den privaten Sektor ist bundesgesetzlich nur zu Strafverfolgungszwecken, zu gesetzlich berechtigten Zwecken oder aufgrund einer besonderen Vereinbarung mit einer Justizbehörde zulässig. In diesem Fall ist die Verwendung an einen genannten Zweck gebunden. Jeder Einzelstaat ermöglicht die Verwendung von *nonconviction data* und sogar *arrest data* mit entsprechenden Ermächtigungsgrundlagen. Dies führt schließlich zu der folgenden Bewertung:

630 Zu Einzelheiten der rechtlichen Grundlagen der einzelstaatlichen Datenübermittlung siehe *U. S. Department of Justice*, Compendium of State Privacy and Security Legislation: 2002 Overview, Bureau of Justice Statistics, 2003.

631 Labor Code 432.7.

Jede Art von Daten darf ohne Einschränkung verwendet werden, solange es eine entsprechende Ermächtigungsnorm gibt. Denn es gibt sowohl bundesgesetzlich als auch einzelstaatlich so gut wie keine Beschränkung der Verwendung von *conviction data*, *nonconviction data* oder *arrest data*. Außer der Einschränkung von Strafregistrierungen, die im Rahmen des III-Systems übermittelt werden dürfen, gibt es also keine besonderen Beschränkungen für die Verwendung von Strafregistrierung, um einen Einzelnen vor einer unbegrenzten Verwendung zu schützen.

Die bundes- und einzelstaatsgesetzlich erlaubten oder sogar beauftragten kriminalpolizeilichen Überprüfungen in bestimmten Bereichen, Megans Gesetze und die Zunahme der privaten Informationsdienstunternehmen führen dazu, dass jeder nur mit Namensangabe gegen eine Gebühr die *conviction data* oder sogar die *arrest data* von jemandem erhalten kann – obwohl die gesetzlichen Grundlagen in jedem Staat unterschiedlich sind.[632] Dafür gibt es nur eine Einschränkung, nämlich, dass die Daten nicht für den Zweck einer Beschäftigungsentscheidung verwendet werden dürfen.[633] Dies macht die Strafregistrierungen einer anderen Person zu niedrigen Kosten für jedermann leicht zugänglich. Eine Weitergabe der Daten an eine andere Behörde, die unter dem III-System, aufgrund einer Hintergrundprüfung oder von privaten Informationsdienstunternehmen erhalten wurden, ist weder verboten noch eingeschränkt.

Wie oben bereits erwähnt, wurden in Deutschland verschiedene Maßnahmen ergriffen, um eine unbefugte oder unbegrenzte Verwendung personenbezogener Daten in Bezug auf die Vorbestrafungen zu verhindern. Die Auskunftsberechtigten, die Verwendungszwecke, die aufzunehmenden Eintragungen nach Auskunftsweise und Weitergabe schon übermittelter Auskünfte sind unter der Abwägung des Interesses der Allgemeinheit an der Abwehr besonderer Gefahren und des Interesses des Betroffenen an einer möglichst reibungslosen Wiedereingliederung gesetzlich konkret geregelt. Obwohl die Strafregistrierungen in der Politik tendenziell allgemein zugänglicher werden, scheinen in den USA fast keine Einschränkungen zur Vermeidung einer unbegrenzten oder übermäßigen Nutzung von Strafregistrierungen vorgesehen zu sein, unabhängig davon, ob sie zu den

632 Private Informationsdienstunternehmen warnen Arbeitgeber, Vermieter, Hotels und andere Unternehmen davor, dass die unterlassenen Hintergrundprüfungen zu erheblicher Haftung wegen unerlaubter Handlungen führen könnten (*Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 178).

633 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 187 m. w. N.

conviction data oder *nonconviction data* gehören.[634] Die Politik scheint sich hier viel mehr auf die Versorgung mit genauen Daten als auf den Datenschutz zu konzentrieren. Denn ebenso wie Deutschland fordern die USA dazu auf, technische Maßnahmen zu treffen, um die Vollständigkeit, die Genauigkeit und die Sicherheit der Daten sicherzustellen. Gemeinsam ist die Gewährleistung des Einsichtsrechts der Betroffenen, um Fehlinformationen zu korrigieren. Anders als in Deutschland, wo die Verwendung des Inhalts des Registers von der verhängten Strafe abhängt, richtet sich die Verwendung von Strafregistrierungen in den USA nach einer begangenen oder verdächtigten Straftat; dies spiegelt die Sensibilität der Gesellschaft für bestimmte Verbrechen wider. Im Falle etwa von Sexualdelikten oder Straftaten im Zusammenhang mit häuslicher Gewalt werden nicht nur die *conviction data*, sondern auch die *arrest data* in den besonderen Registern gespeichert und zur Verfügung gestellt. Insbesondere für Sexualstraftäter stehen aufgrund der Verbreitung der Megans Gesetze und des *Adam Walsh*-Gesetzes erhebliche personenbezogene Daten aus dem Strafregister kostenlos online zur Verfügung.

d) Speicherdauer

Während das deutsche Strafregistersystem bundesgesetzlich einheitliche Vorschriften über die Speicherdauer von Daten sowohl im BZR und als auch im ZStV kennt, ist die Verarbeitung der Eintragungen in den einzelstaatlichen Strafregistern in den USA jedem Staat überlassen. Dies beruht auf dem Unterschied zwischen den politischen Strukturen der beiden Länder, obwohl beide Bundesstaaten sind. Bezüglich der Speicherdauer von Strafregistrierungen ist auf bundesstaatlicher Ebene – abgesehen von einigen Ausnahmen – keine einheitliche Vorschrift vorgesehen. Die meisten Einzelstaaten stellen in den USA zwar eine Form der Löschung von Strafregistrierungen oder ähnlichen Begünstigungen zur Verfügung. Aber die Voraussetzungen, die Mechanismen und die Objektverbrechen zur Tilgung unterscheiden sich voneinander. Ebenso wie bei der Speicherung strafrechtlich relevanter Daten erfolgt die Tilgung bestimmter Strafregistrierungen in einigen Staaten häufig, aber in anderen nicht. Ob die Strafregistrierung getilgt werden kann, hängt vom Anklage- und Ver-

634 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 419.

handlungsort ab.[635] Aber die Verurteilungsdaten werden normalerweise nicht getilgt, auch wenn sie in wenigen Staaten unter bestimmten Voraussetzungen gelöscht werden können. Dies gilt insbesondere im Falle von Verurteilungsdaten wegen sexueller Verbrechen. Daraus ergibt sich, dass das öffentliche Interesse daran, die Strafregistrierungen für zukünftige Verbrechensermittlungen beizubehalten, dem individuellen Interesse des Betroffenen an seinen Verurteilungsdaten überlegen ist. Außerdem werden die Strafregistrierungen in einigen Staaten dann automatisch getilgt, wenn bestimmte Voraussetzungen erfüllt sind, aber in anderen muss eine auf eine Tilgung ersuchende Person die tatsächliche Unschuld beweisen.[636] Das entscheidende Element bei der Tilgung ist nicht die Höhe der Hauptstrafe, sondern die Art des Verbrechens. Ein Beispiel bildet das sexuelle Verbrechen. Die Strafregistrierungen wegen sexueller Verbrechen werden aufgrund ihres höheren Rückfallrisikos schwer oder gar nicht getilgt.[637]

In Deutschland sind hingegen die Möglichkeiten der grundsätzlichen fristabhängigen Tilgung einerseits und der fristunabhängigen außergewöhnlichen Tilgung andererseits sowie der Sperrung als Ausnahmefall gesetzlich einheitlich vorgeschrieben. Eintragungen, die nach dem BZRG gespeichert werden, werden nach Ablauf einer bestimmten Frist grundsätzlich aus dem Register entfernt. Dabei richtet sich die Speicherdauer nach dem verhängten Strafmaß. Die Fristen werden bereits bei der Einordnung von Entscheidungen in das Register von einem Fristenprogramm berechnet und die zu tilgenden Daten werden bei der täglichen Überprüfung der Tilgungsfristen von einem besonderen Löschprogramm automatisch gelöscht.[638] Der Ablauf der Tilgungsfrist einer Verurteilung kann durch die in § 47 BZRG vorgesehene Voraussetzung gehemmt werden. Außerdem sind die fristunabhängige Entfernung von Entscheidungen aus dem Register gemäß §§ 16 Abs. 2, 24 und 63 BZRG und die vorzeitige Tilgung aufgrund einer Anordnung der Registerbehörde auf Antrag oder von Amts wegen möglich.

---

635 *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 8.

636 *Diehm*, Federal Expungement: A Concept in Need of a Definition, Federal Expungement: A Concept in Need of a Definition, St. John's Law Review, Vol 66. No. 1, 1992, 73, 74.

637 *McAdoo*, Creating an Expungement Statute for the District of Columbia: a Report and Proposed Legislation, S. 8.

638 *Rebmann*, Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513, 1516 f.

Der Tilgung kommt in Deutschland über die Bedeutung eines bloßen fristbezogenen Datenschutzes hinaus vor allem eine praktische Bedeutung zu. Eine Eintragung darf nach der Tilgung in den anderen späteren Strafverfahren nicht weiter verwertet werden (Verwertungsverbot). Hierbei steht dem Betroffenen das Schweigerecht zu. Demgegenüber ist die Begünstigungsmaßnahme der Tilgung in den USA nicht mit dem Verwertungsverbot verbunden. Denn das Wesen der Tilgung liegt nicht darin, die Daten tatsächlich zu löschen, sondern darin, die Daten für die Öffentlichkeit unzugänglich zu machen, und ein Mindestmaß an Daten wird damit typischerweise zur Aufbewahrung und zur weiteren Verwertung durch das Strafjustizsystem gesichert.

Abgesehen davon, dass es in den USA keine bundesgesetzliche Speicherdauervorschrift gibt und dass das Tilgungsregime je nach Einzelstaat unterschiedlich ist, liegt ein bedeutsamer Unterschied in der Behandlung der bloßen Strafverfahrensdaten. Wie oben bereits erwähnt, werden in den USA im Gegensatz zu Deutschland die Verhaftungsdaten ohne Verurteilungen auch im Strafregister gespeichert und können damit nachteilige Folgen für den Betroffenen haben. In einigen Staaten ist es sogar unmöglich, die Verhaftungsdaten zu tilgen, obwohl die Tatsache, dass eine Person schon einmal verhaftet, aber nicht verurteilt wurde, an nachteilige Verfügungen in vielen Bereichen geknüpft werden kann. Dementsprechend sind selbst zu Unrecht beschuldigte Personen von den Vorwürfen und dem damit verbundenen Stigma betroffen.

Die Verwendung der Eintragungen im deutschen ZStV wird hingegen durch zwei Möglichkeiten eingeschränkt: zum einen durch die Löschung, zum anderen durch die Sperrung. Die Speicherung im ZStV endet notwendigerweise, sobald die im ZStV gespeicherten Daten in das BZR eingetragen werden. Die Löschung beim ZStV erfolgt automatisch ebenso wie beim BZR, wenn die Löschungsvoraussetzung erfüllt wird. Die schon im ZStV gespeicherten, aber aufgrund des rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und nicht nur vorläufiger sowie endgültiger Verfahrenseinstellung in das BZR nicht einzutragenden Daten werden erst zwei Jahre nach Verfahrenserledigung aus dem ZStV entfernt. Ein möglicher Nachteil aufgrund bloßer Strafverfahrensdaten wird damit abgesichert. Die schon entfernten Strafverfahrensdaten existieren entsprechend der Bedeutung des Wortes „Entfernung“ nicht mehr und können deshalb nicht weiter verwertet werden. Außerdem sind alle übermittelten Daten im Rahmen des ZStV nach ihrer Verwendung unverzüglich zu löschen. Neben der endgültigen Entfernung können die im ZStV gespeicherten Daten unter bestimmten Voraussetzun-

gen gesperrt werden. Die Verwendung der gesperrten Daten ist unter den im Gesetz vorgesehenen engen Ausnahmen verboten.

II. Rasterfahndung

1. Deutschland

a) Organisationsstruktur

Da im deutschen Datenschutzsystem jede Datenverarbeitung grundsätzlich verboten ist, ermächtigt die StPO mit § 98 a bis c die Strafverfolgungsbehörden dazu, die Daten automatisiert abzugleichen. Die Befugnis erstreckt sich dabei darauf, sowohl polizeiinterne als auch -externe Dateien, also Dateien, die bei einer öffentlichen Behörde oder einer privaten Stelle gespeichert sind, miteinander abzugleichen. Eine Rasterfahndung im eigentlichen Sinne (§ 98a StPO) beschränkt sich auf einen maschinell-automatisierten Datenabgleich zwischen bestimmten, auf den Täter vermutlich zutreffenden Prüfungsmerkmalen mit aus anderen Gründen an anderen Stellen gespeicherten Daten. Von der Rasterfahndung unterscheidet sich damit der Abgleich mit polizeiinternen Daten (z. B. der Abgleich personenbezogener Daten, die die Strafverfolgungsbehörden durch die in der StPO geregelten Ermittlungsmaßnahmen gewonnen haben, oder der Abgleich solcher Daten mit präventiv-polizeilichen Fahndungsdateien) in § 98c StPO. Auf Grundlage dieser Befugnis dürfen die Strafverfolgungsbehörden die Übermittlung der abzugleichenden Dateien von der Speicherstelle anfordern und die Speicherstelle soll dann die Daten aussondern und übermitteln und dabei die Strafverfolgungsbehörden unterstützen.

§ 98a Abs. 1 S. 1 StPO unterscheidet zwischen dem Ausschluss Nichtverdächtiger (negative Rasterfahndung) und der Feststellung von Personen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen (positive Rasterfahndung). Die beiden Arten der Fahndung unterscheiden sich in der Eingriffsintensität. Bei der positiven Rasterfahndung werden sämtliche Daten, die bei verschiedenen Behörden und privaten Einrichtungen gespeichert sind, durchsucht. Nicht nur die Daten, die letztlich auf dem Ergebnisband abgespeichert werden, sondern auch sämtliche Daten bei Suchläufen erfahren hier eine Änderung von ihrem ursprünglichen Bezugsrahmen in den Kontext polizeilicher Fahndungszwecke oder der Verdachtsüberprüfung. Daraus ergibt sich die Gefahr, dass die Personendaten ohne Kontrolle des Betroffenen zu einem teilweisen oder weitgehend voll-

ständigen Persönlichkeitsbild zusammengefügt werden. Damit sind sämtliche Personen, deren Daten sich in den zu untersuchenden Datenbeständen befinden, potenziell von weiteren Fahndungsmaßnahmen bedroht. Dies fördert die Tendenz zu möglichst unauffällig-konformem Verhalten und ist damit geeignet, die Wahrnehmung der allgemeinen Freiheitsrechte durch an Straftaten völlig Unbeteiligte einzuschränken.[639] Bei der negativen Rasterfahndung werden die Abgleichdateien nur dazu genutzt, Daten aus dem Ausgangsdatenbestand zu löschen. Die Abgleichdateien werden von den Strafverfolgungsbehörden nicht eingesehen und die betroffenen Dateninhaber werden von vornherein von Fahndungsmaßnahmen ausgeschlossen und sind somit nicht davon bedroht. Es verbleibt jedoch eine Missbrauchsgefahr, die einen psychischen Druck auf die Dateninhaber auslösen kann, vor dem das Recht auf informationelle Selbstbestimmung sie schützen soll. Bei der negativen Rasterfahndung mit einer Fremddatei als Ausgangsdatei wird die Ausgangsdatei von ihrem ursprünglichen Kontext in den polizeilichen Fahndungskontext überführt, während bei der negativen Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist, die Ausgangsdatei keine Zweckänderung erfährt.

b) Vergleichbare Daten

Die Rasterfahndung unterliegt hinsichtlich der personenbezogenen Daten, die für einen Datenabgleich verwendet werden dürfen, keinen Beschränkungen. Hinsichtlich Art, Inhalt und Umfang der zu Rasterfahndungszwecken heranzuziehenden Daten sieht die StPO keine nähere Erläuterung vor. Die fehlende Eingrenzung personenbezogener Daten kann die Gefahr dafür erhöhen, dass ein Persönlichkeitsprofil zustande kommt. Angesichts dieser Gefahr wurde im Zuge von Gesetzesentwürfen zwar eine Eingrenzung vorgeschlagen, diese Vorschlag hatte jedoch keinen Erfolg.

c) Verwendung des Datenabgleichs

Der Abgleich polizeiexterner Dateien ist gesetzlich mit bestimmten Voraussetzungen verbunden: den zureichenden tatsächlichen Anhaltspunkten

639 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 52.

hinsichtlich einer Katalogtat, die von erheblicher Bedeutung sein muss, der Subsidiarität der Maßnahmen und dem Richtervorbehalt. Nach § 98a Abs. 1 Satz 1 StPO ist eine Rasterfahndung also nur insoweit zulässig, als zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Katalogtat begangen wurde und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die Übermittlung und der Abgleich polizeiexterner Daten dürfen nur auf der Grundlage einer gerichtlichen Anordnung oder bei Gefahr im Verzug auch aufgrund einer staatsanwaltschaftlichen Anordnung erfolgen.

d) Aufbewahrungsdauer der Daten

§ 98b Abs. 3 regelt die Rückgabe- oder die Löschungspflicht übermittelter Daten nach einem Datenabgleich. Danach sind die Daten auf Datenträgern nach Beendigung des Abgleichs unverzüglich zurückzugeben und personenbezogene Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden. Es gibt aber keine Löschungs- oder Vernichtungsvorschrift für Daten, die aufgrund der staatsanwaltschaftlichen Eilanordnung erlangt wurden, jedoch gerichtlich nicht bestätigt wurden und damit außer Kraft treten.

e) Mitteilungspflicht

Zu benachrichtigen sind nach § 101 StPO von allen Betroffenen nur diejenigen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden. Somit fallen alle übrigen Betroffenen, deren personenbezogene Daten ebenfalls in die Rasterfahndung einbezogen waren, aus der Benachrichtigungspflicht heraus.[640] Die Benachrichtigung kann gesetzlich unterbleiben oder zurückgestellt werden. Wie oben bereits erwähnt, werden Personen, die von den Informationsverarbeitungsvorgängen im Zuge einer Rasterfahndung betroffen sind, in ihrem Recht auf informationelle Selbstbestimmung unterschiedlich intensiv beeinträchtigt. Diejenigen, die

640 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 140.

nach mehreren Suchläufen als Merkmalsträger herausgerastert wurden, sind intensiver betroffen als diejenigen, deren Daten sich nur in Abgleichdateien befinden, damit Personendaten aus dem Ausgangsdatenbestand gelöscht werden können. Trotzdem nimmt die StPO keinen Unterschied zwischen den beiden Fällen wahr, sondern schließt die Benachrichtigungspflicht mit weiteren Ermittlungen an. Das bedeutet, dass die Benachrichtigungspflicht letztlich nicht durch die Rasterfahndung an sich ausgelöst wird, sondern erst durch die dadurch veranlasste Vornahme weiterer Ermittlungen gegen diese Personen. Lediglich die Rasterfahndung löst also keine Benachrichtigungspflicht aus.

Über die Benachrichtigung der Betroffenen hinaus ist nach Beendigung einer Rasterfahndung die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist (§ 98b Abs. 4 StPO).

2. USA

a) Organisationsstruktur

Das *Computer Matching* ist ein computergestützter Abgleich von Datensätzen, der vornehmlich eingesetzt wird, um Gesetzesverstöße im Zusammenhang mit dem Empfang staatlicher Leistungen zu ermitteln. Durch US-amerikanische Gesetze wird nur der staatliche Datenabgleich geregelt, der die behördenübergreifende Datenübermittlung voraussetzt. Denn jede Datenverarbeitung ist in den USA grundsätzlich zulässig, soweit es keine spezielle Bestimmung gibt. Dies wird vor allem durch den Privacy Act und den Computer Matching Act als dessen Änderungsgesetz geregelt. Den besonders hohen Gefahren staatlicher automatisierter Datenverarbeitung wurde aber durch eine Einschränkung der behördenübergreifenden Übermittlung bei öffentlichen Stellen gespeicherter Daten Rechnung getragen (Privacy Act § 552a). Das Gesetz sieht insoweit ein Verbot der behördenübergreifenden Offenlegung personenbezogener Daten ohne Zustimmung der Betroffenen vor. Außerdem sind im Gesetz explizitere Richtlinien enthalten, die die Austauschmethode der Daten zwischen Behörden und das Ausmaß bestimmen, in dem die Behörden aufgrund von abgeglichenen Daten handeln dürfen. Eine behördenübergreifende Datenübermittlung darf nur auf Basis einer schriftlichen Vereinbarung zwischen einer Speicherstelle und einer Anfragestelle erfolgen, außer wenn ein *matching* im Anschluss an die Einleitung einer bestimmten strafrechtlichen oder zivil-

rechtlichen Untersuchung gegen eine oder mehrere bekannte Personen von einer Behörde durchgeführt wird, die jegliche Tätigkeit im Zusammenhang mit der Durchsetzung des Strafgesetzes als ihre Hauptaufgabe leistet, um Beweise gegen diese Person oder Personen zu sammeln.

Die Einschränkung erstreckt sich jedoch nicht auf die Übermittlungs- und Verarbeitungsvorgänge der Daten, über die eine Privatperson verfügt. Die Strafverfolgungsbehörden können den Zugang zu Daten im Privatbesitz durch einen entgeltlichen Erwerb beim Datenmarkt oder durch ein unmittelbares Ersuchen an den Privaten haben. Es gibt keine Regelung, nach der die Datenübermittlung Privater an die Strafverfolgungsbehörden verhindert oder aber zur Pflicht gemacht wird. Die Strafverfolgungsbehörden können Daten von Privatpersonen erhalten, aber nur, wenn diese dazu bereit sind. Viele Datenbesitzer willigen ohne eine *subpoena* oder eine gerichtliche Anordnung aber nicht ein, ihre Daten preiszugeben. Zum Zweck des Datenabgleichs dürfen die Strafverfolgungsbehörden somit die Datenübermittlung von einer anderen Behörde mit Zustimmung des Betroffenen fordern, personenbezogene Daten im Datenmarkt entgeltlich erwerben oder die Übermittlung privater Daten durch eine gerichtliche Anordnung erzwingen.

Die auf diese Weise erhaltenen Daten werden durch eine Reihe von Verfahren abgeglichen: einer Auswahl von Daten, einer Datenbereinigung, einem *matching*, einer Inferenz, einem Filtern der Treffer und einer Entscheidung aufgrund von Ergebnissen des Datenabgleichs.

b) Vergleichbare Daten

Beim Blick auf 5 U. S. C. § 552a (a) (4) kann festgestellt werden, dass die Vorschrift keine Beschränkung bezüglich Art, Inhalt und Umfang personenbezogener Daten vorsieht, die behördenübergreifend übermittelt und abgeglichen werden dürfen. Vergleichbare Daten nach dem 5 U. S. C. § 552a (a) (4) sind weder auf unsensible personenbezogene Daten noch auf Namen, Anschrift und Geburtsdatum der betreffenden Personen eingeschränkt. Sämtliche personenbezogenen Daten, die bereits bei einer Behörde gespeichert sind, können zum Zweck des Datenabgleichs herangezogen werden. Eine Behörde kann personenbezogene Daten erheben und speichern, indem sie die Daten durch Beobachtung der betroffenen Person oder ihres Verhaltens und als Nebenprodukt einer Transaktion zwischen der Behörde und der betroffenen Person erstellt sowie von der betroffenen Person selbst, von einer anderen Behörde oder von privaten

Datenbesitzern erwirbt. Die auf diese Weise erhobenen und dann gespeicherten Daten dürfen zum Gegenstand eines Datenabgleichs gemacht werden.

c) Verwendung des Datenabgleichs

Ein *Computer Matching* wird vor allem dazu durchgeführt, um die Berechtigung oder die fortwährende Einhaltung gesetzlicher und aufsichtsrechtlicher Anforderungen von Bewerbern, Empfängern oder Begünstigten von oder Teilnehmern an der Erbringung von Dienstleistungen in Bezug auf Geld- oder Sachleistungen oder Zahlungen im Rahmen von Bundesleistungsprogrammen festzustellen oder zu überprüfen, um Zahlungen zurückzuzahlen oder Schulden im Rahmen solcher Bundesleistungsprogramme zu tilgen.

Bei einer behördenübergreifenden Datenübermittlung zum Zweck eines Datenabgleichs bedarf es einer Zustimmung des Betroffenen, wenn es sich nicht um Fälle nach 5 U.S.C. 552a (b) (1) bis (12) handelt. Denn bei dieser Datenübermittlung müssen Daten eine Zweckentfremdung erfahren. Dies darf nur auf Basis einer Zustimmung der betroffenen Personen erfolgen. Diese Anforderung umgehen die Behörden häufig, indem sie den Ausnahmetatbestand in der Praxis großzügig auslegen und dann viele Abgleichvorgänge im Rahmen des Ausnahmetatbestandes durchführen oder indem sie behaupten, dass alle Datenübertragungen zwischen Regierungsstellen interne und nicht externe Übertragungen sind, weil sie angeblich Mitglieder eines monolithischen öffentlichen Dienstes sind. Diese Haltung kann es in der Praxis weniger sinnvoll oder sogar unmöglich machen, das Recht auf informationelle Selbstbestimmung durch spezifische Kontrollen mit verfahrensrechtlichen und organisatorischen Vorkehrungen zu schützen.

Eine behördenübergreifende Datenübermittlung zum Zweck eines Datenabgleichs darf nur auf Basis einer schriftlichen Vereinbarung zwischen einer Speicher- und einer Anfragestelle erfolgen. Die schriftliche Vereinbarung muss den Zweck des geplanten Datenabgleichs festlegen, die Datensätze beschreiben, abgeglichen werden, und das Verfahren zur Benachrichtigung über unerwünschte Ereignisse auf der Grundlage eines Datenabgleichs festlegen.

d) Aufbewahrungsdauer der Daten

Die Festlegung des Verfahrens zur Aufbewahrung und rechtzeitigen Vernichtung von Daten, die von einer Anfragestelle in einem Datenabgleich erstellt wurden, bleibt den Behörden zur Entscheidung überlassen. Das Verfahren hängt nur von der schriftlichen Vereinbarung ab. Geregelt ist nur, dass die Behörden Verfahren für die Rückgabe der Datensätze an die Speicherstelle oder die Vernichtung von Datensätzen erhalten müssen, die in einem Datenabgleich verwendet werden. Aber die Regelung gilt nur für den Abgleich, der die bei Behörden gespeicherten Daten verwendet. Bei privaten Daten wird diese Anforderung nicht angewendet. Es gibt hier keine Bestimmung über Aufbewahrungsfristen, Rückgabezeiten von Daten an eine Speicherstelle oder Löschungs- oder Vernichtungszeiten nach der Beendigung eines Abgleichs außer unter besonderen Umständen.

e) Mitteilungspflicht

Zum Schutz der Freiheitsrechte der Bürger sind neben den *vor* dem Abgleich erforderlichen Verfahren auch wichtige verfahrensrechtliche Vorkehrungen *nach* dem Datenabgleich getroffen. Die erste Maßnahme stellt die Forderung nach einer unabhängigen Überprüfung der Daten durch die Behörden dar, die an einem Datenabgleich teilgenommen haben. Keine nachteilige Entscheidung aufgrund von Ergebnissen eines Datenabgleichs darf außerdem getroffen werden, bis die Betroffenen über die mögliche Entscheidung benachrichtigt werden. Der Computer Matching Act verpflichtet die Behörden dazu, die Benachrichtigungsmethode der betroffenen Personen in der Vereinbarung anzugeben. Die Benachrichtigungspflicht wird hier nicht durch einen Datenabgleich, sondern durch nachteilige Maßnahmen aufgrund von Ergebnissen eines Datenabgleichs ausgelöst.

Die spezifische Kontrolle zum Schutz der Freiheitsrechte eines Einzelnen bilden die Auskunft des Kongresses sowie die Einrichtung eines Datenaufsichtsausschusses mit Berichtspflicht. Eine Kopie der schriftlichen Vereinbarung ist dreißig Tage vor Beginn der Maßnahme an einen Ausschuss des Kongresses zu schicken. Damit wird die parlamentarische Kontrolle der Maßnahme gesichert. Darüber hinaus müssen alle am *Computer Matching* beteiligten Behörden einen Datenaufsichtsausschuss einrichten. Er dient als ein behördeninternes Kontrollzentrum dazu, die Beachtung der Datenschutzvorschriften durch die Behörde zu überwachen und zu

koordinieren. Er soll einen jährlichen Bericht erstellen und diesen dem Leiter der Behörde und dem *Office of Management and Budget* vorlegen.

3. Vergleich

a) Organisationsstruktur

In Deutschland ist ein maschineller Datenabgleich grundsätzlich verboten und wird erst durch § 98a StPO erlaubt. In § 98a und 98b werden der mögliche Zweck und die Voraussetzungen eines Datenabgleichs, die Übermittlungs- und Unterstützungspflicht einer Speicherstelle, der Richtervorbehalt, eine Rückgabe bzw. Löschung schon ausgeglichener Daten, die Benachrichtigungspflicht der Betroffenen und die Unterrichtungspflicht der für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz zuständigen Stelle konkret geregelt. In den USA ist eine Datenverarbeitung hingegen grundsätzlich erlaubt, soweit keine weiteren Bestimmungen gelten. Ein maschineller Datenabgleich wird also nur in den öffentlichen Bereichen eingeschränkt, aber nicht in den privaten. Denn der Computer Matching and Privacy Protection Act von 1988 legt nur die Verfahren für den Datenabgleich durch die Bundesbehörden fest.

Die deutsche Rasterfahndung ist gemäß § 98a StPO ein maschineller Abgleich von Daten, die sowohl bei öffentlichen als auch bei privaten Stellen bereits gespeichert sind, um Unverdächtige auszuschließen (negative Rasterfahndung) oder bestimmte Verdächtige festzustellen (positive Rasterfahndung). Nicht nur ermächtigt die Vorschrift die Strafverfolgungsbehörden dazu, an eine Speicherstelle das Ersuchen bezüglich bestimmter Daten zu richten und die Daten automatisch abzugleichen, sondern sie verpflichtet die Speicherstelle auch dazu, die Strafverfolgungsbehörden bei einem Datenabgleich zu unterstützen. Die Strafverfolgungsbehörden dürfen Daten einer anderen Stelle nur aufgrund dieser Bestimmungen anfordern und abgleichen. In den USA, wo jede Datenverarbeitung grundsätzlich zulässig ist, unterliegen demgegenüber angesichts hoher Gefahren bei der Datenverarbeitung durch den Staat nur solche Datenabgleiche Gesetzen, bei denen es einer behördenübergreifenden Datenübermittlung bedarf. Ein solcher Datenabgleich, also das *Computer Matching*, ist ein maschineller Abgleich von Daten, die nur bei öffentlichen Stellen bereits gespeichert sind, damit Verstöße vor allem in der Regierungsverwaltung, also im Hinblick auf staatliche Leistungsprogramme festgestellt werden. Es existiert keine spezifische Bestimmung, die von einer privaten Stelle eine

Übermittlung ihrer Datenbestände erzwingen kann, sondern die Strafverfolgungsbehörden können die Daten entweder entgeltlich am Datenmarkt kaufen oder direkt bei der privaten Stelle abhängig von ihrer Übermittlungsbereitschaft oder aufgrund einer gerichtlichen Übermittlungsanordnung erwerben.

Die Rasterfahndung und das *Computer Matching* beziehen die Vielzahl von Nichtverdächtigen ohne ein Vorliegen eines konkreten Verdachts ein. Die beiden Maßnahmen gehen von einem nichtindividualisierten Verdacht aus. Zur Anwendung der deutschen Rasterfahndung reichen zureichende tatsächliche Anhaltspunkte aus. Selbst der nach der Rasterung verbleibende „Bodensatz" weist noch keinen konkreten Tatenbezug auf, sondern dient als Ansatzpunkt für die konventionelle Fahndung, in deren Verlauf sich möglicherweise ein solcher Bezug herausstellt.[641] Es muss ohne einen täterbezogenen Verdacht lediglich der Verdacht vorliegen, dass eine bestimmte Straftat begangen wurde. Der Computer Matching Act setzt als eine Blankettnorm[642] zur Durchführung eines *Computer Matching* nicht einmal einen Anfangsverdacht voraus. Die Rasterfahndung dient als Mittel zur Einleitung konventioneller Ermittlungen, während das *Computer Matching* als eine Entscheidungshilfe funktioniert.

b) Vergleichbare Daten

Die Gemeinsamkeit zwischen den beiden Ländern liegt darin, dass bei den Daten, die für einen Datenabgleich zur Verfügung stehen, weder eine Einschränkung auf Namen, Anschrift und Geburtsdatum der betreffenden Personen noch eine Differenzierung zwischen sensiblen und unsensiblen Daten vorgesehen ist. Die deutsche Strafprozessordnung enthält keine nähere Erläuterung im Hinblick auf Art, Inhalt und Umfang der zu Rasterfahndungszwecken heranzuziehenden Daten. Die US-amerikanische Rechtsordnung zählt zwar konkrete für einen Abgleich verfügbare Daten auf, macht jedoch durch die Anwendung des Ausdrucks „nicht darauf beschränkt" das Nicht-Vorliegen einer Einschränkung deutlich. Solange Daten bereits bei einer anderen Stelle gespeichert sind und erhalten

641 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 72.

642 *Gropp*, Rechtsvergleicher Querschnitt, in: Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, 1993, 815 (844 f.).

werden können, dürfen alle personenbezogenen Daten unbegrenzt zum Datenabgleich herangezogen werden.

c) Verwendung des Datenabgleichs

Die deutsche Rasterfahndung ist mit bestimmten Voraussetzungen verbunden. Für die Zweckentfremdungsnutzung von Daten, also dafür, dass Daten, die für einen bestimmten Zweck erhoben wurden, später aber für einen anderen Zweck verwendet werden, sind einige verfahrensrechtliche Vorkehrungen in den beiden Ländern getroffen worden.

Als erste Voraussetzung fordert die Rasterfahndung ein Vorliegen zureichender tatsächlicher Anhaltspunkte dafür, dass eine Katalogtat von erheblicher Bedeutung, die in § 98a Abs. 1 Satz 1 aufgeführt wird, begangen wurde. Schwierigkeiten bezüglich des Begriffs „von erheblicher Bedeutung" und unüberschaubare Katalogtaten wurden schon oben erwähnt. Die zweite Voraussetzung ist die Subsidiarität der Rasterfahndung gegenüber konkurrierenden Maßnahmen. Eine Rasterfahndung darf nur dann angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder wesentlich erschwert wäre. Drittens darf eine Rasterfahndung grundsätzlich durch einen Richter angeordnet werden. Damit wird den Gefahren einer Rasterfahndung begegnet. Der Richtervorbehalt kann aber durch die Möglichkeit der staatsanwaltschaftlichen Eilanordnung gefährdet werden, auch wenn diese nachträglich eine richterliche Entscheidung einholen muss. Angesichts der Bedeutung der Rasterfahndung ist es schwierig, die Umstände vorzustellen, unter denen eine staatsanwaltschaftliche Eilanordnung benötigt wird.

Der Computer Matching Act schließt eine Datenübermittlung zum Zweck eines Datenabgleichs an bestimmten Voraussetzungen an. Erstens ist eine Zustimmung der betroffenen Personen erforderlich. Eine Datenübermittlung ohne Zustimmung der Betroffenen ist grundsätzlich verboten. Aber die Anforderung wird in der Praxis durch die behördlichen totalitären Tendenzen und die weite Auslegung eines Ausnahmetatbestandes namens ‚routine use' vielfach umgangen. Dies schwächt die Bedeutung der Zustimmung des Betroffenen als eine Schwelle für die Datenübermittlung. Zweitens beinhaltet der Computer Matching Act keine inhaltlichen Leitlinien, sondern fordert für Datenübermittlungen zum Zweck eines Datenabgleichs, dass eine schriftliche Vereinbarung zwischen einer Speicherstelle und einer Anfragestelle getroffen wird. Die konkreten Inhalte

über die Vereinbarung werden nicht gesetzlich geregelt. Sie sind den Behörden überlassen. Die Behörden müssen den Zweck des geplanten Datenabgleichs, die abzugleichenden Datensätze und die Verfahren zur Benachrichtigung der Betroffenen in der Vereinbarung festlegen.

Für die Durchsetzung der Rasterfahndung sind gesetzlich verschiedene Schwellen festgelegt, indem zureichende tatsächliche Anhaltspunkte für Katalogtaten von erheblicher Bedeutung, die Subsidiarität einer Rasterfahndung und der Richtervorbehalt angefordert werden. Demgegenüber ist in den USA nur die behördenübergreifende Datenübermittlung zum Zweck des Datenabgleichs von einer Zustimmung der Betroffenen und dem Bedürfnis einer schriftlichen Vereinbarung abhängig. Es ist aber zweifelhaft, ob die Anforderungen als tatsächliche Schwellen funktionieren können, weil die Bedeutung einer Zustimmung der Betroffenen schwach ist und die schriftliche Vereinbarung inhaltlich nicht gesetzlich geregelt wird.

d) Aufbewahrungsdauer der Daten

Die deutsche Rechtsordnung sieht angesichts der Missbrauchsgefahr und der großen Bedeutung personenbezogener Daten in der modernen Gesellschaft eine maximale Aufbewahrungsdauer der Daten vor. So sind die erhaltenen Datenträger nach Beendigung des Abgleichs unverzüglich an die betreffenden Speicherstellen zurückzugeben und Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden.

Die Aufbewahrungsdauer der Daten, die zum Zweck des Datenabgleichs übermittelt wurden, wird in der US-amerikanischen Regelung hingegen nicht berücksichtigt. Es obliegt den betroffenen Behörden, die Aufbewahrungsfristen oder die Rückgabe-, Löschungs- oder Vernichtungszeiten von Daten nach der Beendigung des Datenabgleichs festzulegen.

e) Mitteilungspflicht

Die deutsche Strafprozessordnung statuiert die Pflicht zur nachträglichen Unterrichtung der betroffenen Personen und des zuständigen Datenschutzbeauftragten. Die nachträgliche Unterrichtung der betroffenen Personen wird aber nur auf die Personen eingeschränkt, gegen die nach Abgleich der Daten weitere Ermittlungen geführt wurden. Die Unterrichtung

des zuständigen Datenschutzbeauftragten erfolgt erst nach Beendigung der Rasterfahndung. Personen, die zwar in eine Rasterfahndung einbezogen waren, aber gegen die keine weiteren Ermittlungen geführt wurden, werden nicht benachrichtigt. Die nachträgliche Unterrichtung des zuständigen Datenschutzbeauftragten kann außerdem mangels der Möglichkeit der Vorabunterrichtung, der Beratung und der begleitenden Kontrolle die effektive Kontrolle des Datenschutzes nicht garantieren.

In den USA werden die betroffenen Personen zur Gewährleistung der Anfechtungschance des Einzelnen benachrichtigt, wenn aufgrund der Ergebnisse des Datenabgleichs Leistungen reduziert oder gekündigt werden, also wenn eine nachteilige Entscheidung aufgrund der Ergebnisse des Datenabgleichs erwartet wird. Die Benachrichtigung ist mit einer möglichen nachteiligen Entscheidung nach Beendigung des Datenabgleichs, aber nicht mit dem Datenabgleich als solchem durchgeführt. Personen, gegen die keine nachteilige Entscheidung nach Beendigung des Datenabgleichs erwartet wird, werden nicht benachrichtigt. Mit der Pflicht zur Vorabeinbringung der schriftlichen Vereinbarung an einen zuständigen Ausschuss des Kongresses und zur Einrichtung des Datenaufsichtsausschusses mit Berichtspflicht innerhalb jeder Behörde ist die Möglichkeit der Vorabunterrichtung, Beratung und begleitenden Kontrolle garantiert.[643]

Tabelle 5: Gesetzliche Ausgestaltungen des Datenabgleichs in den beiden Ländern

	Anwendungsbereich	Voraussetzungen	Spezifische Kontrolle
Deutschland	§ 98a StPO Behördlicher computergestützter Datenabgleich mit polizeiexternen Dateien	Straftat von erheblicher Bedeutung; ergänzt durch typisierenden Katalog	Richtervorbehalt (staatsanwaltschaftliche Eilanordnungsmöglichkeit); Unterrichtung des Betroffenen; Unterrichtung des Datenschutzbeauftragten

643 Einen anschaulichen Vergleich des Datenabgleichs in den beiden Ländern siehe Tabelle 5.

USA	Behördlicher computergestützter Datenabgleich nur mit bei öffentlichen Stellen gespeicherten Dateien	Prozedurale Blankettnorm Zustimmung des Betroffenen für Zweckentfremdungsnutzung von Daten	Matching Agreement; Information an den Kongress; Errichtung eines Datenaufsichtsausschusses

III. Vorratsdatenspeicherung

1. Deutschland

a) Geschichtlicher Hintergrund

Nach § 12 FAG[644] und § 5 TDSV[645] wurde es möglich, Auskunft über bestimmte Verbindungsdaten zu verlangen. Ausschließlich damit konnte die Erhebung von bei einer Anordnung schon gelöschten bzw. nicht gespeicherten vergangenen Verbindungdaten jedoch nicht garantiert werden. Als Reaktion darauf wurden sowohl in Deutschland als auch auf europäischer Ebene mehrfach Versuche unternommen, die Telekommunikationsanbieter gesetzlich zur vorrätigen Speicherung bestimmter Verbindungsdaten zu verpflichten, aber diese Versuche scheiterten. Die gesetzliche Verpflichtung vorrätiger Speicherung bestimmter Verbindungsdaten in Deutschland gelang als Umsetzungspflicht der Vorratsdatenspeicherungsrichtlinie auf europäischer Ebene, die als Reaktion auf eine Reihe von Terroranschlägen erlassen wurde.[646]

Auf europäischer Ebene werden nicht nur das Recht auf Privatsphäre, sondern auch das Recht auf Schutz der sie betreffenden personenbezogenen Daten sowohl im Primärrecht als auch im Sekundärrecht ausdrücklich

644 Das Gesetz über Fernmeldeanlagen vom 3. Juli 1989 (BGBl. I S. 1455). Siehe auch oben Fn. 206.

645 Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (Telekom-Datenschutzverordnung) vom 24. Juni 1991, BGBl. 1991, I. S. 1391.

646 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105, S. 54–60.

anerkannt und geschützt. Vor allem bildet die Datenschutzrichtlinie[647] die Grundsätze bei der Verarbeitung von personenbezogenen Daten: dass die Datenerhebung verhältnismäßig zum jeweiligen Zweck ist; dass die Datenerhebung in der Regel die Zustimmung des Betroffenen voraussetzt; dass die Verarbeitung sensibler Daten grundsätzlich verboten ist. Durch die Richtlinie 2002/58/EG[648] und die Verordnung 45/2001/EG[649] werden darüber hinaus die Grundsätze der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation aktualisiert und die Rechtsvorschriften der Mitgliedstaaten zur Sicherstellung eines gleichwertigen Schutzniveaus der Grundrechte und Grundfreiheiten harmonisiert. Diese Harmonisierungsbemühungen haben aber wenig Wirkung, da die Datenschutzregelungen in der Europäischen Union immer noch viel dem Ermessen der Mitgliedstaaten überlassen. Dies hat zu den verschiedenen nationalen Gesetzen bezüglich des Datenschutzes geführt. Um diesen großen Unterschied zu vermeiden, wurde die Vorratsdatenspeicherungsrichtlinie[650] mit dem Ziel verabschiedet, diese verschiedenen nationalen Gesetze miteinander in Einklang zu bringen. Damit wurde die Verpflichtung der Mitgliedstaaten, bestimmte Daten auf Vorrat zu speichern, vorgesehen. Die Vorratsdatenspeicherungsrichtlinie zielt auf die Harmonisierung mitgliedstaatlicher Vorschriften über Vorratsdatenspeicherung und die Sicherstellung bestimmter Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten ab. Dafür werden die zu speichernden Daten und die Verwendungszwecke abschließend geordnet. Unter der Vorratsdatenspeicherung werden die Daten für eine eventuelle Anfrage mindestens sechs

---

647 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 23. November 1995 (ABl. EG Nr. L 281 S. 31–50).

648 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 31. Juli 2002 (ABl. EG Nr. L 201 S. 37–47).

649 Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

650 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105.

Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert.

Gegen die Vorratsdatenspeicherungsrichtlinie wurde zweimal Beschwerde eingereicht: zuerst wegen der Frage der Wahl der Rechtsgrundlage und danach wegen der Frage der Vereinbarkeit der Richtlinie mit den EU-Grundrechten. Die erste Klage wurde mit der Begründung abgewiesen, dass sich die Regelungen zur Vorratsdatenspeicherung „unmittelbar auf das Funktionieren des Binnenmarkts auswirken und die Richtlinie Tätigkeiten regelt, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind, damit sie die Dienstanbieter verpflichtet, bestimmte Daten auf Vorrat zu speichern“[651]. Die Frage über die Vereinbarkeit der Richtlinie mit den EU-Grundrechten wurde in der Vorabentscheidung des irischen High Court und des österreichischen Verfassungsgerichtshofs vorgelegt. Der EuGH erklärte dabei die Richtlinie für ungültig, weil sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkung auf das absolut Notwendige beschränken müssen, aber die in der Richtlinie vorgesehene Verpflichtung der Telekommunikationsanbieter nicht auf das Notwendige beschränkt gewesen sei.[652] Das Problem liege darin, die Daten aller Personen anlassunabhängig in umfassender Weise zu speichern, keine Einschränkung auf konkrete schwere Straftaten vorzusehen und die Speicherungsdauer unabhängig von den unterschiedlichen Datenkategorien zu bestimmen.[653] Auch in den weiteren Vorabentscheidungsverfahren hat der EuGH klargestellt, dass eine nationale Regelung, die eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien zulässt, nicht mit dem Unionsrecht vereinbar sei.[654] Mit den Urteilen des EuGHs wird betont, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben haben, mit dem Europarecht nicht vereinbar ist und dass die Vorratsdatenspeicherung hinsichtlich der Art der Daten, der betroffenen Kommunikationsmittel sowie der betroffenen Personen und der Speicherungsdauer auf das absolut Notwendige zu beschränken ist.

651 EuGH, C-301/06, 10.2.2009, Rn. 71 und 82 f.
652 EuGH, C-293/12, 8.4.2014, Rn. 52 und 65.
653 EuGH, C-293/12, 8.4.2014, Rn. 58, 60 und 63.
654 EuGH, C-203/15, C-698/15, 21.12.2016.

Die Richtlinie wurde im Jahr 2007 in das deutsche Recht aufgenommen,[655] bevor der EuGH sie für ungültig erklärte. Dabei wurde das Doppeltürmodell gewählt. Die Ermächtigungsgrundlage zur Verwendung der Daten im Rahmen der Strafverfolgung ist in der StPO und die konkrete Verpflichtung der Telekommunikationsanbieter im TKG vorgesehen. Der durch die Umsetzung der Vorratsdatenspeicherungsrichtlinie neu eingeführte § 113a TKG a. F. forderte, dass die unterschiedlichen Datenkategorien je nach der angebotenen Dienstleistung sechs Monate lang gespeichert werden, dass die erforderlichen Maßnahmen zur Sicherstellung der Qualität und des Schutzes der gespeicherten Daten ergriffen werden und dass die gespeicherten Daten innerhalb eines Monats nach Ablauf der Speicherungsfrist zu löschen sind. § 113b TKG a. F. bestimmte hier die Verwendungszwecke und die Verlangens- und Übermittlungsvoraussetzungen der Daten. Mit dem § 100g StPO wurden die Voraussetzungen vorgesehen. Danach dürften ohne Wissen des Betroffenen Verkehrsdaten erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat oder eine Straftat mittels Telekommunikation, begangen hat. Bei einer Straftat mittels Telekommunikation wurden gesetzlich die Subsidiarität und die Verhältnismäßigkeit gefordert.

Das Umsetzungsgesetz ist auf Kritik gestoßen, die aus verfassungsrechtlichen Bedenken hervorging. Aufgrund von zahlreichen Verfassungsbeschwerden hat das Bundesverfassungsgericht mit seinem Urteil vom 2. März 2010 festgestellt, dass die §§ 113a und 113b des Telekommunikationsgesetzes in der Fassung des Artikels 2 Nummer 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 gegen Artikel 10 Abs. 1 des Grundgesetzes verstoßen und nichtig sind und dass 100g Abs. 1 Satz 1 der Strafprozessordnung, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden dürfen, auch gegen Artikel 10 Absatz 1 des Grundgesetzes verstößt und insoweit

655 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, vom 21. Dezember 2007 BGBl. I S. 3198 (Nr. 70); Geltung ab 01. Januar 2008.

nichtig ist.[656] Nach der Entscheidung sei die Vorratsdatenspeicherung zwar nicht schlechthin mit dem Grundgesetz unvereinbar und nicht von vornherein unverhältnismäßig im engeren Sinn, aber die Regelungen entsprechen nicht den verfassungsrechtlichen Anforderungen. Das Bundesverfassungsgericht forderte diesbezüglich die gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit, die eng beschränkten sowie konkreten gesetzlichen Regelungen über die Voraussetzungen für die Datenverwendung und deren Umfang und die hinreichenden Vorkehrungen zur Transparenz der Daten sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen.

Trotz der Tatsache, dass die Vorratsdatenspeicherung durch das Bundesverfassungsgericht für nichtig erklärt wurde, hat das praktische Sehnen nach ihr im Jahr 2015 zur erneuten Verabschiedung des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten geführt. Der Erlass dieses Gesetzes rührt nicht von der Umsetzungspflicht innerhalb der Europäischen Union her. Das Gesetz ist nach den Anforderungen des Bundesverfassungsgerichts von der abschließenden Aufzählung der Straftaten flankiert, bei denen die nach § 113b TKG gespeicherten Daten erhoben werden, und den Vorkehrungen zur Datensicherheit und zur Transparenz der Datenverwendung. Gegen das Gesetz haben sich erneut Antragsteller mit Anträgen auf Erlass einer einstweiligen Anordnung gewandt. Die Anträge wurden vom Bundesverfassungsgericht zwar abgelehnt. Hinsichtlich der verfassungsrechtlichen Bewertung der angegriffenen Regelungen stellen sich jedoch immer noch Fragen, die nicht zur Klärung im Eilrechtsschutzverfahren geeignet sind. Anschließend haben das Oberverwaltungsgericht für das Land Nordrhein-Westfalen[657] und das Verwaltungsgericht Köln[658] bei weiteren Klagen die Unvereinbarkeit des Gesetzes mit dem Unionsrecht erklärt. Das Bundesverfassungsgericht hat jedoch eine Aussetzung des Vollzugs der §§ 113a und 113b TKG sowie §§ 100g, 101a und 101b StPO ausdrücklich abgelehnt.[659] Eine Entscheidung der Hauptsache ist noch abzuwarten. Das geltende Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten ist jedenfalls bis zur endgültigen Entscheidung des Bundesverfassungsgerichts immer noch gültig.

656 BVerfGE 125, 260.
657 OVG NRW, 13 B 238/17.
658 VG Köln, 9 K 7417/17.
659 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240.

b) Aktuelle Rechtslage

Die Systematik der Vorratsdatenspeicherung gründet sich mit der Begründung der Speicherpflicht sowie der Bestimmung der Verantwortlichen und sonstiger Parameter im TKG und der korrespondierenden Zugriffsnorm für den Abruf durch die Strafverfolgungsbehörden in der StPO auf das Doppeltürmodell.[660] Da die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach dem BDSG grundsätzlich verboten sind, sind das TKG und die StPO hier die Ermächtigungsnormen. Der Diensteanbieter der Telekommunikation darf prinzipiell gemäß § 95 TKG Bestandsdaten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, und gemäß § 96 TKG bestimmte Verkehrsdaten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern erheben und verwenden. Außerdem dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. Unabhängig von dieser üblichen Datenerhebung und -verwendung hat der Diensteanbieter gemäß § 111 TKG zusätzlich für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern und andere Anschlusskennungen, den Namen und die Anschrift des Anschlussinhabers, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen zudem die Anschrift des Anschlusses, in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie das Datum des Vertragsbeginns vor der Freischaltung zu erheben und unverzüglich zu speichern, auch wenn diese Daten nicht für betriebliche Zwecke erforderlich sind. Vor der Einführung der Vorratsdatenspeicherung durfte die Strafverfolgungsbehörde nach den §§ 100g und 100j StPO nur die nach den §§ 95, 96 und 111 TKG beim Diensteanbieter gespeicherten Daten und die Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit erheben.

Vor der Einführung der Vorratsdatenspeicherung waren die Verkehrsdaten, die die Strafverfolgungsbehörde erheben darf bzw. kann, sehr eingeschränkt. Aber nach der Einführung der Vorratsdatenspeicherung werden

660 *Dalby*, Vorratsdatenspeicherung – Endlich?! KriPoZ 2016, 113, 113.

die Verkehrsdaten, die der Diensteanbieter zu speichern verpflichtet ist, erweitert und die Übermittlung dieser Daten wird abgesichert. Zugleich werden mehrere Maßnahmen getroffen, die die hohe Eingriffsintensität der Vorratsdatenspeicherung abfedern können.

aa) Zu speichernde Daten

Erbringer öffentlich zugänglicher Telekommunikationsdienste sind nach der Vorratsdatenspeicherung dazu verpflichtet, bestimmte Verkehrsdaten zu speichern. § 113b Abs. 2 bis 4 TKG beschreibt abschließend die Verkehrsdaten und die Standortdaten, die von den Erbringern öffentlich zugänglicher Telefon- und Internetzugangsdienste zu speichern sind.

§ 113b Abs. 2 regelt die einzelnen Speicherpflichten für Erbringer öffentlich zugänglicher Telefondienste. Er umfasst Ausprägungen wie Festnetz, Mobilfunk und Internettelefonie. Erbringer von Telefondiensten haben die folgenden Daten zu speichern: Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses, Datum und Uhrzeit von Beginn und Ende der Verbindung sowie Angaben zu dem genutzten Dienst. Die Erbringer mobiler Telefondienste haben zusätzlich die internationale Kennung des anrufenden und des angerufenen Endgerätes sowie Datum und Uhrzeit der ersten Aktivierung des Dienstes im Fall von Prepaid-Angeboten zu speichern. Im Fall von Internet-Telefondiensten wird auch die Speicherung der Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses sowie der zugewiesenen Benutzerkennungen verlangt. Die Speicherpflicht erstreckt sich auf unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe. Damit werden beispielsweise Fälle erfasst, in denen ein Teilnehmer von seinem Diensteanbieter per Kurznachricht darüber informiert wird, dass ein für seinen Anschluss bestimmter Anruf nicht entgegengenommen wurde, etwa weil der Anschluss belegt war oder sich das Mobiltelefon zur Zeit des Anrufs außerhalb des Versorgungsbereichs einer Funkzelle befand.[661]

Erbringer öffentlich zugänglicher Internetzugangsdienste haben die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, eine eindeutige Kennung des Anschlusses, über den der Internetzugang erfolgt, sowie eine zugewiesene Benutzerkennung sowie Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewie-

661 BT-Drs. 18/5088, S. 39.

senen Internetprotokoll-Adresse zu speichern.[662] Hier findet eine Speicherung der im Internet aufgerufenen Adressen nicht statt, damit auch auf Grundlage der zu speichernden Internetdaten nicht das gesamte Surfverhalten von Internetnutzern nachvollziehbar wird.[663]

Darüber hinaus sind im Fall der Nutzung mobiler Telefondienste die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung, also die konkreten Bezeichnungen der Funkzellen, zu speichern, über die die Telekommunikationsteilnehmer beim Verbindungsaufbau versorgt werden. Bei der Nutzung von öffentlich zugänglichen Internetzugangsdiensten durch Mobilfunk wird die Bezeichnung der Funkzelle gespeichert, die bei Beginn der Internetverbindung genutzt wird. In beiden Fällen sind zusätzlich die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben. Dies begründete der Gesetzgeber damit, dass die Funkzellen von den Erbringern öffentlich zugänglicher Telekommunikationsdienste nicht dauerhaft zugewiesen werden und die Angabe der Hauptstrahlrichtungen der einzelnen Funkantennen der Ermöglichung einer genauen Ermittlung des Standortes dient, von dem aus oder zu dem eine Telekommunikationsverbindung aufgebaut wurde.[664]

Ein merkwürdiger Aspekt der Vorratsdatenspeicherung ist vor allem, dass eine solche Datenspeicherung nicht durch einen Anlass hervorgerufen wird. Ohne dass ein Anlass zur Speicherung der in § 113b TKG genannten Daten erforderlich ist, werden die Daten aller Bürger für eventuelle Anfragen vorrätig gespeichert. Zur Speicherung dieser Daten wird weder ein Zusammenhang mit schweren Straftaten noch eine Zweckbeschränkung gefordert. Trotz erheblicher Bedenken bezüglich der Eingriffsintensität der

662 *Dalby* hält die Speicherpflicht für dynamische IP-Adressen für begrüßenswert. Für Bestandsdatenauskünfte zu dynamischen IP-Adressen darf nach § 113b TKG auf gespeicherte Verkehrsdaten zurückgegriffen werden. Zwar war bereits vorher ein Pool dynamischer IP-Adressen abfrag- und zuordenbar, doch die Speicherung dieser dynamischen IP-Adressen auf Grundlage der §§ 96 ff. TKG war hochstreitig, weil das Diensteunternehmen diese nicht für Abrechnungszwecke bei der heutigen Verbreitung von Flatrate-Tarifen benötigt: *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 116.

663 BT-Drs. 18/5088, S. 39. Das Bundesverfassungsgericht befürchtete in seinem Volkszählungsurteil die Gefahr eines umfassenden und detaillierten Bildes der jeweiligen Person – einer Herstellung von Persönlichkeitsprofilen: BVerfGE 65, 1 (17, 25).

664 BT-Drs. 18/5088, S. 39.

anlasslosen Speicherung[665] behauptet der Gesetzgeber die Minderung der Eingriffsintensität durch verschiedenste Anforderungen.[666]

bb) Zugriff auf Daten

Eine verpflichtend anlassunabhängige Datenspeicherung durch den Anbieter öffentlich zugänglicher Telekommunikationsdienste ergänzt sich durch die strengen Abrufmechanismen. Auf die nach der Vorratsdatenspeicherung gespeicherten Daten darf unter strikteren Voraussetzungen zugegriffen werden als auf die Daten, die gemäß § 96 TKG gespeichert sind. Der Unterschied beruht auf dem Risiko der Grundrechtsbeeinträchtigung der anlasslosen Speicherung der Vielzahl von Daten Unbeteiligter.

Das Telekommunikationsgesetz, das die Vorratsdatenspeicherung vorsieht, schränkt mit § 113c den Verwendungszweck der Vorratsdaten ein. Für den Zugriff auf die Daten zur Verfolgung besonders schwerer Straftaten werden ein Verdacht einer Katalogtat im Sinne des § 100g Abs. 2 Satz 2 Nr. 1–8 StPO, die auch im Einzelfall besonders schwer wiegt, die Erforderlichkeit zur Sachverhaltserforschung oder zur Aufenthaltsermittlung und die besondere Verhältnismäßigkeit vorausgesetzt. Hier sind also eine Einschränkung auf eine der Katalogstraftaten als eine Anlasstat zum Zugriff auf die Daten, die wesentliche Erschwernis oder die Erfolgsaussichten anderer Maßnahmen und die besondere Verhältnismäßigkeit dafür erforderlich, dass sich die Ausnahmen zum Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen. Alle Voraussetzungen gelten auch für die Erhebung aller Verkehrsdaten (sog. Funkzellenabfrage), die in einer bestimmten Funkzelle angefallen und nach § 113b TKG gespeichert sind. Im Vergleich zu der Erhebung der Vorratsdaten des bekannten Verdächtigen wäre bei einer Funkzellenabfrage, die die Telekommunikationsdaten völlig unbeteiligter Personen erheben lässt, die Gefahr einer Grundrechtsbeeinträchtigung viel höher. Dieser unterschiedliche Grad der Gefahr kommt aber gesetzlich nicht in Betracht.

Der Datenerhebung nach § 100g StPO muss eine richterliche Anordnung vorausgehen. Richtigerweise ist für die Erhebung der nach § 113b

665 Bejahend *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 116; kritisch dazu *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 538.

666 BT-Drs. 18/5088, S. 39.

TKG gespeicherten Daten die Möglichkeit der Anordnung der Staatsanwaltschaft bei Gefahr im Verzug ausgeschlossen.

Die Weitergabe der Daten, die durch Maßnahmen nach § 100g Abs. 2 StPO, auch in Verbindung mit § 100g Abs. 3 Satz 2, erhoben wurden, ist unter dem Zweckbindungsgrundsatz nach § 101a Abs. 4 eingeschränkt zulässig. Diese Daten dürfen also ohne Einwilligung der Beteiligten der betroffenen Telekommunikation in anderen Strafverfahren zur Aufklärung einer Straftat, aufgrund derer eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person, verwendet werden.

Der Gesetzgeber versucht damit, die Gefahr einer Grundrechtsbeeinträchtigung durch eine verpflichtende Speicherung bestimmter Daten aller Bürger mit einer strikten Einschränkung der Voraussetzungen der Datenverwendung und -weitergabe aufzurechnen.

cc) Löschungspflicht

Die Speicherung der Verkehrsdaten, die grundsätzlich nach dem BDSG verboten, jedoch nach dem TKG ausnahmsweise zulässig ist, erfolgt nicht auf unbestimmte Zeit. Zum Schutz personenbezogener Daten und zur Minderung der Eingriffsintensität der Vorratsdatenspeicherung sieht das TKG eine bestimmte Speicherungsfrist vor. Bei der Bestimmung der Speicherungsfrist kommt die unterschiedliche Bedeutung verschiedener Daten in Betracht. Die nach der Vorratsdatenspeicherung gespeicherten Daten müssen nach maximal zehn Wochen irreversibel gelöscht werden. Hingegen erfordert das TKG keine Löschung oder Rückgabe für die vom Diensteanbieter bereits an eine zuständige Behörde übermittelten Daten. Denn die nach einer gerichtlichen Anordnung erhaltenen Daten, die vom Gericht unter einer hinreichenden Erörterung der Angemessenheit der Maßnahme zur Ermittlung erteilt wird, dürfen aufgrund einer engen Zweckbegrenzung für die Verwendung dieser Daten nicht für andere Zwecke verwendet werden.

dd) Mitteilungspflicht

Zum Rechtsschutz des Einzelnen wird eine Benachrichtigung an die Beteiligten der betroffenen Telekommunikation grundsätzlich vor der Erhe-

bung der Verkehrsdaten nach § 100g StPO garantiert. Aber die Benachrichtigung kann ausnahmsweise zurückgestellt werden oder unterbleiben, wenn das öffentliche Interesse überwiegt. Das Unterbleiben oder die Zurückstellung der Benachrichtigung ist nur auf Anordnung des zuständigen Gerichts zulässig.

2. USA

a) Geschichtlicher Hintergrund

Eine vorrätige und anlasslose Speicherung bestimmter Daten für eine eventuelle Ermittlung ist in den US-amerikanischen Gesetzen nicht zu finden. Zwar wurde die Einführung dieser Speicherungspflicht im Parlament mehrmals versucht, aber ihre Gesetzgebung konnte kein einziges Mal verwirklicht werden. Das Scheitern kann auf zwei Gründe zurückgeführt werden. Ein Grund ist das fehlende Datenschutzgesetz im Privatsektor. Da es kaum Einschränkungen der Datenspeicherungspraxis im Privatsektor gibt, kann ein privates Unternehmen ohne weitere Einschränkungen ungeheure Daten speichern und diese soweit es das will auch verarbeiten. Der Staat sorgt sich relativ wenig darum, ob die Daten zum Anfragezeitpunkt nicht oder nicht mehr gespeichert sind.

Ein anderer Grund liegt in den Erfahrungen mit der staatlichen Datenspeicherungspraxis im Laufe der Geschichte. Die Antidrogenbehörde DEA hat zwanzig Jahre lang Milliarden von Telefonverbindungsdaten gespeichert. Sie hat nur mit der administrativen *subpoena* von Telefonanbietern die Listen aller Anrufe aus den USA ins Ausland erhalten und erforderlichenfalls an andere Behörden weitergeleitet. Diese Anfangsdaten, die Hinweise für die Ermittlung geben, wurden durch die *parallel construction* abgedeckt. Diese Speicherungspraxis durch die DEA wird auf verschiedene Weisen von der NSA fortgesetzt. Da die Praxis der Metadatensammlung der NSA vor der Snowden-Offenlegung kaum bekannt war, wurden die Datensammlungs- und Datenverwendungsbefugnisse der NSA unter verdeckten Programmen missbraucht. Um den Missbrauch zu verhindern, wurde der Foreign Intelligence Surveillance Act (FISA) erlassen und der FISA-Court etabliert. Das Gesetz setzt für eine Datensammlung einen *probable cause* voraus. Der *probable cause* bezieht sich darauf, dass das Ziel der elektronischen Überwachung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist und dass sich die gesuchten Informationen auf die nationale Sicherheit beziehen, aber nicht auf einen Anlass dazu

oder auf einen Verdacht darauf, dass das Ziel ein Verbrechen begangen hat oder begehen wird. Der Datenaustausch zwischen dem Geheimdienst und der Strafverfolgungsbehörde wurde blockiert, damit eine Negierung der Notwendigkeit einer rechtmäßigen Titel-III-Anordnung und eine Umgehung ihrer Voraussetzungen vermieden werden.

Die Terroranschläge vom 11. September 2001 haben vieles verändert. Eine der Veränderungen war die Erweiterung der Befugnisse der NSA durch den PATRIOT Act. Mit diesem Gesetz konnten Telekommunikationsunternehmen unter bestimmten Bedingungen freiwillig Kommunikations- und Standortdaten an die Strafverfolgungsbehörden übergeben. Die Datenarten, die mit einer *subpoena* erhoben werden können, wurden ebenfalls erweitert. Außerdem wurde die Mauer zwischen den Nachrichtendienst- und den Strafverfolgungsbehörden durchbrochen. Der Abschnitt 215 PATRIOT Act eröffnete die Möglichkeit, vor dem FISC eine geheime gerichtliche Anordnung zu beantragen. Der Abschnitt 215 stellte auch die parlamentarische Kontrolle für das FISA-Programm zur Verfügung. Trotz der erweiterten Möglichkeit einer geheimen gerichtlichen Anordnung meinte die Regierung, dass sie aufgrund der Third-Party-Doktrin auch ohne gerichtliche Anordnungen Daten erheben darf. Unter diesen Umständen hat die NSA anlasslos und ohne einen Verdacht Listen mit allen Anrufen erhoben.

Die Massentelefoniemetadatensammlung durch die NSA wurde erst durch die Enthüllung des ehemaligen NSA-Mitarbeiters Snowden entdeckt. Die Massenüberwachung wurde zwar mit einigen Sicherungen wie etwa einer gerichtlichen sowie einer parlamentarischen Kontrolle und den *minimization procedures*,[667] die durch den FISA eingeführt wurden, in gewissem Maße begrenzt. Die Speicherpraxis der NSA ist jedoch wegen der einseitigen Vorlegung der Daten durch die Regierung als Grundlage der Entscheidung des FISC, des Zusammenbruchs der Mauer zwischen Nachrichtendienst- und Strafverfolgungsbehörden, der Erweiterung der Befugnisse der NSA und der Third-Party-Doktrin auf heftige Kritik gestoßen.

Nach dem Snowden-Skandal hat die Frage über die Rechtmäßigkeit und die Verfassungsmäßigkeit des Metadatensammlungsprogramms der NSA für Massentelefonie vor den Gerichten zu völlig unterschiedlichen

667 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 442 f.

Ergebnissen geführt.[668] Um das Problem der Rechtsunsicherheit zu lösen, wurde der Freedom Act[669] erlassen. Das Gesetz stellt das Metadatensammlungsprogramm der NSA in zweierlei Hinsicht unter strengere Voraussetzungen: zum einen gibt es eine Einschränkung des Mechanismus, zum anderen eine starke Forderung nach Datenverarbeitungstransparenz und öffentlicher Berichterstattung. Unter dem Gesetz muss die Einholung einer FISC-Anordnung für die Metadatensammlung erfolgen. Die Datensammlung ist keine allgemeine, sondern eine gezielte Sammlung von Telefonmetadaten. Nicht mehr die Regierung speichert die Daten, sondern auch das Unternehmen selbst. Es speichert die Verbindungsdaten für eventuelle Anfragen. Mit diesem Gesetz wurde die geheime Natur der FISA-Anordnung ausgeschlossen und die Möglichkeit der Benachrichtigung an den Betroffenen eröffnet. Angesichts dieser geschichtlichen Erfahrungen und der Umstände des fehlenden Datenschutzgesetzes wird in den USA keine Vorratsdatenspeicherung, sondern nur die anlassgebundene Datenspeicherung (das sog. Quick-Freeze-Verfahren) praktiziert.

b) Aktuelle Rechtslage

Um die absichtliche Überwachung kabelgebundener Kommunikationen ohne Einschränkung im Hinblick auf die aussagekräftige Bedeutung der Speicherung und der Nutzung von Telekommunikationsdaten zu verhindern, haben die USA im Jahr 1968 den Federal Wiretap Act[670] erlassen. Anschließend wurde das Gesetz durch den ECPA von 1986[671] geändert, damit auch die drahtlosen Kommunikationen erfasst werden können. Das ECPA besteht aus dem Wiretap Act, dem Stored Communications Act und dem Pen Register Act. Im Wiretap Act geht es um die Überwachung laufender Kommunikationen, im SCA um die Erhebung gespeicherter Kommunikationsdaten und im Pen Register Act um die Zulassungsbedingungen eines Geräts für die Ausspähung künftiger Kommunikationsdaten. Für einen bedeutungsvollen Vergleich konzentrierte sich die vorliegende Arbeit auf die Behandlung bereits gespeicherter oder künftig zu speichern-

668 Beispielsweise ACLU v. Clapper, 959 F. Supp. 2d 724 (S. D. N. Y. 2013); Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D. D. C. 2013).

669 USA FREEDOM Act (the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), H. R. 3361, 113th Cong. (2013–2014).

670 Pub. L. 90-351, June 19, 1968, 82 Stat. 42 U. S. C. § 3711.

671 Pub. L. 99-508, October 21, 1986, 100 Stat. 1848.

der Kommunikationsdaten im SCA und Pen Register Act. Mit dem PATRIOT Act,[672] dem Freedom Act und dem Privacy Act werden der Zugang der Strafverfolgungsbehörden zu elektronischen Daten verbessert und der Datenschutz für die Verbraucher verringert. Das Gesetz ermöglicht das freiwillige Weitergeben von Verkehrs- und Bestandsdaten durch den Diensteanbieter der Telekommunikation an die Strafverfolgungsbehörden. Außerdem können mehr Daten von der Strafverfolgungsbehörde nur mit einer *subpoena* ohne Benachrichtigung des Betroffenen erhoben werden.

Die Systematik der US-amerikanischen Datenspeicherung stützt sich auf ein Verfahren, bei dem die Daten einer verdächtigen Person ab dem Zeitpunkt einer polizeilichen Anordnung gegen ein Telekommunikationsunternehmen erhoben und gespeichert werden (das sog. Quick-Freeze-Verfahren). Bei diesem Verfahren kann nur auf die zu und ab dem Zeitpunkt einer Anordnung noch vorhandenen und entstehenden Verbindungsdaten zugegriffen werden. Dabei ist der Diensteanbieter nach dem CALEA von 1994[673] dazu verpflichtet, seine Netze so auszulegen, dass er auf das befugte behördliche Überwachungsersuchen reagieren kann.

aa) Zu speichernde Daten

Es gibt weder eine Verpflichtung für die Erbringer öffentlich zugänglicher Telekommunikationsdienste, anlasslos bestimmte Daten vorrätig zu speichern, noch gibt es eine Aufzählung, in der eindeutig identifiziert wird, welche die zu speichernden Daten wären. Früher speicherte die NSA selbst die von den Telekommunikationsanbietern übertragenen Daten. Eine Speicherung liegt nun ausschließlich in der Hand der Telekommunikationsanbieter. Der ECPA schreibt nicht die zu speichernden Daten vor, sondern die Voraussetzungen für den Zugriff auf die Daten, die von Anbietern schon gespeichert wurden. Der Erfolg eines behördlichen Zugriffs hängt von der Speicherpraxis der Telekommunikationsunternehmen vor der berechtigten Aufbewahrungsanordnung ab, weil gesetzlich keine Speicherpflicht bestimmt ist. Die Abhängigkeit von der privaten Speicherpraxis kann möglicherweise die Effektivität der strafrechtlichen Ermittlungen nicht gefährden, wenn eine Erhebung, Speicherung und

672 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

673 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001–1010.

Verarbeitung personenbezogener Daten grundsätzlich erlaubt sind. Ein Verbot gilt nach dem ECPA nicht schon für die Speicherung der Daten, sondern erst für die Übermittlung der Daten. § 2703 Abs. a ECPA schreibt ein grundsätzliches Verbot der Übermittlung von Kommunikationsinhalten und Verkehrsdaten vor, § 2703 Abs. b und c eröffnet jedoch die Ausnahmemöglichkeit der Übermittlung von Kommunikationsinhalten und Verkehrsdaten.

Außerdem werden die Daten, auf die eine Behörde zugreifen darf, mit Ausnahme von Daten, auf die aufgrund einer *subpoena* zugegriffen wird,[674] gesetzlich nicht eingeschränkt, solange sich diese Daten noch im Besitz von Erbringern öffentlich zugänglicher Telekommunikationsdienste befinden. Der Diensteanbieter von Telekommunikationen ergreift nach § 2703 Abs. f auf Ersuchen einer staatlichen Stelle alle erforderlichen Maßnahmen, um die Verkehrsdaten und andere Beweismittel in seinem Besitz bis zur Erteilung eines Gerichtsbeschlusses oder eines anderen Verfahrens aufzubewahren. Dabei sichert der CALEA die Durchsetzung der anlassgebundenen Datenspeicherung, indem die Telekommunikationsunternehmen mit der Übermittlung der verfügbaren Telekommunikationsdaten an die zuständige Stelle beauftragt werden. Eine Aufbewahrung erfolgt auf der Basis eines *warrant* oder einer gerichtlichen Anordnung. Nur beim Vorliegen eines *probable cause* oder wenn die staatliche Stelle konkrete und verständliche Fakten vorlegt, aus denen hervorgeht, dass Grund zu der Annahme besteht, Kommunikationsinhalt, Verkehrsdaten oder sonstige Informationen seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich, ist der Diensteanbieter dazu verpflichtet, diese Daten aufzubewahren. Hier ist weder ein Zusammenhang mit schweren Straftaten noch eine Zweckbeschränkung etwa zur Bekämpfung der organisierten Kriminalität erforderlich. Für eine Aufbewahrungsanordnung reicht es aus, den Zusammenhang mit der laufenden Untersuchung zu klären.

674 Eine Behörde kann die folgenden Daten, die mit den in Deutschland so genannten Bestandsdaten vergleichbar sind, auch allein mit einer *subpoena* erhalten: Namen, Adressen, Listen von Fernsprechanschlüssen, Daten über die Anzahl und die Dauer der Anrufe in einem bestimmten Zeitraum, die Dienstdauer (einschließlich des Anfangsdatums) und die Art der benutzten Dienste und Zahlungsmittel (einschließlich Kreditkarten- oder Bankkontonummer).

bb) Zugriff auf Daten

Für die Erhebung von Verkehrsdaten außer Inhaltsdaten, deren Speicherung eine staatliche Behörde vom Anbieter öffentlich zugänglicher Telekommunikationsdienste unter bestimmten Voraussetzungen anfordert, schränkt der ECPA den Verwendungszweck nicht ein, sondern sieht nur die Voraussetzungen vor, die die Datenverwendung ermöglichen. Die Verkehrsdaten dürfen entweder auf Basis der Zustimmung des Betroffenen oder eines *warrant* erhoben werden, eine gerichtliche Anordnung, die durch die Darstellung der spezifischen und klaren Tatsachen erworben wird, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, die angeforderten Daten seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich. Bestimmte Verkehrsdaten dürfen auch nur mit einem formellen schriftlichen Antrag oder einer *subpoena* erhoben werden. Der Diensteanbieter ist dabei nach dem CALEA dazu verpflichtet, die Behörde zu unterstützen. Damit wird die Datenübermittlung durch den Anbieter an die Behörde sichergestellt.

Während für die Verwendung eines Standorttrackers, der den Standort im mit bloßem Auge nicht sichtbaren Innenraum bekannt macht, ein *warrant* grundsätzlich vorausgesetzt wird, werden für die Standortdaten durch die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss während der Verbindung genutzt werden, die erleichterten Voraussetzungen nach dem SCA angewendet.

Gesetzlich ist weder ein Verwendungszweck noch eine Zweckbindung erforderlich. Die Verkehrsdaten, die eine Behörde auf diese Weise erhoben hat, dürfen daher ohne Einschränkungen an eine andere Behörde weitergeleitet werden.

cc) Löschungspflicht

Als die notwendige Folge eines Mangels eines Datenschutzgesetzes im Privatsektor sind die Anbieter von Telekommunikationsdiensten nicht dazu verpflichtet, ihre Daten innerhalb eines bestimmten Zeitraums zu löschen oder zu vernichten. Den Telekommunikationsunternehmen wird gesetzlich nur ein Rat erteilt, die personenbezogenen Daten effektiv und sicher zu löschen, wenn die Unternehmen ihre Daten löschen wollen. Zur effektiven Strafverfolgung wird nicht die Regelung einer Löschungspflicht, sondern die Sicherstellung bestimmter Daten innerhalb eines bestimmten Zeitraums gewählt. Die Telekommunikationsunternehmen bewahren ihre

Daten in der Praxis in der Regel dreißig bis neunzig Tage auf.[675] 18 U. S. C. § 2703 (f) stellt dabei die Speicherung der Daten mindestens für neunzig Tage – die zusätzlich noch um neunzig Tage verlängert werden können – sicher. Die Vorschrift garantiert die Speicherung der Daten für diesen Zeitraum, aber nicht die Löschung der Daten nach diesem Zeitraum. Darüber hinaus ist die unterschiedliche Speicherungsdauer je nach der Bedeutung der angefragten Daten nicht vorgesehen.

Es gibt auch keine Löschungs- oder Übermittlungsverbotsvorschrift bezüglich der bereits bei einer Behörde liegenden Daten nach deren Verwendung. Bei der Datenverwendung wird ebenfalls keine strikte Zweckbegrenzung gefordert. Zwar wird die Datenübermittlung an eine andere Behörde nach dem Privacy Act an eine schriftliche Aufforderung oder Einverständniserklärung der Betroffenen gebunden, es scheint aber schwierig zu sein, die Datenverwendung für andere Zwecke einzuschränken. Dies liegt daran, dass eine gerichtliche Anordnung, die die Datenübermittlung vom Telekommunikationsunternehmen an eine zuständige Behörde ermöglicht, nur mit bestimmten und klaren Fakten erteilt wird, die eine vernünftige Grundlage für die Annahme darstellen, dass die geforderten Daten im Zusammenhang mit einer laufenden Untersuchung stehen.

dd) Mitteilungspflicht

Die Benachrichtigung an die Beteiligten der betroffenen Telekommunikation ist nach dem 18 U. S. C. § 2703 ausschließlich für die Erhebung von Telekommunikationsinhalten nicht durch einen *warrant*, sondern durch eine *subpoena* oder eine gerichtliche Anordnung erforderlich, aber nicht für die Erhebung von Verkehrsdaten. Der Betroffene nimmt also keine Kenntnis von der staatlichen Erhebung seiner Verkehrsdaten und kann folgerichtig keinen Anspruch auf den Schutz gegen eine unbefugte oder übermäßige Erhebung, Speicherung oder Verwendung seiner Daten erheben.

675 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *McCullagh*, Gonzales Pressures ISPs on Data Retention, ZDNET News v. 27. Mai 2006, abrufbar unter: https://www.zdnet.com/article/gonzales-pressures-isps-on-data-retention/.

3. Vergleich

a) Geschichtlicher Hintergrund

Die Vorratsdatenspeicherung war in Deutschland inzwischen Widerspruch ausgesetzt: Mehrere Gesetzgebungsversuche waren gescheitert, das gelungene Gesetz wurde für nichtig erklärt und ein neues Gesetz zwar erneut erlassen, doch auch gegen dieses Gesetz wurden viele Einwände erhoben. Die praktische Erforderlichkeit der vorrätigen Datenspeicherung für eventuelle Anfragen wird teilweise anerkannt, wobei man angesichts der hohen Intensität des Eingriffs dieser Datenspeicherung viele Sicherungsmaßnahmen zum Privatsphären- oder Datenschutz des Einzelnen implementiert hat.

Demgegenüber ist der Gesetzgebungswille der Vorratsdatenspeicherung in den USA trotz vieler Forderungen nicht erfolgreich, nachdem die Tatsache offenbart wurde, dass in der Vergangenheit in der Praxis die Daten aller Personen ohne Einschränkung und im Geheimen erhoben und gespeichert wurden. Die anlassgebundene Datenspeicherung wird indes weiterhin aufrechterhalten und es wird angestrebt, zum Schutz der Freiheitsrechte des Einzelnen die Datenspeicherung durch den Freedom Act einzuschränken.

Mit der Vorratsdatenspeicherung wurde in Deutschland ein System eingeführt, das dem Überwachungsprogramm der NSA in den USA ähnelt. Dabei werden die Metadaten (jedoch nicht die Daten) der Anrufe, Textnachrichten oder E-Mails aller Bürger für zukünftige Strafverfolgungs- und Terrorismusbekämpfungszwecke erhoben und gespeichert. Die beiden Programme wurden von ähnlichen Bestrebungen inspiriert, die nationalen Sicherheitsbehörden mit wirksamen Instrumenten zur Bekämpfung terroristischer Bedrohungen auszustatten, indem digitale Muster von Interaktionen und Verbindungen zwischen Individuen identifiziert werden.[676]

Ein systematischer und funktionaler Vergleich zwischen der anlasslosen vorrätigen Datenspeicherung und der anlassgebundenen Datenspeicherung ist hinsichtlich der Frage bemerkenswert, ob Schutzlücken durch Wegfall der Vorratsdatenspeicherung entstehen würden, worüber sich

676 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 90.

manche sorgen, oder ob die Vorratsdatenspeicherung im Hinblick auf den Datenschutz schwächer wäre als eine anlassgebundene Datenspeicherung.

b) Aktuelle Rechtslage

Da in Deutschland die Erhebung, Speicherung und Verarbeitung personenbezogener Daten nach dem Bundesdatenschutzgesetz grundsätzlich verboten sind, werden sie durch die Ermächtigungsnormen mit den grundrechtlichen Einschränkungen erlaubt. Dagegen ist der Umgang mit den personenbezogenen Daten in den USA grundsätzlich erlaubt, wo man über fast kein einzelnes Datenschutzgesetz verfügt, weshalb dieser Umgang gesetzlich eingeschränkt wird, was auf den Erfahrungen mit der staatlichen Datenspeicherungspraxis beruht.

Hierbei sind das TKG und die StPO die Ermächtigungsnormen zur Vorratsdatenspeicherung. Mit der Einführung der Vorratsdatenspeicherung werden die Verkehrsdaten, auf die die Ermittlungsbehörden zugreifen dürfen, abgesichert und erweitert. Allgemein wird anerkannt, dass die Erhebung, Speicherung und Verwendung personenbezogener Daten eine Einschränkung der Grundrechte zur Folge haben. Zur Rechtfertigung dieses Grundrechtseingriffs soll verfassungsrechtlich der Grundsatz der Verhältnismäßigkeit betont werden. Der Gesetzgeber musste einerseits die praktische Erforderlichkeit anerkennen, aber andererseits die Eingriffsintensität der anlasslosen vorrätigen Datenspeicherung in Betracht ziehen. Er wollte nach den Anforderungen des Bundesverfassungsgerichts mehrere Datenschutzvorkehrungen gesetzlich bereitstellen und die Eingriffsintensität vermindern. Trotz gesetzgeberischer Datenschutzbemühungen werden weiterhin Einwände gegen die Vorratsdatenspeicherung erhoben.

Bei der US-amerikanischen anlassgebundenen Datenspeicherung wurden umgekehrt einige Gesetze erlassen, damit die Datenspeicherung nicht erlaubt wird, sondern die einschränkungslose Datenspeicherung zum Zweck des Datenschutzes verhindert wird. Die Gesetze zielen darauf ab, die Datenerhebung durch die Ermittlungsbehörden zu erleichtern und zugleich ihre Datenerhebung an bestimmte Voraussetzung zum Datenschutz zu binden. In einem solchen System muss der Erfolg der behördlichen Datenerhebung von der Datenspeicherungspraxis der privaten Telekommunikationsunternehmen abhängen. Die USA wenden dennoch ein solches System an, da die Datenerhebung und -speicherung durch den Diensteanbieter der Telekommunikation wegen eines fehlenden einheitlichen Datenschutzgesetzes abgesehen von bestimmten Bereichen in der Regel

fast nicht eingeschränkt werden kann. Das anlassgebundene Datenspeicherungssystem gewinnt hier eine Wirkungskraft durch das CALEA von 1994,[677] das technische Unterstützung für den Diensteanbieter vorschreibt.

aa) Zu speichernde Daten

In Deutschland stützt sich die Vorratsdatenspeicherung auf die vorrätige Speicherung elektronischer Kommunikationsdaten durch private Diensteanbieter. Die Ermittlungsbehörden kontrollieren die Daten nicht direkt, sondern sie können nur den Zugriff auf diese Daten über private Telekommunikationsanbieter nach gesetzlichen Kriterien beantragen. Im Gegensatz hierzu erhob und speicherte in den USA früher die Regierung selbst die Daten über ihr einst geheimes elektronisches Überwachungsprogramm. Bei den Reformdebatten wurde diskutiert, ob die Datenspeicherung tatsächlich von der NSA auf private Unternehmen verlagert werden sollte.[678] US-Präsident *Obama* veranlasste die Übernahme dieser Aufgabe durch die Diensteanbieter der Telekommunikation. Die Gesetzgebung hat auch in diese Richtung gezeigt, um die Probleme zu lösen, die durch die Überwachung durch die NSA aufgeworfen wurden.[679] Die Diensteanbieter der Telekommunikation speichern die Daten, staatliche Behörden dürfen nach dem ECPA auf diese Daten aber nur zugreifen.

In Deutschland, wo eine Erhebung, Speicherung und Verarbeitung personenbezogener Daten nach dem BDSG grundsätzlich verboten sind, handelt es sich beim TKG um die Ermächtigungsnormen, mit denen die Diensteanbieter die darin genannten Daten speichern und verarbeiten können. Im TKG werden folgerichtig die Daten abschließend aufgezählt, die der Diensteanbieter gewerblich und zusätzlich nach der Vorratsdatenspeicherung speichern darf. Die Vorratsdatenspeicherung erfordert die Speicherung bestimmter Verkehrs- und Standortdaten im Fall der Nutzung mobiler Telefondienste bzw. der mobilen Nutzung öffentlich

677 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001–1010.

678 *Londras*, Privatized Counter-Terrorism Surveillance: Constitutionalism Undermined, in: Surveillance, Counter-Terrorism and Comparative Constitutionalism. Abingdon, Oxon: Routledge, Routledge research in terrorism and the law, 2013, 59, 73.

679 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 92–93 m. w. N.

zugänglicher Internetzugangsdienste. Hingegen hängt in den USA der Erfolg eines Zugriffs auf die erforderlichen Daten durch eine staatliche Stelle von der Speicherpraxis privater Telekommunikationsunternehmen ab, weil keine gesetzliche Beschränkung bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch sie Anwendung findet. Bei der Datenspeicherung ist der Diensteanbieter gesetzlich nicht gebunden. Während bei der deutschen Vorratsdatenspeicherung eine Speicherung bestimmter Daten aller Bürger anlasslos und vorrätig erfolgt, wird die Aufbewahrung der Daten in den USA durch den *warrant* oder eine gerichtliche Anordnung auf Grundlage eines *probable cause* oder einer bloßen Erklärung des Zusammenhangs mit der laufenden Untersuchung gesichert. Die Sicherung der Datenaufbewahrung ist konsequenterweise anlassgebunden sowie nachträglich und richtet sich gegen bestimmte Verdächtige.

bb) Zugriff auf Daten

Deutschland erwägt die hohe Eingriffsintensität der anlassunabhängigen Datenspeicherung, indem es die Erhebungsvoraussetzungen für die nach § 113b TKG gespeicherten Daten verschärft. In den USA, die über keine Vorratsdatenspeicherung verfügen, sondern eine verpflichtende Datenspeicherung durch den Diensteanbieter vom vorherigen Ersuchen einer staatlichen Behörde abhängig machen, werden diese Daten eher unter erleichterten Voraussetzungen erhoben.

Für die Erhebung vorrätig anlasslos gespeicherter Daten müssen ein Verdacht eines Verbrechenskatalogs, eine strenge Subsidiarität, die besondere Verhältnismäßigkeit und die gerichtliche Anordnung vorausgesetzt werden. Im Gegensatz hierzu erfordern die USA für die Erhebung von Verkehrsdaten nicht einmal eine Einschränkung auf bestimmte Katalogtaten, eine Subsidiarität oder eine Verhältnismäßigkeit. Die Daten dürfen nicht nur durch einen *warrant* erhoben werden, sondern auch durch eine gerichtliche Anordnung, die auf spezifischen und klaren Tatsachen beruht, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, die angeforderten Daten seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich. Bestimmte Verkehrsdaten können sogar mit einer schriftlichen Anfrage oder einer *subpoena* erhoben werden. Diese Voraussetzungen scheinen auch im Vergleich zur Erhebung der nach § 96 des deutschen Telekommunikationsgesetzes gespeicherten Daten sehr locker zu sein. Mit Blick auf die Grundrechtsbeeinträchtigungsgefahr durch die staatliche Verwendung der Telekommunikationsdaten könnte die lockere

Voraussetzung sehr problematisch sein. Das Problem ist noch größer in den USA, wo es keinerlei solche Bestimmungen gibt, im Gegensatz zu Deutschland, wo das Gesetz die zu speichernden Daten klar vorsieht.

Die nach § 113b TKG gespeicherten Daten dürfen außerdem unter dem Zweckbindungsgrundsatz eingeschränkt verwendet und weitergeleitet werden. Der Verwendungszweck der nach § 113b TKG gespeicherten Verkehrsdaten und die Weitergabe dieser Daten an eine andere Behörde sind also im Gesetz deutlich eingeschränkt, während sich die entsprechenden Einschränkungen im US-amerikanischen Recht nicht finden. In den USA werden die Verkehrsdaten nicht im Voraus gespeichert, aber eine Behörde kann unter erleichterten Voraussetzungen eine Vielzahl von Daten von Telekommunikationsunternehmen ohne Einschränkung erheben, sofern die Behörde dies verlangt.

cc) Löschungspflicht

In Deutschland, wo die Speicherung, Verwendung und Verarbeitung personenbezogener Daten mit einigen Ausnahmen grundsätzlich verboten sind, ist die Löschungspflicht der nach der Vorratsdatenspeicherung gespeicherten Daten vorgesehen. Dabei ist die Speicherdauer unterschiedlich je nach der Eingriffsintensität jener Daten bestimmt, die die zuständige Behörde anfragt. In den USA gibt es hingegen für Telekommunikationsunternehmen keine Löschungspflicht, sondern eine Regelung der Speicherungssicherstellung für einen bestimmten Zeitraum. Dabei kommt die unterschiedliche Bedeutung der Daten beim Grundrechtseingriff nicht in Betracht.

In beiden Ländern wird weder eine Löschung noch ein Übermittlungsverbot nach der Datenverwendung gesetzlich gefordert. Während bei der Datenverwendung die USA keine strikte Zweckbegrenzung vorsehen und die Datenübermittlung bloß an bestimmte und klare Fakten gebunden ist, die eine vernünftige Grundlage für die Annahme darstellen, dass die geforderten Daten im Zusammenhang mit einer laufenden Untersuchung stehen, wird bei der deutschen anlasslosen vorrätigen Datenspeicherung keine Löschungsvorschrift nach der Datenverwendung durch eine enge Zweckbegrenzung des § 113c TKG flankiert. Im Vergleich mit den USA werden in Deutschland verschiedene Maßnahmen – die Löschungspflicht nach einem bestimmten Zeitraum, die unterschiedliche Speicherdauer und die enge Zweckbegrenzung bei der Datenverwendung – ergriffen, damit das Risiko einer Verletzung von Grundrechten aufgrund von Daten-

speicherungspraktiken verringert wird. Bedauerlich ist aber weiterhin der trotz dieser grundrechtsschützenden Bemühungen bestehende Mangel an einer Regelung zur Löschung der bereits an die Behörden übermittelten und für den eigentlichen Zweck verwendeten Daten.

dd) Mitteilungspflicht

Eine Kenntnisnahme über eine Maßnahme ist die notwendige Voraussetzung für den Rechtsschutz des Einzelnen. Dieser kann den Schutz gegen eine unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Verarbeitung seiner personenbezogenen Daten nur beanspruchen, wenn er davon weiß. In diesem Sinn wird in Deutschland die Pflicht der Benachrichtigung an die Beteiligten der betroffenen Telekommunikation gesetzlich sichergestellt – aber es besteht noch die Unterbleibens- oder Zurückstellungsmöglichkeit bei einem überwiegenden öffentlichen Interesse. Dadurch kann der Einzelne seinen Rechtsschutz verwirklichen. Demgegenüber bleibt die US-amerikanische Verkehrsdatenerhebung ein heimlicher Zugriff, weil für die Erhebung von Verkehrsdaten keine Benachrichtigung erforderlich ist. Damit kann der Einzelne von der staatlichen Maßnahme keine Kenntnis nehmen und seinen Rechtsschutz nicht beanspruchen.[680]

680 Das ist in 18 U. S. C.§ 2703 Abs. e ausdrücklich vorgesehen: "No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter."