Teil 2: Landesbericht Deutschland

A. Der verfassungsrechtliche Datenschutz

I. Privatsphären- und Datenschutz

1. Privatsphärenschutz

Sowohl auf nationaler als auch auf internationaler Ebene ist das Recht auf Privatsphäre i. w. S. anerkannt. Das deutsche Grundgesetz benennt allerdings kein spezielles Grundrecht auf den Schutz der Privatsphäre. Im deutschen Rechtsverständnis ist die Privatsphäre als ein nichtöffentlicher Bereich zu verstehen, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt.[93] Die Privatsphäre des Einzelnen wird unter verschiedenen Aspekten und in Bereichen, die als Teile der Privatsphäre anzusehen sind, geschützt. Dem verfassungsrechtlichen Schutz der Privatsphäre dienen im Wesentlichen jene Rechte, die in Art. 2 Abs. 1, Art. 10 und Art. 13 GG niedergelegt sind.

Das Recht auf Unverletzlichkeit der Wohnung aus Art. 13 GG garantiert z. B. den Schutz der Integrität der Wohnung, die eine bedeutende Rolle im Privatsphärenschutz spielt. Dabei wird die Privatheit der Wohnung als „elementarer Lebensraum“[94] geschützt, der der freien Persönlichkeitsentfaltung des Einzelnen dient. In der eigenen Wohnung hat jedermann im Zusammenhang mit dem allgemeinen Persönlichkeitsrecht das Recht, in Ruhe gelassen zu werden, sodass staatliche Organe nicht gegen seinen Willen in den Wohnungsbereich eindringen oder darin verweilen dürfen.[95] Unter „Wohnung“ sind dabei die Räume zu verstehen, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht werden.[96] Ausreichend ist hierfür bereits ein vorübergehender Aufenthalt etwa in Hotel- oder Krankenzimmern, Campingwagen oder Zelten.[97] Unbebaute Flächen

93 BVerfGE 101, 361.
94 BVerfGE 42, 212 (219).
95 So bereits BVerfGE 51, 97 (107); BVerfGE 103, 142 (150 f.).
96 *Jarass*, Grundgesetz, Art. 13 Rn. 4.
97 *Epping*, Grundrechte, S. 342.

fallen dann in den Schutzbereich, wenn sie entweder gegenüber der Öffentlichkeit abgeschirmt sind oder wenn sie sich in unmittelbarer Nähe eines Gebäudes befinden und damit in erkennbarem Zusammenhang mit Wohnzwecken stehen.[98] Umstritten ist hingegen, ob auch Betriebs- und Geschäftsräume unter den Wohnungsbegriff zu subsumieren sind: Während in der Literatur mit Verweis auf den herkömmlichen Sprachgebrauch von „Wohnung" die Meinung verbreitet ist, dass Betriebs- und Geschäftsräume allein dem Schutz des Art. 2 Abs. 1 unterliegen,[99] und dass Betriebs- und Geschäftsräume nur dann als Wohnungen geschützt sind, wenn kein unkontrollierter öffentlicher Zutritt möglich ist,[100] werden solche Räume nach der Rechtsprechung uneingeschränkt von Art. 13 Abs. 1 geschützt.[101] Jedenfalls werden Betriebs- und Geschäftsräume, sei es als Wohnung oder als eine Grundlage der freien Persönlichkeitsentfaltung, als ein wichtiger Teil der Privatsphäre verfassungsrechtlich geschützt.

Der elementare Lebensraum wird zunächst gegen das unbegründete Eindringen oder Verweilen in einem Raum durch staatliche Organe gegen den Willen eines Einzelnen geschützt. Dementsprechend stellen Durchsuchungen von Wohnräumen – sei es zur Ergreifung von Tatverdächtigen (sog. Ergreifungsdurchsuchung) oder zum Auffinden von Beweismitteln (sog. Ermittlungsdurchsuchung) – laut Art. 13 Abs. 1 GG Eingriffe dar und unterliegen damit gemäß Abs. 2 dem Richtervorbehalt. Bei Gefahr im Verzug ist auch eine Anordnung durch die in den Gesetzen vorgesehenen anderen Organe möglich.

Die räumliche Privatsphäre wird auch vor technisch unterstützten Überwachungsmaßnahmen geschützt, selbst wenn diese von einem Bereich außerhalb der Wohnung ohne körperliches Betreten eingesetzt werden.[102] Diesen Schutz hat der technische Fortschritt in der modernen Gesellschaft erforderlich gemacht. Davon werden vor allem technische Mittel zur Überwachung von Wohnungen (sog. großer Lauschangriff)[103] erfasst. Im

98 *Kühne*, Grundgesetz, Art. 13 Rn. 3.

99 *Behr*, Vollstreckung ohne Durchsuchungsanordnung, NJW 1992, 2125, 2126; *Epping*, Grundrechte, S. 342.

100 *Ruthig*, Die Unverletzlichkeit der Wohnung (Art. 13 GG n. F.), JuS 1998, 506, 510.

101 BVerfGE 32, 54 (71 ff.).

102 Vgl. BVerfGE 109, 279 (309).

103 Mit der Einfügung der Abs. 3–6 wurden die verfassungsrechtlichen Grundlagen technischer Überwachungsmittel schon zuvor normierter und praktizierter Maßnahmen gelegt. Die Einfügung unterlag dabei der Kritik, die Grundgesetzänderung sei der Beginn der Einrichtung eines Überwachungsstaates. Zur nor-

Gegensatz zum großen Lauschangriff wird der kleine Lauschangriff eingesetzt, um einen in der Wohnung befindlichen Ermittler bzw. eine Vertrauensperson zu schützen. Durch diese Maßnahme werden Erkenntnisse darüber erlangt, was in der Wohnung geschieht. Diese Erkenntnisse hätte sich der in der Wohnung befindliche verdeckte Ermittler ohnehin angeeignet. Ausreichend ist eine Anordnung durch eine gesetzlich bestimmte Stelle. Es bedarf nur in dem Fall einer richterlichen Überprüfung, wenn die hierbei gewonnenen Informationen zum Zwecke der Strafverfolgung oder der Gefahrenabwehr verwertet werden sollen. Bei einer Gefahr im Verzug besteht eine Nachholmöglichkeit einer richterlichen Entscheidung. Hingegen werden durch den großen Lauschangriff Informationen über die Privatsphäre erlangt, die nicht im Beisein einer für die Polizei tätigen Person offenbart werden. Es werden dabei zweierlei Maßnahmen unterschieden. Einerseits handelt es sich um den repressiven Einsatz technischer Mittel – nur derjenigen, die der akustischen Überwachung dienen – zum Zweck der Strafverfolgung. Der Rechtfertigung repressiver akustischer Überwachung von Wohnungen sind spezielle Schranken gesetzt worden: Sie darf nur dann und nur auf Grund einer richterlichen Anordnung eingesetzt werden, wenn die Erforschung des Sachverhalts auf eine andere Weise unverhältnismäßig erschwert oder aussichtslos ist. Weiterhin ist die Maßnahme zeitlich zu befristen (Art. 13 Abs. 3 GG). Andererseits besteht bei präventiven Maßnahmen keine Beschränkung auf akustische Mittel. Optische Mittel wie Video- und Infrarotaufnahmen oder sonstige Mittel wie Peilsender sind demzufolge auch zulässig. Der kleine Lauschangriff ist also nur zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit zulässig. Um die Qualität der Begründetheit der Maßnahme zu gewinnen, bedarf sie einer richterlichen Anordnung, die bei Gefahr im Verzug auch nachgeholt werden kann.

Die Privatheit der Wohnung kann auch durch sonstige Maßnahmen wie das Betreten, Besichtigen oder Verweilen zu anderen Zwecken als der Durchsuchung beeinträchtigt werden. Die Wohnung als elementarer Lebensraum wird daher gegen Eingriffe und Beschränkungen i. S. d. Art. 13 Abs. 7 GG geschützt. Erforderlich ist dabei nicht das physische Eintreten, sondern der Einsatz technischer Mittel. Denn die Privatheit kann auch durch die Observation von außerhalb der Wohnung beeinträchtigt werden, beispielsweise, wenn der Betroffene sich „auf der Straße“ und

---

mativen Seite *Götz*, Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995, Rn. 520 f.; zur – nur lückenhaft verzeichneten – Praxis zuvor vgl. BT-Drs. 13/4942, S. 37 ff. Vgl. *Hermes*, Grundgesetz, Art. 13 Rn. 50 m. w. N.

damit außerhalb seiner Wohnung und dem hierdurch geschützten Bereich über sein Leben äußert, sodass diese Äußerungen von jedem mitgehört werden können.[104] Der Einsatz technischer Maßnahmen ist hierbei nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere zur Behebung der Raumnot, zur Bekämpfung von Seuchengefahr oder zum Schutze gefährdeter Jugendlicher zulässig.

Mit technischen Mitteln abgehörte und aufgezeichnete Gespräche innerhalb von Wohnräumen unterliegen ebenfalls dem grundrechtlichen Schutz nach Art. 13 Abs. 1 GG. Dieser Schutz erstreckt sich auf den Informations- und Datenverarbeitungsprozess, der sich an die Datenerhebung anschließt.[105] Werden erlangte Sachverhalte gespeichert und weiter genutzt, ist dieser Umgang mit personenbezogenen Daten auch an dem Grundrecht aus Art. 13 GG zu messen.[106]

Besonders kontrovers diskutiert wurde und wird in juristischen Kreisen die Grundrechtsrelevanz der verdeckten Online-Durchsuchung hinsichtlich des Wohnungsgrundrechts aus Art. 13 Abs. 1 GG. Bei Maßnahmen der Online-Durchsuchung handelt es sich um einen heimlichen Zugriff auf informationstechnische Systeme ohne physisches Betreten der Wohnung. Bei diesen liegt nach der Ansicht des Bundesverfassungsgerichts allein ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme vor.[107] Dazu werden weiter unten nähere Ausführungen vorgenommen.

Außerdem wird durch Art. 10 Abs. 1 GG das Brief-, Post- sowie Fernmeldegeheimnis geschützt. Der Artikel dient dem Schutz der Privatsphäre, damit die Kommunikation mit einem ortsabwesenden Partner, die durch die Vermittlung Dritter zustande kommt, vor einer mit dem Kommunikationsweg zusammenhängenden typischen Gefährdungslage geschützt wird, nämlich vor dem möglichen erleichterten Zugriff Dritter auf den Inhalt und die Umstände der Kommunikation.[108] Hierbei wird die freie

104 *Guttenberg*, Die heimliche Überwachung von Wohnungen – Zur verfassungsrechtlichen Problematik des § 9 II, III BVerfSchG und verwandter Vorschriften, NJW 1993, 567, 568 f.; *Jarass*, Grundgesetz, Art. 13 Rn. 8; *Ruthig*, Die Unverletzlichkeit der Wohnung (Art. 13 GG n. F.), JuS 1998, 506, 512.

105 *Tinnefeld*, in: *Tinnefeld/Buchner/Petri/Hof* (Hrsg.), Einführung in das Datenschutzrecht, S. 104.

106 Vgl. BVerfGE 109, 279 (326).

107 BVerfGE 120, 274 (274 ff.).

108 *Epping*, Grundrechte, S. 358.

Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen geschützt.

Das Briefgeheimnis erfasst Sendungen mit individueller schriftlicher Mitteilung sowie die mit der Briefsendung notwendigerweise anfallenden Daten wie Absender- und Empfängeradresse, Überbringer und Einzelheiten der Beförderung.[109] Demgegenüber werden vom Postgeheimnis alle postalisch beförderten Sendungen und die mit der Beförderung zusammenhängenden Daten unabhängig von einer individuellen Mitteilung geschützt.

Das Fernmeldegeheimnis, dem zurzeit eine erhebliche Bedeutung zukommt, schützt die Vertraulichkeit elektronisch vermittelter Kommunikation.[110] Dem grundrechtlichen Schutz unterliegen alle mittels Fernmeldetechnik ausgetauschten Informationen und die Kommunikationsumstände, die darüber Auskunft geben, „ob, wann, wie oft und zwischen welchen Personen oder Fernmeldeanschlüssen Telekommunikation erfolgte oder versucht wurde".[111] Damit fallen neben den Kommunikationsinhalten auch die näheren Umstände einer Kommunikation, nämlich solche Verbindungsdaten wie Ort, Zeit sowie Art und Weise der Kommunikation unter den Schutz des Fernmeldegeheimnisses. Vom Schutzbereich auszuschließen sind Rundfunkübertragungen oder Internetseiten, die an die Allgemeinheit oder an einen unbestimmten Personenkreis gerichtet sind,[112] sowie die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation.[113] Es kommt dabei auf den Herrschaftsbereich des Kommunikationsteilnehmers an. Diese Schutzlücken in Bezug auf den Datenschutz können dank der Ergänzungsfunktion des allgemeinen Persönlichkeitsrechts zum Fernmeldegeheimnis gefüllt werden.

In das Grundrecht aus Art. 10 Abs. 1 GG kann dadurch eingegriffen werden, dass der Staat Kenntnis vom Inhalt der Kommunikation und den mit ihr zusammenhängenden Daten erlangt. Werden einmal durch einen Eingriff in das Grundrecht aus Art. 10 GG Daten erhoben, ist auch die spätere Verwendung dieser Daten an diesem Grundrecht zu messen.[114] Die Grundrechte binden direkt zwar ausschließlich die Gesetzgebung,

109 *Pagenkopf*, Grundgesetz, Art. 10 Rn. 12.
110 *Zippelius/Würtenberger*, Deutsches Staatsrecht, § 28 Rn. 2.
111 BVerfGE 67, 157 (172); BVerfGE 85, 386 (396).
112 *Pagenkopf*, Grundgesetz, Art. 10 Rn. 14a; *Hermes*, Grundgesetz, Art. 10 Rn. 28; *Jarass*, Grundgesetz, Art. 10 Rn. 4.
113 BVerfGE 115, 166 (166).
114 BVerfGE 125, 260 (313).

die vollziehende Gewalt und die Rechtsprechung, jedoch kommen sie indirekt auch für die Regelung der Beteiligung nichtöffentlicher Stellen an Telekommunikationsdiensten zur Geltung, weil § 88 TKG jeden Dienstanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet und darüber hinaus der Staat aufgrund der staatlichen Schutzpflichten dafür Sorge zu tragen hat, dass die privaten Dienstleister die Vertraulichkeit der Kommunikation ebenso gewährleisten wie die staatliche Post.[115] Das Fernmeldegeheimnis schützt demzufolge den einzelnen Bürger nicht nur vor der Kenntnisnahme von Telekommunikationsinhalten durch staatliche Stellen, sondern auch davor, dass öffentliche Stellen die Telekommunikation der Kenntnisnahme Dritter aussetzen. Bei einem derartigen mittelbaren Eingriff in das Fernmeldegeheimnis durch die Veranlassung Dritter zur Kenntnisnahme fremder Telekommunikation in der Übermittlungsphase kann der Schutzanspruch geltend gemacht werden.

Beschränkungen dieses Grundrechts bedürfen gemäß Art. 10 Abs. 2 S. 1 GG einer gesetzlichen Grundlage. Anders als bei der Unverletzlichkeit der Wohnung aus Art. 13 GG enthält dieses Grundrecht keinen Richtervorbehalt. Da Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG zumeist heimlich erfolgen, kann die Gewährleistung effektiven Rechtsschutzes allerdings einen Richtervorbehalt erforderlich machen.[116] In der Regel findet sich ein solcher zwar in den einschränkenden Gesetzen wie z. B. in § 100b StPO, jedoch scheint das auch deshalb noch problematisch zu sein, da der Richtervorbehalt in der Praxis nur eingeschränkt funktioniert: Nach einer Studie von *Backes* und *Gusy*[117] wurde lediglich bei einem Viertel der Anträge auf Telefonüberwachung eine dem Gesetz entsprechende richterliche Prüfung durchgeführt. Nach Art. 10 Abs. 2 S. 2 GG ist es möglich, bei Beschränkungen zum Zweck des Schutzes der freiheitlich demokratischen Grundordnung auf die Mitteilung an den Betroffenen zu verzichten und sie stattdessen durch die Information eines von der Volksvertretung bestimmten Organs bzw. Hilfsorgans zu ersetzen. Daraus kann geschlossen werden, dass die Betroffenen bei Eingriffen in das Grundrecht aus Art. 10 Abs. 1 GG zum effektiven Rechtsschutz zu benachrichtigen sind. Da eine richterliche Überprüfung der Maßnahme demgegenüber ohne eine Mitteilung an den Betroffenen unmöglich gemacht wird, wurden in der Literatur im Hinblick auf die Menschenwürde, das Rechtsstaatsprinzip und

115 BVerfGE 106, 28 (37).
116 BVerfGE 125, 260 (337 ff.).
117 *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung? – Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, 2003, S. 44.

die Gewaltenteilung Bedenken gegen die Verfassungsmäßigkeit des Art. 10 Abs. 2 S. 2 GG angemeldet, denen jedoch das Bundesverfassungsgericht entgegengetreten ist.[118]

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährt außerdem den Schutz eines wesentlichen, unantastbaren Bereichs privater Lebensgestaltung. Es wurde im Rahmen der Zivilrechtsprechung in der „Leserbrief-Entscheidung"[119] des Bundesgerichtshofs erstmals als ein verfassungsmäßig gewährleistetes Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1[120] abgeleitet und der Schutz vor dem Eingriff in die Privatsphäre des Einzelnen wurde als wesentlicher Bestandteil des verfassungsrechtlichen Persönlichkeitsschutzes definiert.[121] In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht für den Einzelnen die Existenz eines räumlich und thematisch bestimmten Bereichs, der grundsätzlich frei von unerwünschter staatlicher Einsichtnahme bleiben soll.[122] Das Bundesverfassungsgericht hebt gegenüber dem „aktiven" Element der freien Entfaltung der Persönlichkeit – der allgemeinen Handlungsfreiheit – das Recht auf Respektierung der Privatsphäre und des sozialen Geltungsanspruchs des Einzelnen hervor.[123] Aufgabe des allgemeinen Persönlichkeitsrechts sei es, „die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen".[124] Das Bundesverfassungsgericht trägt damit den vielfältigen Ausprägungen des allgemeinen Persönlichkeitsrechts im Sinne der Sphärentheorie Rechnung, nach der zwischen der Intimsphäre, der Privatsphäre und der Sozialsphäre zu unterscheiden ist. Diese Differenzierung ist deswegen von Bedeutung, weil sich die Anforderungen, die an eine Eingriffsrechtfertigung zu stellen sind, danach richten, welche Lebenssphäre berührt ist. Beispielsweise darf in die

118 BVerfGE 30, 1 (1 ff.); vgl. *Jarass*, Grundgesetz, Art. 10 Rn. 20.
119 BGHZ 13, 334 (334 ff.).
120 Die Verbindung von Art. 1 Abs. 1 und Art. 2 Abs. 1 bedeutet nicht, dass hier zwei Grundrechte kumulativ zur Anwendung kämen. Aus dieser Verbindung ergibt sich vielmehr eine Verstärkung des Schutzes (*Murswiek/Rixen*, Grundgesetz, Art. 2 Rn. 63).
121 *Degenhart*, Das allgemeine Persönlichkeitsrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, JuS 1992, 362.
122 BVerfGE 120, 274 (311); vgl. auch BVerfGE 27, 344 (350 ff.); BVerfGE 44, 353 (372 f.); BVerfGE 90, 255 (260); BVerfGE 101, 361 (382 f.).
123 BVerfGE 54, 148 (153 f.).
124 BVerfGE 54, 148 (153).

Intimsphäre als einen Bereich der totalen Zurückgezogenheit auf keinen Fall eingegriffen werden. In die Privatsphäre soll hingegen zwar eingegriffen werden können, allerdings nur unter besonders strenger Wahrung des Verhältnismäßigkeitsgrundsatzes, während Eingriffe in die Sozialsphäre unter „normalen" Kriterien als Eingriffe in die Handlungsfreiheit gerechtfertigt werden können.

Der Schutzbereich des allgemeinen Persönlichkeitsrechts ist relativ offen. Damit das allgemeine Persönlichkeitsrecht die Entwicklungsoffenheit gewinnt, wird dessen Schutzbereich von der Rechtsprechung nicht abschließend definiert.[125] Damit können neue, bisher unbenannte Ausprägungen des allgemeinen Persönlichkeitsrechts, die zum gegenwärtigen Zeitpunkt noch nicht ersichtlich sind, geschützt werden. Dadurch kann das allgemeine Persönlichkeitsrecht mit neuartigen Gefährdungen der Persönlichkeitsentfaltung Schritt halten, wie sie insbesondere vom wissenschaftlich-technischen Fortschritt ausgehen.[126] Dies ist vor allem im Bereich des Datenschutzes von Bedeutung. Im Hinblick auf die Entwicklung moderner Kommunikations- und Informationstechnologien sowie mit Blick auf vorhandene EDV-Bedingungen trägt das allgemeine Persönlichkeitsrecht als eine Grundlage der Gewährleistung der allgemeinen Freiheit maßgeblich zu einer umfassenden sowie effektiven Sicherung des Persönlichkeitsschutzes im digitalen Zeitalter bei.

In diesem Zusammenhang sind vom Bundesverfassungsgericht bestimmte Ausprägungen des allgemeinen Persönlichkeitsrechts entwickelt worden: das Recht auf sexuelle Selbstbestimmung, das Recht auf individuelle Selbstbestimmung, das Recht auf wirtschaftliche Selbstbestimmung, das Recht am eigenen Wort, das Recht auf Selbstdarstellung, gar das Recht an der eigenen Wohnung und das Recht an eigenen Daten.[127]

Das allgemeine Persönlichkeitsrecht wird jedoch nicht uneingeschränkt gewährleistet. Es unterliegt der Schrankentrias der Rechte Anderer, der verfassungsmäßigen Ordnung und des Sittengesetzes. Die Schranken des Art. 2 Abs. 1 sind allerdings keine verfassungsunmittelbaren Freiheitseinschränkungen, sondern sie ermächtigen den Gesetzgeber, Freiheitseinschränkungen vorzunehmen. Eingriffe der öffentlichen Gewalt sind daher

125 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 76.

126 *Murswiek/Rixen*, Grundgesetz, Art. 2 Rn. 66.

127 Vgl. *Ehmann*, Zur Struktur des Allgemeinen Persönlichkeitsrechts, JuS 1997, 193, 197.

nur auf Grundlage eines hinreichend bestimmten und verhältnismäßigen Gesetzes zulässig.[128]

2. Die Bedeutung des Datenschutzes für den Privatsphärenschutz

Genau wie das Recht auf den Privatsphärenschutz ist auch *das Recht auf Datenschutz* im Grundgesetz nicht ausdrücklich genannt. Als die öffentliche Verwaltung damit begann, personenbezogene Daten zunehmend automatisiert zu verarbeiten, entstand die Möglichkeit, personenbezogene Daten schnell miteinander zu verknüpfen, zu übermitteln und in neue Sachzusammenhänge zu stellen. Damit einhergehend erhöhte sich die Furcht vor der Möglichkeit der aus den Entwicklungen der Informationstechnik resultierenden Persönlichkeitsgefährdungen und vor einem gänzlich erfassten, „gläsernen" Einzelnen, der unsichtbar und unkontrolliert gesteuert werden kann. Das Bundesverfassungsgericht hat infolgedessen mit seinem Volkszählungsurteil[129] vom 15. Dezember 1983 das Recht auf informationelle Selbstbestimmung[130] als einem weiteren spezifischen Aspekt der Privatsphäre und elementaren Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 abgeleitet.[131] Damit hat das Bundesverfassungsgericht nicht nur das allgemeine Persönlichkeitsrecht präzisiert, sondern aus diesem *ein Grundrecht auf Datenschutz* herausgearbeitet.

Wie bereits dargelegt, lässt sich im Grundgesetz zwar kein ausdrückliches Grundrecht auf Privatsphäre finden, jedoch werden mehrere Aspekte der Privatsphäre verfassungsrechtlich gewährleistet, um die Privatsphäre als Grundbedingung der freien Entfaltung der Persönlichkeit zu schützen. Dabei spielen Art. 13 und Art. 10 GG eine bedeutende Rolle. Während

128 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 75.

129 Im Volkszählungsurteil geht es um die Verfassungskonformität der im VoZählG im Jahre 1983 vorgesehenen Datenerhebungsregelungen für statistische Zwecke und Übermittlungsregelungen.

130 Der Ausdruck „das Recht auf informationelle Selbstbestimmung" wurde erstmals im Jahre 1971 von Steinmüller genutzt, wobei er das Recht auf informationelle Selbstbestimmung in dem Sinne erfasste, dass der Einzelne selbst darüber bestimmt, unter welchen Umständen er welche personenbezogenen Daten an wen übermittelt (*Steinmüller*, Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag – 6. Wahlperiode – BT-Drs. 6/3826 Anlage I, 1971.

131 BVerfGE 65, 1 (41 ff.).

Art. 13 die Unverletzlichkeit der Wohnung als einen räumlichen elementaren Lebensraum schützt, dient Art. 10 dem Schutz eines privaten, vor der Öffentlichkeit verborgenen Austausches von Informationen. Außerdem kann das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 GG die Füllmasse der durch die beiden Grundrechte entstandenen Schutzlücken bieten. Daraus leitet das Bundesverfassungsgericht die konkreten Ausprägungen um des Schutzes der Privatsphäre willen ab und bewältigt zugleich mit der Sphärentheorie das Problem von Eingriffen in das allgemeine Persönlichkeitsrecht. Es entsteht demnach die Intimsphäre, die vollständig vor staatlichen Eingriffen geschützt wird und in die ein Eingriff daher in keinem Fall gerechtfertigt werden kann. In die Privatsphäre und die Sozialsphäre darf hingegen eingegriffen werden, allerdings nur unter verschiedenen Voraussetzungen zur Rechtfertigung, abhängig davon, welche Lebenssphäre berührt wird. Für einen Eingriff in die Privatsphäre wird eine strengere Wahrung des Verhältnismäßigkeitsgrundsatzes als für den Eingriff in die Sozialsphäre gefordert.

Im Hinblick auf den Datenschutz hat das Bundesverfassungsgericht zwei Grundrechte aus dem allgemeinen Persönlichkeitsrecht entwickelt: das Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Unter den modernen Bedingungen der Datenverarbeitung kommt dem Recht auf informationelle Selbstbestimmung eine erhebliche Bedeutung zu. Es schützt den Einzelnen vor einzelnen, punktuellen Datenerhebungen mit personenbezogenem Inhalt und den sich der Datengewinnung anschließenden Interpretationsmöglichkeiten.[132] Demgegenüber wird bezweifelt, ob das IT-Grundrecht, welches das Bundesverfassungsgericht mit Bezug auf Online-Durchsuchungen neu geschaffen hat, erforderlich ist bzw. ob es überhaupt dem effektiveren Schutz der Privatsphäre dient.

3. Der verfassungsrechtliche Datenschutz

Die personenbezogenen Daten, denen beim Privatsphärenschutz eine große Bedeutung zukommt, werden auch verfassungsrechtlich geschützt. Für

132 Ausführlich zu dem Recht auf Datenschutz, *Poscher*, The Right to Data Protection – A No-Right Thesis, in: *Miller*, Privacy and Power – a Transatlantic Dialogue in the Shadow of the NSA-Affair, S. 129–142, Cambridge University Press, 2017.

deren Schutz hat das Bundesverfassungsgericht ein besonderes Grundrecht aus dem allgemeinen Persönlichkeitsrecht abgeleitet: das Recht auf informationelle Selbstbestimmung. Das Grundrecht dient dem Privatsphären- und insbesondere dem Datenschutz.

Das Recht auf informationelle Selbstbestimmung gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[133] Personenbezogene Daten sind gemäß § 27 Abs. 3 BDSG angelehnt an „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person".[134] Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus, da es den Schutz bereits auf der Stufe der Persönlichkeitsgefährdung in Kraft treten lässt.[135] Es schützt also vor einzelnen, punktuellen Datenerhebungen mit personenbezogenem Inhalt und den sich der Datengewinnung anschließenden Interpretationsmöglichkeiten.[136]

Unter den Bedingungen der modernen Datenverarbeitung setzt die freie Entfaltung der Persönlichkeit voraus, dass der Einzelne vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten geschützt wird.[137] Es ist für den einzelnen Bürger jedoch schwierig, Kenntnis davon zu haben, welche Daten gesammelt werden, wo sie erhoben werden, ob sie gespeichert werden und was mit diesen Daten geschieht. Menschen, die denken, dass ihre Daten systematisch identifiziert und überwacht werden, verzichten wahrscheinlich darauf, ihre Rechte auszuüben und sich der Öffentlichkeit zu stellen, weil sie fürchten, dass sie durch diese Aktivitäten benachteiligt werden. In diesem Zusammenhang hat das Bundesverfassungsgericht mit seinem Volkszählungsurteil vom 15. Dezember 1983 die Notwendigkeit eines besonderen Maßes an Schutz des Rechts auf informationelle Selbstbestimmung unter den damaligen, heutigen und künftigen Bedingungen der automatischen Datenverarbeitung anerkannt. Denn die personenbezogenen Daten seien laut Bundesverfassungsgericht heute mit Hilfe der automatischen Datenverarbeitung technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Das Bundesverfassungsgericht befürchtet außerdem, dass personenbezogene Daten oh-

133 BVerfGE 120, 274 (312); BVerfGE 65, 1 (43).
134 BVerfGE 65, 1 (42).
135 BVerfGE 120, 274 (311 f.).
136 *Kingreen/Poscher*, Grundrechte Staatsrecht II, S. 120 f.
137 BVerfGE 65, 1.

ne die zureichende Kontrollmöglichkeit des Betroffenen im Hinblick auf Richtigkeit und Verwendung seiner Daten mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden.[138] Das Bundesverfassungsgericht spricht hier von einer gewaltigen Bedrohung für die Ausübung der Freiheitsrechte.

Mit der Ableitung dieses Rechts aus dem allgemeinen Persönlichkeitsrecht zielt das Bundesverfassungsgericht darauf ab, den neuen Gefährdungen durch die automatisierte Datenverarbeitung wirksam entgegenzutreten. Nach der Rechtsprechung wird in das Recht nur unter den folgenden Voraussetzungen eingegriffen:

1. Ein Eingriff in das Recht bedarf einer verfassungsgemäßen gesetzlichen Grundlage;
2. Die gesetzliche Grundlage muss so normenklar bestimmt werden, dass der Einzelne die Voraussetzungen und den Umfang des Eingriffs klar erkennen kann (Normenklarheitsgebot);
3. Die Eingriffsnorm muss dem Verhältnismäßigkeitsgrundsatz entsprechen;
4. Der Verwendungszweck muss im Voraus festgelegt werden und hinreichend bestimmt sein (Zweckbindungsgrundsatz);
5. Es bedarf organisatorischer und verfahrensrechtlicher Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung. Zu diesen Vorkehrungen zählen die Transparenz der Datenvorgänge durch Aufklärung des Betroffenen, eine dem Betroffenen zur Verfügung gestellte Auskunft und Sperrung bzw. Löschung seiner Daten zum gegebenen Zeitpunkt sowie die Einrichtung und Beteiligung von Datenschutzinstanzen, die rechtlich unabhängig und faktisch dazu befähigt sind, über die Rechte der Bürger zu wachen.

Die Bedeutung dieses Urteils besteht darin, dass damit einheitliche Grundsätze als Prüfungsmaßstab für jeden Eingriff in personenbezogene Daten, unabhängig von ihrer Sensibilität,[139]geschaffen wurden. Denn es gibt unter modernen Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr.[140]

---

138 BVerfGE 65, 1 (42).

139 BVerfGE 65, 1 (44 f.): Nach der Rechtsprechung gebe es unter den Bedingungen der automatisierten Datenverarbeitung wegen der der Informationstechnologie inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten „kein belangloses Datum“ mehr.

140 BVerfGE 65, 1 (45).

Dennoch kommt das Recht auf informationelle Selbstbestimmung als Konkretisierung des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht zur Anwendung, wenn speziellere Grundrechte betroffen sind. Speziellere Grundrechte verdrängen also in ihrem Anwendungsbereich das Recht auf informationelle Selbstbestimmung bzw. das allgemeine Persönlichkeitsrecht. Sofern laufende Kommunikationsvorgänge betroffen sind, wird Art. 10 Abs. 1 GG angewendet. In das Recht auf informationelle Selbstbestimmung darf erst dann eingegriffen werden, wenn die Telekommunikation abgeschlossen und die Daten endgültig auf einem Speichersystem gespeichert sind.[141]

Das Bundesverfassungsgericht hat mit seinem Online-Durchsuchungsurteil vom 27. Februar 2008 neben dem Recht auf informationelle Selbstbestimmung auch ein verfassungsrechtlich neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt.[142] Das Grundrecht ist subsidiär zu dem Recht auf informationelle Selbstbestimmung.[143] Bei der Online-Durchsuchung greifen staatliche Organe ohne Beschlagnahmung des Geräts auf die Daten eines Computers zu. Stattdessen erfolgt der Zugriff dadurch, dass unbemerkt eine staatliche Überwachungssoftware auf dem Computer installiert wird. Anders als beim informationellen Selbstbestimmungsrecht, dessen Schutzgegenstand die Entscheidungsfreiheit des Einzelnen über seine persönlichen Daten ist, werden bei diesem Grundrecht die informationstechnischen Systeme selbst geschützt.

Das neue „IT-Grundrecht", das das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 erstmals als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme explizit benannte,[144] begründet sich darin, dass die Gewährleistung der Grundrechte aus Art. 10 und Art. 13 GG sowie die vom Bundesverfassungsgericht bisher entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts dem Bedürfnis des Schutzes vor den Persönlichkeitsgefährdungen, die sich

141 BVerfGE 110, 33 (53); *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 251.

142 BVerfGE 120, 274.

143 Das „neue" Grundrecht begrüßend: *Hömig*, „Neues" Grundrecht, neue Fragen?, Zum Urteil des BVerfG zur Online-Durchsuchung, Jura 2009, 207, 213; siehe auch sehr kritisch zur Erforderlichkeit der eigenständigen Existenz des Grundrechts: *Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521, 521 ff.

144 BVerfGE 120, 274 (302).

aus der Entwicklung der Informationstechnik ergeben, nicht hinreichend Rechnung tragen.[145] Das Grundrecht schließt die Lücke im Grundrechtsschutz, die für eine solche Infiltration des gesamten informationstechnischen Systems besteht, das außerhalb einer Wohnung steht, und für solche Daten, die nach Abschluss eines Kommunikationsprozesses nicht mehr von Art. 10 Abs. 1 GG gedeckt sind und mangels einzelner punktueller Datenerhebung auch nicht oder nicht ausreichend dem Recht auf informationelle Selbstbestimmung unterliegen.[146,147]

Nach der Entscheidung des Bundesverfassungsgerichts ist der Schutzbereich von Art. 13 Abs. 1 GG im Falle von Online-Durchsuchungen nicht betroffen. Dafür sprechen einige Argumente: Online-Durchsuchungen würden die räumliche Sphäre der Wohnung als geschütztem Rückzugsraum nicht beeinträchtigen, weil sie sich rechtlich und tatsächlich ausschließlich auf eine dem Betroffenen gehörende Sache beschränken.[148] Ein raumbezogener Schutz sei nicht in der Lage, die spezifische Gefährdung des informationstechnischen Systems abzuwehren.[149] Da informationstechnische Systeme oft mobil sind und daher sowohl innerhalb als auch außerhalb einer Wohnung im Sinne von Art. 13 GG betrieben werden können, halten einige Autoren das Wohnungsgrundrecht für nicht anwendbar.[150] Die Betroffenheit des Schutzbereichs wird also verneint, weil der Staat bei einer Online-Durchsuchung lediglich Einsicht in einen

145 BVerfGE 120, 274 (306).

146 *Horn*, Grundrechte, Art. 2 Rn. 51.

147 Vgl. *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009, 1016. Erst die sich an die Infiltration anschließende Datenauswertung fällt wieder unter das Recht auf informationelle Selbstbestimmung.

148 BGH, Ermittlungsrichter, StV 2007, 60 (62); *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250; *Hoffmann*, Die Online-Durchsuchung: staatliches Hacken oder zulässige Ermittlungsmaßnahme?, NStZ 2005, 121, 124.

149 BVerfGE 120, 274 (310); zustimmend *Bär*, Anmerkung zum Urteil des BVerfG: Verfassungsmäßigkeit der Online-Durchsuchung und anderer verdeckter Ermittlungsmaßnahmen in Datennetzen, MMR 2008, 325, 325.

150 *Böckenförde*, Grundrechtstheorie und Grundrechtsinterpretation, in: *ders.*, Staat, Gesellschaft, Freiheit. Studien zur Staatstheorie und zum Verfassungsrecht, S. 223 f.; *Lepsius*, Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *Roggan* (Hrsg.), Online-Durchsuchung – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 2008, 21, 25: Es mute merkwürdig an, wenn der Grundrechtsschutz davon abhinge, ob der Nutzer informationstechnischer Systeme auf diese innerhalb oder außerhalb der Wohnung zugreife.

begrenzten Teil der Wohnung habe und somit dem Betroffenen noch Raum bleibe, den er als privaten Rückzugsort nutzen könne.[151] Schließlich wird die Schutzbereichseröffnung mit dem Hinweis darauf verneint, dass Online-Durchsuchungen ohne die Überwindung physischer Barrieren vorgenommen werden können.[152] Da das Fernmeldegeheimnis nicht auf den Schutz von Daten abzielt, die sich nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers befinden,[153] ist Art. 10 GG nicht einschlägig. Schlussendlich sieht das Bundesverfassungsgericht auch das Recht auf informationelle Selbstbestimmung nicht als einschlägig an, da es dabei nicht um die Erhebung einzelner Daten gehe, sondern um einen Datenbestand, der Einblicke in wesentliche Teile der Lebensgestaltung ermögliche.[154]

Jedoch ist die Argumentation, nach der Online-Durchsuchungen keine Beeinträchtigung der räumlichen Sphäre, sondern nur eine begrenzte Einsicht in die Wohnung darstellen würden, nicht überzeugend. Das Wohnungsgrundrecht gewährt grundsätzlich einen Ort, an dem sich jeder Einzelne ohne staatliche Einsichtnahmen frei entfalten kann. Geschützt werden konsequenterweise alle Vorgänge und auch alle Gegenstände, soweit sie innerhalb der Wohnung geschehen bzw. sich darin befinden. Die Unmöglichkeit der umfassenden Schutzgewährleistung des Wohnungsgrundrechts läuft auch nicht notwendigerweise darauf hinaus, dass die Nutzung informationstechnischer Systeme niemals in den Schutzbereich des Wohnungsgrundrechts fallen würde. Auch ein wechselnder Standort verhindert nicht die Schutzbereichseröffnung. Gerade der Umstand, dass ein und dieselbe Handlung je nach ihrem Standort vom Wohnungsgrundrecht geschützt ist oder nicht, ist das Wesensmerkmal eines raumbezogenen Schutzes.[155] Wie bei der Ablehnung der Schutzbereichseröffnung des Art. 13 GG ist auch die Begründung der Anerkennung von Schutzlücken des Rechts auf informationelle Selbstbestimmung nicht überzeugend. Denn

151 So *Schlegel*, Warum die Festplatte keine Wohnung ist – Art 13 GG und die „Online-Durchsuchung", GA 2007, 648, 659; ähnlich wohl auch *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250.

152 *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250: Nach seiner Meinung sei die Situation vergleichbar mit dem Blick eines Ermittlungsbeamten durch ein Fenster. Niemand würde dies als eine Wohnraumüberwachung qualifizieren.

153 BVerfGE 120, 274 (307 f.).

154 BVerfGE 120, 274 (312 f.).

155 *Schneider*, Rechtliche Rahmenbedingungen für die Vornahme von Online-Durchsuchungen, S. 54.

das Recht auf informationelle Selbstbestimmung ist auf keinen Fall auf die Erhebung eines einzelnen Datums beschränkt.[156] Nicht ersichtlich ist, aus welchem Grund man einen Unterschied zwischen der Behandlung einer einzelnen Datenabfrage und der Erhebung ganzer Datenbestände verbunden mit der Potenzierung der Gefährdung der Persönlichkeitsrechte machen sollte. In diesem Zusammenhang wird bezweifelt, ob neben der Unverletzlichkeit der Wohnung und dem Recht auf informationelle Selbstbestimmung die weitere Schaffung des *neuen* Grundrechts um des besonderen Schutzes der Freiheit der Bürger willen effektiver oder sogar überhaupt erforderlich ist. Denn den gesteigerten Gefahren für das Persönlichkeitsrecht des Einzelnen infolge der technischen Entwicklung könnte mit dem strengeren Verhältnismäßigkeitsgrundsatz begegnet werden: An den verfolgten Zweck sind umso höhere Anforderungen zu stellen, je stärker in den Bereich privater Lebensgestaltung eingegriffen wird. Darüber hinaus könnten diese neuen Herausforderungen auch nur mit dem Schutz des absolut geschützten Kernbereichs, den konkreten Gefährdungsdelikten vor der Rechtsgutsverletzung, der Beachtung der Normklarheit sowie -bestimmtheit und den verfahrensrechtlichen Voraussetzungen überwunden werden.

Das Bundesverfassungsgericht hat insoweit besondere Anforderungen an die Rechtfertigung von Eingriffen mit hoher Intensität gestellt, nämlich gesteigerte Anforderungen an die mit dem Eingriff verfolgten Ziele sowie an die Sicherstellung verfahrensrechtlicher Vorkehrungen. Weiterhin ist der Betroffene auch nachträglich über die Möglichkeit des Rechtsschutzes zu benachrichtigen.[157]

II. Übersicht des einfachgesetzlichen Datenschutzsystems

Im Jahr 1977 erließ die Bundesrepublik Deutschland die erste Fassung des Bundesdatenschutzgesetzes (BDSG). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 war klar, dass das bisherige Datenschutzgesetz den verfassungsrechtlichen Anforderungen nicht genügte. Das Gesetz musste also einige Novellierungen erfahren. Entsprechend den im Volkszählungsurteil des Bundesverfassungsgerichts genannten Anforderungen wurde das BDSG vor allem im Jahre 1990 novelliert.

156 *Epping*, Grundrechte, S. 328.
157 BVerfGE 120, 274 (323 ff.).

Das BDSG regelt die Datenerhebung, -verarbeitung und -nutzung. Ein Erheben im Sinne des Gesetzes liegt bei der bloßen Beschaffung von Daten über natürliche Personen beim Betroffenen oder bei Dritten vor. Zur Verarbeitung gehören das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Unter einer Nutzung ist jede Verwendung personenbezogener Daten zu verstehen, soweit es sich nicht um die Verarbeitung handelt. Im BDSG wird zwar zwischen dem Datenschutz in öffentlichen und nichtöffentlichen Stellen unterschieden, es regelt jedoch den Datenschutz in beiden Bereichen.

Wird das deutsche Datenschutzrechtssystem übersichtlich vorgestellt, können zwei Besonderheiten festgestellt werden. Die erste betrifft den Datenschutzansatz. Das deutsche Datenschutzrecht folgt einem umfassenden Ansatz. Es gibt ein umfassendes Datenschutzgesetz (BDSG), in dem alle Datenverarbeitungsvorgänge im öffentlichen und privaten Sektor reguliert werden. Zweitens ist im BDSG das Verarbeiten personenbezogener Daten nur auf Basis eines Erlaubnistatbestandes zulässig. Ein Ausgangspunkt ist das Verbot einer Verarbeitung.

B. Datenschutz bei den konkreten Maßnahmen

Das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht im Volkszählungsurteil aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet hat, schützt die Bürger gegen eine unbegrenzte Erhebung und Verwendung ihrer persönlichen Daten. Einschränkungen dieses Rechts bedürfen einer gesetzlichen Grundlage, die vor der verfassungsmäßigen Ordnung Bestand haben und insbesondere dem Grundsatz der Verhältnismäßigkeit genügen muss.[158] Eine Erhebung und Verwendung persönlicher Daten auf Grundlage der einfachgesetzlichen Ermächtigung stellt insoweit eine von der Verfassung gebotene Einschränkung des Grundrechts auf informationelle Selbstbestimmung dar und soll in der Prüfung der Verhältnismäßigkeit als sog. Schranken-Schranke bestehen. Wegen seiner erheblichen Bedeutung im Hinblick auf die starke Betroffenheit der privaten Lebensgestaltung wird aus dem Grundrecht ferner der Grundsatz der Zweckbindung personenbezogener Daten gefolgert. Die Forderung der strikten Zweckbindung ist angesichts der mit der heutigen

158 BVerfGE 65, 1 (41 ff.); BVerfGE 78, 77 (84 ff.); BVerfGE 80, 367 (373); BVerfGE 115 (320 ff.); BVerfGE 124, 78 (78 ff.); BVerfGE 125, 260 (260 ff.).

elektronischen Datenverarbeitung verbundenen Gefahren selbstverständlich.

Auf der Grundlage dieser Erkenntnisse soll im Folgenden untersucht werden, ob die Verwertung persönlicher Daten in den oben ausgewählten Bereichen – also dem Strafregister, der Rasterfahndung und der Vorratsdatenspeicherung – den verfassungsrechtlichen Anforderung genügt und ob dabei die verfassungsrechtlich gebotenen Schutzvorkehrungen gegen einen unbefugten oder übermäßigen Zugriff auf die Daten hinreichend vorbereitet sind.

I. Strafregister

Gerichte, Staatsanwaltschaften und andere Justizbehörden sind gemäß § 474 StPO und § 41 BZRG dazu berechtigt, personenbezogene Daten aus dem Strafregister für Zwecke der Rechtspflege zu verwenden. Für die Erhebung und Verwendung personenbezogener Daten aus dem Strafregister im Strafverfahren bieten also §§ 474 bis 495 StPO die gesetzliche Ermächtigungsgrundlage. Die Verwendungszwecke beschränken sich auf die dort genannten Zwecke. Während § 161 Abs. 1 Satz 1 und 2 sowie § 163 Abs. 1 Satz 2 die Erhebung von Auskünften innerhalb desselben Verfahrens regeln, normieren §§ 474 Abs. 1, 478 Abs. 1 Satz 5 die Weitergabe von bereits in anderen, vorangegangenen Verfahren ermittelten Erkenntnissen für Zwecke der Rechtspflege.[159]

Die Speicherung strafrechtlich relevanter Daten spielt im Strafverfahren eine große Rolle. Daher wurden schon seit langem die zahlreichen Strafregister der Staatsanwaltschaften bei den Landgerichten und das Bundesstrafregister zur Verfügung gestellt,[160] das seit 1954 durch den Generalbundesanwalt beim BGH geführt wurde. Im Jahr 1972 wurden beide mit dem Bundeszentralregister in ein einheitliches, zentrales Register der Justiz integriert, das noch immer durch den Generalbundesanwalt beim BGH – Dienststelle Bundeszentralregister – in Berlin geführt wird.[161] Außerdem kann, wenn von Strafregistrierung gesprochen wird, nicht über das Straf-

159 *Schmitt*, Strafprozessordnung, § 474, Rn. 2; *Gieg*, KK-StPO, § 474 Rn. 1.

160 Vgl. Allg. Verwaltungsvorschriften des BMJ vom 27. Januar und vom 6. Juli 1954 (BAnz Nr. 21 und 129).

161 Dies geschah durch das am 1. Januar 1972 in Kraft getretene Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG) vom 18. März 1971.

verfahrensregister gemäß §§ 492 ff. StPO hinweggesehen werden. Die gesetzliche Grundlage für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister wurde durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994[162] erstmals in die StPO eingefügt und durch das Strafverfahrensänderungsgesetz 1999 vom 11. August 2000[163] geändert und erweitert. Dem Strafverfahrensregister kommt auch deshalb eine Bedeutung zu, weil die möglichen Gefahren im Hinblick auf die Frage des Datenschutzes bei einer Strafregistrierung als nicht gering einzuschätzen sind.

Um Aussagen darüber treffen zu können, wie die persönlichen Daten beim Strafregister geschützt werden, wird zunächst analysiert, wie die Strafregistrierung organisiert ist, was wie lange und wozu erhoben und gespeichert wird und welche Vorkehrungen zum Datenschutz getroffen werden (was also passieren kann, wenn die personenbezogenen Daten auch nach Ablauf eines bestimmten Zeitraums nicht gelöscht werden). Deshalb soll im Folgenden zunächst ein Überblick über das Strafregistersystem gegeben und dann auf die genannten Fragen eingegangen werden. Damit können die gegen die mit der automatisierten Datenverarbeitung verbundenen Gefahren vorgesehenen Schutzmaßnahmen unter dem Aspekt Datenschutz analysiert werden.

1. Organisationsstruktur

Die personenbezogenen Daten, die im Strafverfahren verwertet werden dürfen, können hauptsächlich aus dem Bundeszentralregister (BZR) und dem zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV) erhalten werden. Während es sich beim BZR grundsätzlich um gerichtliche Verurteilungen handelt, betrifft das ZStV das Ermittlungs- und Strafverfahren der Staatsanwaltschaft. Dieser Regelungsbereich gehört also zum unmittelbaren Vorfeld des gerichtlichen Verfahrens. Angesichts der Besonderheiten des Jugendstrafrechts und der darin normierten vorwiegend auf erzieherische Wirkungen abstellenden Maßnahmen ist in das BZR ein gesondertes Erziehungsregister (§§ 55 ff. BZRG) integriert, in dem derartige Entscheidungen gegen Jugendliche gesondert registriert werden.

---

162 Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28. Oktober 1994, BGBl. I 1994, S. 3186.

163 Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1999 (StVÄG 1999), BGBl. I 2000, S. 1253.

Im Folgenden soll die Organisationsstruktur dieser beiden Formen der Strafregistrierung untersucht werden. Dabei kann festgestellt werden, in welcher Form das Mitteilungs- und das Speicherungsverfahren von Daten im deutschen Strafregistersystem verlaufen.

a) Das Bundeszentralregister

Das BZR wurde mit gleichzeitiger Umstellung der Registerführung auf die elektronische Datenverarbeitung eingerichtet. Es setzte erhebliche organisatorische und technische Anstrengungen voraus, etwa die Übernahme der Altbestände und die zentrale Erfassung der aktuellen Entscheidungen bei gleichzeitiger Aufrechterhaltung des Auskunftsbetriebes.

Die Organisationsstruktur des BZR wird zuerst grob vorgestellt. Die mitteilungspflichtigen Stellen der Registerbehörde sollen die nach dem BZRG einzutragenden Entscheidungen übermitteln. Die Registerbehörde soll sie dann speichern und damit auf das Auskunftsersuchen antworten. Nach § 1 Abs. 1 BZRGVwV erfolgen die Mitteilungen an das Zentralregister durch die Vollstreckungsbehörde, die Verwaltungsbehörde, das Gericht und die Strafverfolgungsbehörde. Die mitteilungspflichtigen Stellen sollen die Formularmitteilungen mit speziellen Schreibmaschinen nach vorgegebenen Regeln ausfüllen und der Registerbehörde im Wege der Datenfernübertragung übermitteln. Die Mitteilungen sollen bei Entscheidungen binnen eines Monats nach Eintritt der Vollziehbarkeit, Unanfechtbarkeit oder Rechtskraft, bei rechtskräftigen strafgerichtlichen Verurteilungen (§ 3 Nr. 1 BZRG) binnen eines Monats nach Ablauf der gemäß § 275 Abs. 1 Satz 2 der Strafprozessordnung bestimmten Frist, bei Entscheidungen ohne solche Rechtswirkungen binnen eines Monats nach ihrem Erlass und bei anderen Tatsachen binnen eines Monats nach ihrem Eintritt übermittelt werden.[164] Die Formularmitteilungen werden dann beim BZR von einer Maschine eingelesen, die die maschinenschriftlichen Einträge optisch erkennt und in eine der Datenverarbeitungsanlage verständliche Sprache umsetzt. Die Mitteilungen werden, sobald sie vom Seitenleser-System gelesen und in einen Magnetbandsatz umgewandelt wurden, nach zahlreichen Plausibilitätsprüfungen programmgesteuert in das EDV-geführte Register eingegliedert. Bei der Einordnung von Neueintragungen wird eine Identitätsfeststellung durchgeführt.

164 § 3 BZRGVwV.

Auch die Anfragen (Ersuchen um Erteilung von Führungszeugnissen, unbeschränkte Auskünfte aus dem Zentralregister und Auskünfte aus dem Erziehungsregister von Gerichten und Behörden, Anträge von Privatpersonen auf Erteilung von Führungszeugnissen) sollen der Registerbehörde im Wege der Datenübertragung übermittelt werden (§ 4 I 1. Satz BZRGVwV). Die Beantwortung von Auskunftsersuchen, also die Auskunftserteilung aus dem BZR, erfolgt im Wege der Erteilung von Führungszeugnissen (§§ 30 bis 32 BZRG) und unbeschränkten Auskünften (§§ 41 und 42 BZRG). Um die personenbezogenen Daten im System zu schützen, erfordert das BZRG für die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, bestimmte Umstände, nämlich dass diese Übermittlungsform unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen angemessen ist und dass gewährleistet ist, dass die Daten bei der Übermittlung wirksam gegen einen unbefugten Zugriff Dritter geschützt sind.[165] Bei der Datenfernübertragung sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und -sicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden. Die Registerbehörde lässt eine schriftliche Übermittlung durch Gerichte auf Vordrucken zu, soweit sie hierfür keine webbasierte Datenübertragungslösung bereitstellt. Im Übrigen kann die Registerbehörde eine schriftliche Übermittlung auf Vordrucken zulassen (§ 4 I Satz 2 bis 4 BZRGVwV).

Die beiden Auskunftserteilungsmöglichkeiten sind allerdings mit jeweils anderen Voraussetzungen und Einschränkungen verbunden. Beim Führungszeugnis ist je nach Verwendungszweck zwischen einem Privatführungszeugnis (§ 30 Abs. 1 BZRG) und einem Behördenführungszeugnis (§ 30 Abs. 5, § 31 BZRG) mit unterschiedlichen Inhalten zu differenzieren. Den inhaltlichen Unterschied gibt es ebenso bei der unbeschränkten Auskunft, ebenfalls je nach Empfängerkreis. In § 41 Abs. 3 BZRG ist vorgeschrieben, dass nur noch den Strafgerichten und den Staatsanwaltschaften für ein Strafverfahren gegen den Betroffenen Auskunft erteilt werden darf. Der Inhalt des Registers und die Verwertung der Auskünfte aus dem Register werden unten eingehender diskutiert.

165 § 21 Satz 1 BZRG.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Wie erwähnt, können die Daten, die im Strafverfahren verwertet werden dürfen, nicht nur aus dem BZR, sondern auch aus dem ZStV hergenommen werden. Letzteres kann allerdings nicht als das Strafregister im eigentlichen Sinne bezeichnet werden. Das in den §§ 492 bis 495 StPO geregelte länderübergreifende staatsanwaltschaftliche Verfahrensregister, dessen Einrichtung durch Art. 4 Nr. 1 des Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze – Verbrechensbekämpfungsgesetz – vom 28. Oktober 1994[166] in die Strafprozessordnung eingefügt wurde, wird vom Bundesamt für Justiz (BfJ)[167] als zentraler Dienstleistungsbehörde der Bundesjustiz mit Sitz in Bonn geführt.

Anders als das BZR soll das ZStV nach der Entwurfsbegründung dazu dienen, mit umfassenden und schnell verfügbaren Informationen über die bundesweit gegen einen Beschuldigten geführten Ermittlungs- und Strafverfahren der Staatsanwaltschaft die sachgerechte Führung eines Ermittlungsverfahrens zu erleichtern.[168] Damit will der Gesetzgeber insbesondere im Interesse der Allgemeinheit und der von den Strafverfolgungsmaßnahmen Betroffenen die Effektivität der Strafrechtspflege erhöhen.[169] Die Einrichtung des ZStV beruht also auf der Überlegung, dass zur Gewährleistung der Funktionstüchtigkeit der Strafrechtspflege auch die Verbesserung der Information der Staatsanwaltschaften gehört, damit Entscheidungen auf der Grundlage umfassender Erkenntnisse aus allen Ermittlungs- und Strafverfahren getroffen werden können. Dieser Regelungsbereich gehört zum unmittelbaren Vorfeld des gerichtlichen Verfahrens. Das heißt: Trifft ein Gericht eine im BZR einzutragende Entscheidung – sobald die Entscheidung also rechtskräftig geworden ist –, so erhält die Registerbehörde des BZR eine Mitteilung nach § 20 BZRG. Wird eine solche Entscheidung in das BZR eingetragen, so wird die entsprechende Eintragung im ZStV automatisch gelöscht.[170]

166 BGBl. I, S. 3186.

167 Das Register wurde seit Anfang 1999 bei der Dienststelle Bundeszentralregister des Generalbundesanwalts in Bonn geführt, seit dem 1. Januar 2007 beim Bundesamt für Justiz (BfJ), das aufgrund des Gesetzes zur Errichtung und zur Regelung der Aufgaben des Bundesamts für Justiz vom 17. Dezember 2006 neu eingerichtet wurde (BGBl. I, S. 3171–3174).

168 BT-Drs. 12/6853, S. 3.

169 BT-Drs. 12/6853, S. 37.

170 *Gieg*, KK-StPO, § 494 Rn. 4.

Das länderübergreifende staatsanwaltschaftliche Verfahrensregister ist als eine Datenbank zur Speicherung der anhängigen Ermittlungsverfahren konzipiert und wird sich in Teilen an die Struktur des BZR-Verfahrens anlehnen.[171] Zur Identifizierung eines Beschuldigten und zur sachgerechten Führung des Ermittlungsverfahrens teilt die mitteilungspflichtige Stelle, also die Staatsanwaltschaft oder die dieser in steuerstrafrechtlichen Angelegenheiten gleichgestellte Finanzbehörde, der Registerbehörde – Bundesamt für Justiz (BfJ) – insbesondere die Personendaten des Beschuldigten, die Tatzeiten und -vorwürfe, das Aktenzeichen sowie die Verfahrenseinleitung und -erledigung mit. Die Mitteilung erfolgt bei jedem Beschuldigten unabhängig von der Bedeutung der vorgeworfenen Tat. Über jeden Beschuldigten sind der Registerbehörde in jedem Fall zwei Mitteilungen zu machen: die Erstmitteilung über die Einleitung des Verfahrens sowie die Erledigungsmitteilung über den Abschluss des Ermittlungsverfahrens.[172] Mit diesen Informationen wird eine Vollspeicherung im Register erreicht. Die Einzelheiten legt die mit Zustimmung des Bundesrates erlassene Errichtungsanordnung des Bundesjustizministeriums gemäß § 494 Abs. 4 StPO fest.[173] Danach kann im Falle einer besonderen Geheimhaltungsbedürftigkeit des Strafverfahrens die Übermittlung unter Maßgabe der Norm erfolgen, dass Auskünfte über die übermittelten Daten an eine andere als die mitteilende Stelle ganz oder teilweise zu unterbleiben haben (§ 3 Abs. 2 ZStVBetrV). Daneben ist unter bestimmten Voraussetzungen auch die vorübergehende Zurückstellung der Übermittlung möglich (§ 3 Abs. 3 Satz 1 ZStVBetrV). Um dieses Register jederzeit aktuell zu halten, wird gefordert, dass die Übermittlung der vorhandenen Daten an die Registerbehörde grundsätzlich zeitgleich mit der Einleitung eines Ermittlungsverfahrens vorgenommen wird (§ 3 Abs. 1 Satz 1 ZStVBetrV).

Die Datenübermittlung erfolgt grundsätzlich im Wege eines automatisierten Abrufverfahrens oder eines automatisierten Anfrage- und Auskunftsverfahrens, also im Wege der Datenfernübertragung. Auf Ersuchen mit nicht eindeutig zuordenbaren oder unvollständigen Identifizierungsdatensätzen übermittelt die Registerbehörde an die ersuchende Stelle für Zwecke der Identitätsprüfung die in § 4 Abs. 1, 2 Satz 1 Nr. 1 und 2 sowie Abs. 3 bezeichneten Daten von bis zu zwanzig unter ähnlichen Identifizie-

171 BT-Drs. 13/386.

172 *Hilger*, LR-StPO, § 492 Rn. 20.

173 Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrens-registers (ZStVBetrV) vom 23. September 2005.

rungsdaten gespeicherten Personen und teilt mit, wie viele weitere Datensätze zu Personen mit ähnlichen Identifizierungsdaten vorhanden sind.

2. Inhalt des Registers

a) Das Bundeszentralregister

Durch das BZRG wurde die Registeraufgabe wesentlich erweitert. § 3 BZRG schreibt vor, welche Daten in das Register einzutragen sind. Danach sind neben rechtskräftigen strafgerichtlichen Verurteilungen (§§ 4 bis 9 BZRG), Entmündigungen (§ 10 Abs. 1 BZRG) und Vermerken über Schuldunfähigkeit (§ 12 Abs. 1 BZRG) auch bestimmte Entscheidungen von Verwaltungsbehörden und Gerichten (§ 11 BZRG) einzutragen. Außerdem werden die gerichtlichen Entscheidungen registriert, die im Zusammenhang mit Betäubungsmittelabhängigkeit stehen (§ 17 Abs. 2 BZRG), sowie diejenigen Entscheidungen, die eine im Zusammenhang mit der Ausübung eines Gewerbes begangene Tat betreffen (§§ 18, 32 Abs. 4 BZRG). Ferner können Suchvermerke und Steckbriefnachrichten im Register niedergelegt werden (§ 25 BZRG). Gemäß § 54 BZRG müssen ebenso strafgerichtliche Verurteilungen ausländischer Gerichte in das BZR eingetragen werden, wenn sie sich auf deutsche Staatsbürger oder im Geltungsbereich des BZR geborene oder wohnhafte Ausländer beziehen und eine Straftat betreffen, die nach deutschem Recht ein Vergehen oder Verbrechen darstellt. Wenn strafrechtliche Verurteilungen Deutscher durch einen anderen Mitgliedstaat der Europäischen Union deshalb nicht in das Register einzutragen sind, weil die Voraussetzungen des § 54 Abs. 1 Nr. 2 BZRG nicht erfüllt sind, müssen diese durch das BfJ im Register gesondert gespeichert werden (§ 56b BZRG). Die Speicherungen dürfen an einen anderen Mitgliedstaat nur zur Unterstützung eines strafrechtlichen Verfahrens in diesem Staat auf Grund eines Ersuchens übermittelt werden.

Entscheidungen und Anordnungen, die in Anbetracht der Besonderheiten des Jugendstrafrechts, das vorwiegend auf den Erziehungsgedanken abzielt, in das Erziehungsregister eingetragen werden, sind gesondert in § 60 BZRG geregelt. Gespeichert werden Anordnungen von Maßnahmen nach § 3 Satz 2 JGG sowie Erziehungsmaßregeln oder Zuchtmittel, Schuldsprüche, Anordnungen des Familiengerichts sowie Freisprüche oder Verfahrenseinstellungen wegen mangelnder Reife.

Im Hinblick auf die erweiterte Aufgabe des Registers ist der Begriff "Strafregister" durch den nicht als diskriminierend empfundenen neutralen Begriff "Bundeszentralregister" ersetzt worden.[174]

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die in das ZStV einzutragenden Daten regeln § 492 Abs. 2 StPO und § 4 ZStVBetrV. In den Vorschriften werden die einzutragenden Daten abschließend ausgeführt. Es dürfen danach keine anderen Daten als die Personendaten der beschuldigten Person, die Daten zur Straftat, Vorgangsdaten wie etwa die mitteilende Stelle, die sachbearbeitende Stelle der Polizei sowie die Aktenzeichen und die Daten zum Verfahrensstand gespeichert werden. Im ZStV werden also die Daten neu eingeleiteter, laufender und auch bereits eingestellter Ermittlungsverfahren über alle beschuldigten Personen unabhängig vom Gewicht vorgeworfener Taten gespeichert.

3. Verwendung der Daten aus dem Register

a) Das Bundeszentralregister

Das Strafregister stellt sich durch die einheitliche Einrichtung von Strafverzeichnissen auf die umfassende Versorgung – insbesondere der Justizbehörden – mit den erforderlichen Informationen ein. Damit wird der Zugang zu zuverlässigen Angaben über die kriminelle Vergangenheit sowie zu anderen für die Beurteilung der Persönlichkeit eines Beschuldigten wichtigen Gesichtspunkten als Voraussetzung für Täterschaftsindiz, Strafzumessung und Rückfallverschärfung gewährleistet.[175] Hierbei sind die Regelungen des Bundeszentralgesetzes bedeutsam. Da bei der Verwendung von 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. Daraus folgen verfassungsrechtliche Anforderungen wie Zweckbindungsgrundsatz, Datensparsamkeit usw.

174 *Tolzmann*, Bundeszentralregistergesetz, S. 9.
175 *Rebmann*, Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513, 1513.

Die Registereintragungen werden grundsätzlich im Wege des Privat- sowie Behördenführungszeugnisses und der unbeschränkten Auskunft angekündigt. Auch Eintragungen ausländischer Verurteilungen im Zentralregister sind entsprechend den für deutsche Verurteilungen geltenden Regelungen in Führungszeugnisse und Auskünfte aus dem Register aufzunehmen. Über Führungszeugnisse wird Auskunft über die eine bestimmte Person betreffenden Inhalte des BZR grundsätzlich auf Antrag des Betroffenen (§ 30 BZRG) und ausnahmsweise auf Anforderung von Behörden (§ 31 BZRG) erteilt. Die Daten, die im Strafverfahren verwendet werden dürfen, erhalten bestimmte Behörden, z. B. Gerichte und Staatsanwaltschaften, für die in § 41 BZRG genannten Zwecke (z. B. in Strafverfahren, vor der Erteilung eines Waffenscheines, vor einer Einbürgerung, vor einer Verbeamtung usw.). Sie können diesbezüglich eine unbeschränkte Auskunft in Anspruch nehmen und einen entsprechenden Auszug aus eigener Veranlassung direkt beim Bundesamt für Justiz anfordern, ohne dass der Betroffene davon Kenntnis erhält. In unbeschränkten Auskünften sind auch solche Eintragungen enthalten, die nicht oder jedenfalls nicht mehr in das Führungszeugnis aufzunehmen sind.

aa) Führungszeugnis

Im Privatführungszeugnis, das auf Antrag jeder Person, die das 14. Lebensjahr vollendet hat, oder ihres gesetzlichen Vertreters erteilt wird, wird nur ein begrenzter Ausschnitt der tatsächlich möglichen Eintragungen aufgenommen. Die in das Führungszeugnis aufzunehmenden und nicht aufzunehmenden Inhalte regelt im Einzelnen § 32 BZRG. Das Führungszeugnis kann für eigene Zwecke (Privatführungszeugnis) oder zur Vorlage bei einer deutschen Behörde (Behördenführungszeugnis) erteilt werden. Der Inhalt des Behördenführungszeugnisses geht dabei über das Privatführungszeugnis hinaus (§ 32 Abs. 3, 4 BZRG). Weiters hat jede Person, die das 14. Lebensjahr vollendet hat, gemäß § 42 BZRG einen Anspruch auf eine Auskunft darüber, welche Eintragungen über sie im Register enthalten sind. Die Mitteilung kann durch Einsichtnahme bei der Registerbehörde oder durch Übersendung der Auskunft an ein von der betroffenen Person benanntes Amtsgericht erfolgen, bei dem die betroffene Person die Auskunft persönlich einsehen kann. Ein Antrag nach § 42 BZRG ist schriftlich oder durch persönliches Erscheinen an das BfJ (Referat IV 1) zu richten. Dieser muss die vollständigen Personendaten der antragstellenden Person (Geburtsname, Familienname, sämtliche Vornamen, Geburts-

datum und -ort) enthalten. Ein Privatführungszeugnis ist im Hinblick auf den Aspekt der Wiedereingliederung der Bestraften in Beruf und Gesellschaft oder des Datenschutzes jedoch nicht unproblematisch. Zum Beispiel werden Führungszeugnisse als datenschutzrechtliche Selbstauskunft in großem Umfang von der Arbeitgeberseite gefordert und damit von den Stellenbewerberinnen und -bewerbern beantragt. Zweifelhaft erscheint, ob das privatwirtschaftliche Interesse an der Gewinnung unbestrafter Mitarbeiterinnen und Mitarbeiter als schutzbedürftiges Allgemeininteresse gelten kann.[176]

Behörden erhalten grundsätzlich in Form eines Führungszeugnisses Auskunft aus dem Register, das in der Regel von der betroffenen Person beantragt wird. Behörden können gemäß § 31 BZRG jedoch auch selbst ein Führungszeugnis beantragen, soweit sie es zur Erledigung ihrer hoheitlichen Aufgaben benötigen und eine Aufforderung an die betroffene Person, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt (§ 31 Abs. 1 S. 2 BZRG). Die Behörde hat der betroffenen Person auf Antrag Einsicht in ihr Führungszeugnis zu gewähren. Nach § 31 BZRG wird ausnahmslos sämtlichen Behörden die Möglichkeit gegeben, für alle ihnen geeignet erscheinenden Zwecke über jedermann ein Führungszeugnis anfordern zu können, sofern nur eine hoheitliche Aufgabe zu erledigen ist. Die Vorschrift scheint aber schwer mit den verfassungsrechtlichen Anforderungen zum Datenschutz vereinbar, da der Verwendungszweck weder bereichsspezifisch noch präzise bestimmt ist. Vielmehr kann das Behördenführungszeugnis auf der Grundlage einer Generalklausel angefordert werden, ohne dass gesichert wäre, dass die spezifisch hoheitlichen Zwecke, für die das Führungszeugnis angefordert wird, die Offenlegung der im Führungszeugnis enthaltenen Angaben gerade für diesen Zweck erfordern. Noch bedenklicher ist, dass die Behörde die Bereitschaft der Betroffenen, ein ihnen auf Antrag erteiltes Führungszeugnis selbst beizubringen, unter der oben genannten, kaum objektivierbaren Voraussetzung übergehen kann und dass die Anforderung an die Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist, womit dann auch die Möglichkeit der Betroffenen ausgehebelt wird, auf Verlangen Einsicht in das Führungszeugnis zu nehmen. Hier müsste zumindest eine Pflicht der Behörden festgeschrieben werden, zum nachträglichen Rechtsschutz des Betroffenen den Grund ausdrücklich zu dokumentieren, aus dem sie eingeschätzt haben, dass die Vorlegung eines Führungszeugnisses durch den

176 *Tolzmann*, Bundeszentralregistergesetz, S. 12.

Betroffenen nicht zu erwarten ist, und dass die Betroffenen nachträglich von der Einholung des Führungszeugnisses in Kenntnis zu setzen sind.[177]

Die in das Führungszeugnis aufgenommenen Eintragungen bestehen nicht dauerhaft. Die Nichtaufnahme von Verurteilungen in das Führungszeugnis unterscheidet sich von der Tilgung als der endgültigen und unwiederbringlichen Entfernung von Eintragungen im Zentralregister darin, dass Eintragungen bloß im Führungszeugnis nicht mehr angezeigt werden, im Register aber noch verbleiben. Die Aufnahme in das Führungszeugnis hängt von einer Frist ab, die sich grundsätzlich nach der Höhe der Strafe richtet, unabhängig von dem der Verurteilung zugrunde liegenden Delikt. Die Nichtaufnahmefrist beträgt meist fünf Jahre (§ 34 Abs. 1 BZRG), nur ausnahmsweise drei Jahre bei § 34 Abs. 1 Nr. 1 BZRG und zehn Jahre bei § 34 Abs. 1 Nr. 2 BZRG. Sind im Register mehrere Verurteilungen eingetragen, so sind, solange eine von ihnen in das Zeugnis aufzunehmen ist, alle in das Führungszeugnis aufzunehmen (Mitzieheffekt, § 38 Abs. 1 BZRG). Die Regelung kennt Ausnahmen in § 38 Abs. 2 BZRG.

Die Nichtaufnahme von Verurteilungen in das Führungszeugnis kann mit einer Anordnung der Registerbehörde auf Antrag oder von Amts wegen geschehen, soweit diese Anordnung nicht dem öffentlichen Interesse entgegensteht. Die Fristverkürzungsmöglichkeit dient dazu, besonderen Umständen, die in Tat oder Täterpersönlichkeit begründet sein mögen, durch eine Einzelfallentscheidung Rechnung zu tragen.[178] Die Möglichkeit beschränkt sich auf eng begrenzte Ausnahmefälle. Dadurch wird der Interessenwiderstreit zwischen dem öffentlichen Interesse an der Vollständigkeit des Registers und dem Rehabilitationsinteresse des Betroffenen bereits durch die nach der Höhe der Verurteilungen gestaffelten Fristen berücksichtigt.[179]

bb) Unbeschränkte Auskunft

Unter dem Aspekt des Schutzes persönlicher Daten im Strafverfahren hat die unbeschränkte Auskunft eine erhebliche Bedeutung. Bestimmten, in

177 *Tolzmann*, Bundeszentralregistergesetz, S. 15.

178 *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 10.

179 Dazu ausführlich *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 11 ff.; *Kalf*, Die Fristen des Bundeszentralregistergesetzes in der strafrechtlichen Praxis, StV 1991, 137, 138 f.

§ 41 BZRG aufgeführten Stellen (u. a. Gerichten, Staatsanwaltschaften sowie bestimmten Behörden) ist durch die Registerbehörde auf Antrag eine unbeschränkte Auskunft aus dem Zentralregister zu erteilen. In Auskünfte an diese Stellen sind auch solche Eintragungen aufzunehmen, die nicht oder nicht mehr in Führungszeugnisse aufzunehmen sind. In diese Auskünfte wird also der gesamte Inhalt des Registers aufgenommen, auch nach Ablauf bestimmter Nichtaufnahmefristen. Hierbei gibt der Gesetzgeber dem Interesse der Allgemeinheit an der Abwehr besonderer Gefahren Vorrang vor dem Interesse des Betroffenen an einer möglichst reibungslosen Wiedereingliederung.[180]

Bei einer Auskunftsanfrage fordert das BZRG zum Schutz vor einem übermäßigen Zugriff die Zweckbindung, damit bei einer Anfrage eine Zweckangabe gesetzlich vorgesehen ist, die von der Registerbehörde darauf geprüft wird, ob der angegebene Zweck ein Recht auf unbeschränkte Auskunft begründet. Für den Schutz dieser hochsensiblen Daten sind die auskunftsberechtigten Stellen in Verbindung mit der Beschränkung der Auskunftserteilung auf bestimmte Zwecke eng begrenzt und abschließend aufgezählt. Darin werden die Gerichte, Gerichtsvorstände, Staatsanwaltschaften und Aufsichtsstellen (§ 68a des StGB) für Zwecke der Rechtspflege sowie die Justizvollzugsbehörden für Zwecke des Strafvollzugs einschließlich der Überprüfung aller im Strafvollzug tätigen Personen ernannt. Dies gilt also auch für die Nutzung der Daten im Strafverfahren für die Strafrechtspflege. Die unbeschränkte Auskunft wird nur auf ausdrückliches Ersuchen erteilt (§ 41 Abs. 4 BZRG). In diesem Ersuchen muss angegeben werden, aus welchem Grund die angeforderte Auskunft erforderlich ist, die dann ausschließlich zu dem genannten Zweck verwendet werden darf. Grundsätzlich ist das Ersuchen auf einem Vordruck mit einer Zweckangabe an die Registerbehörde zu richten; heute ergeht es aber weitgehend auf elektronischem Weg.[181] Die Weitergabe von Eintragungen, die nicht in ein Führungszeugnis aufgenommen werden, ist nur dann erlaubt, 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 (§ 43 BZRG). Die Weitergabe von Führungszeugnissen für Behörden an eine andere Behörde ist erlaubt,

180 Vgl. OLG Hamm, NStZ 1985, 558 (558); *Tolzmann*, Bundeszentralregistergesetz, § 39 Rn. 4, 17, § 30 Rn. 6 ff.; *Rebmann/Uhlig*, BZRG, § 39, Rn. 31 ff.; *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 10.

181 *Tolzmann*, Bundeszentralregistergesetz, § 41 Rn. 65 f.

wenn bei dieser die Voraussetzung, nämlich die Einwilligung der Betroffenen, erfüllt ist. Schranken wie etwa die abschließende Aufzählung der auskunftsberechtigten Stellen, die grundsätzliche Begrenzung auf Einzelanfragen oder die Beschränkung der Auskunftserteilung auf bestimmte Zwecke sind also gesetzlich eingebaut worden, um den Schutz personenbezogener Daten zu gewährleisten und damit unberechtigten oder übermäßigen Zugriff auf diese Daten zu vermeiden. Die Auskünfte aus dem Zentralregister an Behörden (§ 30 Abs. 5, §§ 31, 41, 43 BZRG) beschränken sich außerdem auf den mit der Entgegennahme oder Bearbeitung betrauten Bediensteten (§ 44 BZRG), damit das Interesse der Betroffenen an einer weitestgehenden Geheimhaltung ihrer Daten garantiert werden kann.

Da die vorliegende Arbeit darauf abzielt, die Frage des Schutzes personenbezogener Daten im Strafverfahren oder, genauer gesagt, die des Schutzes der für Strafverfahren verwendeten personenbezogenen Daten im Strafverfahren, zu untersuchen, aber nicht die des Schutzes der personenbezogenen Daten in sämtlichen Bereichen, wird die Frage des Führungszeugnisses hier nicht weiter diskutiert. Im Mittelpunkt steht vielmehr die unbeschränkte Auskunft, die den Justizbehörden im Strafverfahren erteilt wird.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die im ZStV erhobenen Daten dürfen grundsätzlich nur für Strafverfahren gespeichert, verändert und verwendet werden (§ 492 Abs. 2 S. 2, Abs. 6 StPO) und grundsätzlich erhalten nur die Strafverfolgungsbehörden Auskünfte aus dem ZStV, und zwar ausschließlich zum Zweck der Verwendung im Strafverfahren. Dabei spielt es keine Rolle, ob die Verwertung in dem Verfahren erfolgt, in dem übermittelt wurde, oder in einem anderen. Zu den Strafverfolgungsbehörden gehören hierbei neben den Staatsanwaltschaften und den Finanzbehörden in Ermittlungsverfahren nach §§ 399, 386 AO auch die Polizeibehörden, die Finanzbehörden in Ermittlungsverfahren nach § 402 AO sowie die Steuer- und Zollfahndungsdienststellen, soweit sie im Einzelfall strafverfolgend tätig sind. Nach dem Zweckbindungsgrundsatz ist also die Verwertung personenbezogener Daten aus dem ZStV nur auf ihre Verwendung im Strafverfahren eingeschränkt. Um unnötigen Aufwand zu vermeiden, dürfen allerdings auch den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst und dem Bundesnachrichtendienst Auskünfte erteilt werden, sofern diesen ein Auskunftsrecht gegenüber den

Strafverfolgungsbehörden zusteht. In diesem Fall beschränken sich die Auskünfte auf die in § 492 Abs. 2 Satz 1 Nr. 1 und 2 StPO genannten Daten. Für den Erhalt weiterer Auskünfte wenden sich die Dienste unmittelbar an die betreffenden Staatsanwaltschaften. Um einen unbefugten oder übermäßigen Eingriff in das Recht der Bürger auf informationelle Selbstbestimmung abzuwehren, sind beim ZStV verschiedene Maßnahmen sichergestellt. So ist die Anzahl der Datensätze, die auf Grund eines Abrufs übermittelt werden dürfen, auf das für eine Identifizierung notwendige Maß zu begrenzen (§ 492 Abs. 4a Satz 4 und Abs. 6 StPO). Angesichts der mit der automatisierten Datenverarbeitung verbundenen Gefahr und der besonderen Schutzbedürftigkeit der im Register gespeicherten Daten wird ferner gefordert, dass die erforderlichen und angemessenen Maßnahmen getroffen werden, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen. Für die Zulässigkeit des einzelnen automatisierten Abrufs ist grundsätzlich der Empfänger verantwortlich. Die Registerbehörde muss allerdings nach § 493 Abs. 3 Satz 3 ein Stichprobenverfahren durchführen.[182] Nach § 10 Abs. 2 BDSG ist es gewährleistet, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann.

4. Speicherdauer

a) Das Bundeszentralregister

Eintragungen, die nach dem BZRG gespeichert werden, bleiben nicht ewig im BZR gespeichert, sondern werden unter bestimmten Voraussetzungen getilgt, es sei denn, es handelt sich um eine Verurteilung zu lebenslanger Freiheitsstrafe oder aber die Unterbringung in der Sicherungsverwahrung oder in einem psychiatrischen Krankenhaus wurde angeordnet (§ 45 BZRG).

Die Tilgung besteht in der vollständigen Entfernung der Eintragung aus dem Register durch die Löschung des Datensatzes auf dem Datenträger. Das bedeutet, dass nach der Entfernung niemand mehr – auch nicht die Registerbehörde selbst – Zugriff auf diese Daten nehmen und damit Kenntnis von ihnen erlangen kann. Neben der Nichtaufnahme bestimmter Eintragungen in das Führungszeugnis unterliegen die Regis-

182 Kritisch zur Praktikabilität *Gemählich*, KMR, § 493 Rn. 5; *Hilger*, LR-StPO, § 493 Rn. 20.

tereintragungen der fristgebundenen (§§ 45 bis 47) oder der fristunabhängigen Tilgung (§§ 48, 49). § 16 Abs. 2 BZRG regelt die fristunabhängige Entfernung von Entscheidungen aus dem Register, wenn sie in einem Wiederaufnahmeverfahren rechtskräftig aufgehoben wurden. In § 24 BZRG ist außerdem die Möglichkeit geregelt, die Eintragungen drei Jahre nach dem Eingang der Mitteilung oder der Vollendung des 90. Lebensjahres der von diesen Eintragungen betroffenen Person oder nach dem Todeseintritt zu entfernen, wenn ihr Tod gegenüber der Registerbehörde glaubhaft gemacht wurde.[183] Die Vorschrift zielt darauf ab, einem stetigen Anwachsen des Registers durch Belassen überholter Eintragungen entgegenzuwirken.[184] Außerdem werden Eintragungen im Erziehungsregister entfernt, sobald der Betroffene das 24. Lebensjahr vollendet hat (§ 63 Abs. 1 BZRG).

In besonderen Fällen können Eintragungen aufgrund einer Anordnung auch unabhängig von der Tilgungsfrist getilgt werden, falls die Vollstreckung erledigt ist und das öffentliche Interesse der Anordnung nicht entgegensteht (§ 49 BZRG). Damit kann das Bedürfnis befriedigt werden, die gesetzlich festgelegten Tilgungsfristen aus Gründen der Einzelfallgerechtigkeit um der Rehabilitation und der Resozialisierung des Betroffenen willen abzukürzen. Die Anordnung kann auf Antrag oder von Amts wegen erfolgen, sofern die Registerbehörde aus anderem Anlass einen Registerstand erkennt, der den Betroffenen unverhältnismäßig belastet. Die vorzeitige Tilgung aufgrund einer Anordnung setzt ähnlich wie bei der vorzeitigen Nichtaufnahme einer Verurteilung in das Führungszeugnis voraus, dass die Vollstreckung erledigt ist und das öffentliche Interesse der Anordnung nicht entgegensteht. Sie ist aber nur in außergewöhnlichen Härtefällen möglich, bei denen die Versagung der Registervergünstigung in der Bevölkerung auf Unverständnis stoßen würde.[185] Wenn die Registerbehörde den Antrag für unzulässig oder unbegründet erklärt, kann der Betroffene die Beschwerde führen.

Die Tilgung aufgrund eines Fristablaufs als ein Regelfall erfolgt automatisch, also ohne weitere Überprüfung und ohne besonderen Antrag

183 Die Entfernung einer Eintragung unterscheidet sich von der Tilgung: Mit der Entfernung sind keine materiellen Rechtswirkungen verbunden. Das heißt, weder das Verwertungsverbot nach § 51 noch das Schweigerecht nach § 53 I Nr. 2 gilt für entfernte Eintragungen. Außerdem werden auch Eintragungen entfernt, für die die Tilgung nicht in Betracht kommt (*Tolzmann*, Bundeszentralregistergesetz, § 24 Rn. 9 ff.).

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

185 *Sawade/Schomburg*, Ausgewählte Probleme des Bundeszentralregistergesetzes, NJW 82, 551, 555.

seitens der Betroffenen. Bereits bei der Einordnung von Entscheidungen in das Register werden die Fristen für die Aufnahme in Führungszeugnisse sowie für die unbeschränkten Auskünfte und für die Tilgung von einem Fristenprogramm berechnet. Wird bei der täglichen Überprüfung der Tilgungsfristen festgestellt, dass Eintragungen gelöscht werden müssen, wird die Nummer des Satzes in eine Löschtabelle eingetragen. Der Satz wird anschließend von einem besonderen Löschprogramm untersucht, das sodann die Löschung vornimmt.[186] Bei der fristgebundenen Tilgung richtet sich die Länge der Tilgungsfrist gemäß §§ 46 ff. BZRG im Grundsatz nach der Höhe der Hauptstrafe.[187] Das BZRG regelt jede konkrete Tilgungsfrist nach den verhängten Strafen. Die Tilgungsfrist beträgt fünf Jahre bei Verurteilungen zu einer Geldstrafe von nicht mehr als neunzig Tagessätzen oder zu einer Freiheitsstrafe oder Strafarrest von nicht mehr als drei Monaten, zehn Jahre bei Verurteilungen zu einer Freiheitsstrafe oder Strafarrest von mehr als drei Monaten, aber nicht mehr als einem Jahr, zwanzig Jahre bei Verurteilungen wegen einer Sexualstraftat nach den §§ 174 bis 180 oder 182 StGB zu einer Freiheitsstrafe oder Jugendstrafe von mehr als einem Jahr oder fünfzehn Jahre in allen übrigen Fällen.

Der Ablauf der Tilgungsfrist einer Verurteilung wird durch weitere Verurteilungen gehemmt. Dies führt dazu, dass grundsätzlich alle Verurteilungen erst nach Ablauf der längsten Frist, die sich nicht zwingend nach der letzten Verurteilung bestimmt, gleichzeitig getilgt werden (§ 47 BZRG). Ergibt sich aus dem Register, dass die Vollstreckung einer Strafe oder eine der in § 61 des Strafgesetzbuches aufgeführten Maßregeln der Besserung und Sicherung noch nicht erledigt oder die Strafe noch nicht erlassen ist, ist der Ablauf der Tilgungsfrist ebenfalls gehemmt.

Der Tilgung werden die Rechtswirkungen, das Verwertungsverbot (§ 51 BZRG) und das Schweigerecht der Betroffenen (§ 53 I Nr. 2 BZRG) beigelegt. Von großer Bedeutung ist, dass die getilgte Eintragung in einem später gegen den Betroffenen anhängig gemachten Strafverfahren nicht mehr berücksichtigt werden darf. Ist die Eintragung über eine Verurteilung im Register getilgt worden oder ist sie zu tilgen, dürfen die Tat und die Verurteilung der betroffenen Person also im Rechtsverkehr nicht mehr

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

187 Die tatsächliche Entfernung einer Eintragung erfolgt erst ein Jahr nach Ablauf der Tilgungsfrist im Register endgültig und unwiederbringlich (§ 45 Abs. 2 BZRG). Innerhalb eines Jahres werden bloß keine Auskünfte mehr erteilt. Die Tilgungsfrist betrifft also unmittelbar die Dauer des Anspruchs bestimmter Behörden auf unbeschränkte Auskunft aus dem Register.

vorgehalten oder zu ihrem Nachteil verwertet werden. Dabei umfasst das Verwertungsverbot nach der Rechtsprechung nicht bloß die Tatsache der Vorverurteilung als solche, sondern es untersagt auch die Berücksichtigung der Warnfunktion einer früheren Verurteilung zulasten des Angeklagten.[188] Ausnahmen von diesem Verwertungsverbot regelt § 52 BZRG. Aus der Tat oder der Verurteilung entstandene Rechte Dritter, gesetzliche Rechtsfolgen der Tat oder der Verurteilung und Entscheidungen von Gerichten oder Verwaltungsbehörden, die im Zusammenhang mit der Tat oder der Verurteilung ergangen sind, bleiben von der Tilgung unberührt.

Bei im Register eingetragenen ausländischen Entscheidungen ist deren rechtliche und inhaltliche Überprüfung durch das BfJ gesetzlich nicht vorgesehen. Eine Überprüfung ausländischer Entscheidungen kann nur in dem Staat erreicht werden, in dem die Entscheidung getroffen wurde, durch Einlegung des nach dem Recht dieses Staates zulässigen Rechtsbehelfs. Sofern dem BfJ die Aufhebung einer ausländischen Entscheidung durch den Entscheidungsstaat mitgeteilt wird, wird diese aus dem Register entfernt.

Das BZRG fordert in § 42 Satz 6 überdies, dass nach einer Einsichtnahme in Eintragungen über den Betroffenen im Register die Mitteilung von der Einsichtsstelle vernichtet wird.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die Speicherdauer der in dem Strafverfahrensregister gespeicherten Daten ist in § 494 StPO festgeschrieben. Ihre Entfernung aus dem Register ist mit vier Voraussetzungen verbunden. Der erste Fall betrifft eine versehentliche Eintragung der Daten. Versehentlich eingetragene Daten müssen wieder entfernt werden, weil das ZStV nur solche Daten enthalten darf, deren Speicherung auch zulässig ist. Im zweiten Fall ist sichergestellt, dass Doppelspeicherungen im BZR und im länderübergreifenden ZStV vermieden werden. Wird also eine gerichtliche Entscheidung in das BZR eingetragen, so wird die entsprechende Eintragung im ZStV automatisch gelöscht. Drittens erfolgt die Löschung bei einem rechtskräftigen Freispruch, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und bei einer nicht nur vorläufigen, sondern endgültigen Verfahrenseinstellung,

188 BGHSt 24, 64 (65); BGHSt 28, 338 (340).

allerdings erst zwei Jahre nach der Verfahrenserledigung.[189] Schließlich erfolgt die Löschung in jenen Fällen, in denen dem ZStV ein weiteres Verfahren zu den vorher eingetragenen Daten mitgeteilt wurde, erst dann, wenn für alle Eintragungen die Löschungsvoraussetzungen vorliegen. Der Gesetzgeber hat außerdem in § 492 Abs. 4a Satz 2 und 3 StPO und § 8 Abs. 2 ZStVBetrV der ersuchenden Stelle die Pflicht auferlegt, nach erfolgter Identifizierung oder bei einer unmöglichen Identifizierung alle übermittelten Daten, die sich nicht auf den Betroffenen beziehen, unverzüglich zu löschen hat.

Die im ZStV gespeicherten Daten sind nach § 494 Abs. 3 i. V. m. § 489 Abs. 7 und 8 StPO zu sperren[190] statt zu löschen. Die Sperrung erfolgt, soweit potenziell günstige Informationen für den Betroffenen weiter verfügbar gehalten sowie Daten für laufende Forschungsarbeiten erhalten werden sollen, eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder wenn personenbezogene Daten nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Die gesperrten Daten dürfen verwendet werden, aber nur für den Zweck, für den die Löschung unterblieben ist, und auch nur, soweit dies zur Behebung einer bestehenden Beweisnot unerlässlich ist.

189 Nach der Entwurfsbegründung trägt die zweijährige Aufrechterhaltung der Speicherung trotz rechtskräftigen Freispruchs, unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens oder nicht nur vorläufiger Verfahrenseinstellung dem unverzichtbaren Informationsbedürfnis der Staatsanwaltschaften Rechnung (BT-Drs. 12/6853, S. 39). Diesbezüglich wird allerdings bezweifelt, ob dieses Informationsbedürfnis die für den Betroffenen eintretende Unschuldsvermutung in jedem Fall überwiegt (*Wolter*, Datenschutz und Strafprozeß, ZStW 1995, 793, 802; *Schmitt*, Strafprozessordnung, § 494, Rn. 9; *Temming/Schmidt*, HK-StPO, § 494 Rn. 10; *Kestel*, § 474 ff. StPO – eine unbekannte Größe, StV 1997, 266, 268; *Hellmann*, AK-StPO, § 476 Rn. 7). Der Entwurfsbegründung zustimmende Auffassung: *Kalf*, Die Fristen des Bundeszentralregistergesetzes in der strafrechtlichen Praxis, StV 1991, 137, 613; *Gieg*, KK-StPO, § 494 Rn. 6 unter Hinweis auf BVerfGE 74, 358; 82, 106.

190 Unter Sperrung ist die Kennzeichnung gespeicherter personenbezogener Daten zu verstehen, damit ihre weitere Verarbeitung oder Nutzung eingeschränkt werden kann (*Gieg*, KK-StPO, § 489 Rn. 6; *Schmitt*, Strafprozessordnung, § 489, Rn. 6; *Lemke*, NStZ 1995, 486).

II. Rasterfahndung

Die elektronische Datenverarbeitung durch die Strafverfolgungsbehörden begann bereits Ende der sechziger Jahre, aber ohne eine formalgesetzliche Grundlage.[191] Das Volkszählungsurteil des Bundesverfassungsgerichts, in dem anerkannt wird, dass die elektronische Datenverarbeitung personenbezogener Daten einen Eingriff in das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG hergeleitete Recht auf informationelle Selbstbestimmung darstellen kann, machte die Schaffung präziser bereichsspezifischer gesetzlicher Grundlagen für die elektronische Datenverarbeitung erforderlich. In diesem Zusammenhang wurde die Rasterfahndung durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992 in die StPO eingegliedert (§§ 98a – 98c). Da demnach jede Datenverarbeitung ohne einen gesetzlichen Erlaubnistatbestand grundsätzlich verboten ist, ermächtigen die Vorschriften die Strafverfolgungsbehörden dazu, sowohl polizeiinterne als auch -externe Dateien miteinander abzugleichen, wenn diese Maßnahme die Aufklärung einer Straftat befördern kann. Die Befugnis umfasst die Anordnung der Datenübermittlung gegenüber Dritten – Behörden und Privaten – sowie die maschinelle Abgleichung dieser Daten untereinander und mit Daten, die zur Strafverfolgung erhoben wurden. In diesen Vorschriften sind die Aussonderungs-, Übermittlungs- und Unterstützungspflicht der speichernden Stelle mit geregelt.

Nach § 98a Abs. 1, Satz 1 StPO ist die Rasterfahndung ein maschinell-automatisierter Datenabgleich der personenbezogenen Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit aus anderen Gründen an anderen Stellen gespeicherten Daten. Durch diesen Abgleich sollen Nichtverdächtige ausgeschlossen oder Personen festgestellt werden, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Mit Hilfe dieser Ermittlungsmethode, der sog. Rasterfahndung, bei der die Möglichkeit der automatisierten Datenverarbeitung für Zwecke der Strafverfolgung genutzt wird, sollen Hinweise und Spuren gefunden werden, die nach kriminalistischer Erfahrung

191 Das beruht auf der damaligen Erwägung, dass Datenverarbeitungsvorgänge ohne Grundrechtsrelevanz sind (*Ermisch*, Fahndung und Datenschutz – aus der Sicht der Polizei, in: Bundeskriminalamt (Hrsg.), Möglichkeiten und Grenzen der Fahndung, Vortragsreihe Bd. 25, 63 (63, 67)).

zur Aufklärung einer Straftat beitragen können. Diese werden dann auf herkömmliche Weise abgeklärt.[192]

Die elektronische Datenverarbeitung zu Zwecken der Fahndung gewinnt an Bedeutung. Damit einhergehend steigt auch das Bedürfnis nach dem Schutz personenbezogener Daten im Rahmen der Fahndung. Bei jeder Form von Rasterfahndung werden regelmäßig Daten von den Strafverfolgungsbehörden auf deren Ersuchen und zu deren Zweckverfolgung verarbeitet, ohne dass die Betroffenen von diesem Vorgang Kenntnis erhalten. Die heimliche Datenverarbeitung hemmt die Ausübung des Rechts auf informationelle Selbstbestimmung und kann einen psychischen Anpassungsdruck in Richtung einer möglichst unauffälligen Verhaltensweise auslösen. Dieser würde nach der Auffassung des Bundesverfassungsgerichts nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl. Diese Gefahr verschärft die Möglichkeit einer Persönlichkeitserfassung aufgrund der Verarbeitungsgeschwindigkeit sowie der Verknüpfungs- und Speichermöglichkeiten, über die die moderne Informationsverarbeitungstechnologie verfügt. Die Verknüpfung mehrerer Daten, deren Speicherzwecke unterschiedlich sind, würde die Bürger angesichts der für sie nicht durchschaubaren Möglichkeiten der elektronischen Datenverarbeitung verunsichern und stellt somit einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Angesichts des Umstands, dass in die Massenfahndungsmethode der Rasterfahndung typischerweise eine Vielzahl von unverdächtigen Dritten einbezogen werden, ist die Gefahr eines Missbrauchs der Staatsgewalt nicht von der Hand zu weisen.

Es ist daher zu klären, ob die Ermittlungsmethode der Rasterfahndung das Recht auf informationelle Selbstbestimmung ausreichend schützt, also ob die verfahrensrechtlichen Vorkehrungen für die Durchführung und die Organisation den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätzen zur Einschränkung des Rechts auf informationelle Selbstbestimmung genügen.[193] Dafür soll im Folgenden die gesetzli-

192 BT-Drs. 12/989, S. 36.

193 Siehe auch *Pehl*, Die Implementation der Rasterfahndung – eine empirische Untersuchung zur Anwendung, Umsetzung und Wirkung der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung, 2008, Berlin. Pehl zielt im Hinblick auf die Verfassungsmäßigkeit der Rasterfahndung darauf ab, eine empirische Datenbasis für zukünftige rechtspolitische Diskussionen und Entscheidungen zu schaffen, damit Implementations- und Evaluationsfragestellungen im Zusammenhang mit der Rasterfahndung auf der Basis empirischer Befunde diskutiert werden können.

che Gestaltung der Ermittlungsmethode „Rasterfahndung" konkret analysiert werden. Genauer gesagt soll untersucht werden, welche Daten unter welchen Bedingungen zu Zwecken der Rasterfahndung genutzt werden dürfen, wie lange die Daten gespeichert werden, ob eine Löschungspflicht statuiert wird, und wenn ja, wann die Daten konkret gelöscht werden sollen.

1. Organisationsstruktur

Die StPO differenziert zwischen dem Abgleich von polizeiinternen Dateien – dem üblichen polizeilichen Datenabgleich, das heißt dem Abgleich von Dateien, die der Polizei bereits zur Verfügung stehen (§ 98c StPO) – und polizeiexternen Dateien, die aus anderen Gründen an anderen Stellen gespeichert sind (Rasterfahndung im eigentlichen Sinn, §§ 98a und 98b StPO). Nach § 98c StPO dürfen also zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Die Vorschrift regelt jedoch keine Rasterfahndung wie in § 98a, sondern nur die Befugnis zum Abgleich bereits bei der Gefahrenabwehr oder bei der Strafverfolgung oder Strafvollstreckung gewonnener personenbezogener Daten aus einem Strafverfahren. § 98a Abs. 1 und 2 erlaubt den automatisierten Abgleich von Daten nur durch die Strafverfolgungsbehörden. Dabei ist die öffentliche oder private Stelle, bei der die für den Abgleich benötigten Daten gespeichert sind, verpflichtet, diese Daten aus ihrem Datenbestand auszusondern und den Strafverfolgungsbehörden zu übermitteln. Die speichernde Stelle ist nur dazu verpflichtet, die bereits bei ihr gespeicherten Daten zu übermitteln, aber sie darf nicht erst auf Anfrage der Staatsanwaltschaft Daten zum Zweck der Rasterfahndung erheben. Die Übermittlungspflicht beschränkt sich auf die Übermittlung der für den Datenabgleich erforderlichen Daten. Darüber hinaus hat die speichernde Stelle auf Anforderung der Staatsanwaltschaft die Abgleichstelle zu unterstützen. Der Abgleich darf sowohl zur Aufklärung einer Straftat als auch zur Ermittlung des Aufenthaltsortes einer Person erfolgen, nach der zu Zwecken eines Strafverfahrens gefahndet werden soll. Hierbei sind keine verfahrensrechtlichen Schutzvorkehrungen wie Richtervorbehalt, Straftatenkatalog oder Subsidiaritätsklausel vorgesehen und es bestehen auch keine Regelungen zur Rückgabe und Vernichtung von Daten, zur nachträglichen Unterrichtung der Betroffenen oder zur Mitwirkung von Datenschutzbeauftragten.

Nach § 98a StPO werden bereits vorhandene, personenbezogene Datenbestände, die von öffentlichen und nichtöffentlichen Stellen, die keine Strafverfolgungsbehörden sind, für andere Zwecke als die Strafverfolgung erhoben wurden, computergestützt nach bestimmten tätertypischen Prüfungsmerkmalen (Rastern) überprüft und abgeglichen. Durch die Rasterfahndung sollen Nichtverdächtige ausgeschlossen (negative Rasterfahndung) oder Personen festgestellt werden, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen (positive Rasterfahndung). Der Unterschied zwischen der negativen und der positiven Rasterfahndung liegt darin, dass bei ersterer ein einzelner von den Strafverfolgungsbehörden zu untersuchender Datenbestand durch Löschen von Personaldaten, die auf den Täter nicht zutreffen, auf einen Restbestand reduziert wird, während bei letzterer polizeilicher Einblick in eine Vielzahl von Dateien genommen wird.

Die Rasterfahndungsmethoden können nach der unterschiedlichen Eingriffsintensität unterteilt vorgestellt werden: die positive Rasterfahndung nach unbekannten Tätern, die negative Rasterfahndung mit einer Fremddatei als Ausgangsdatei und die negative Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist. Jede Form von Rasterfahndung hat eine jeweils unterschiedliche Eingriffsintensität. Bei der positiven Rasterfahndung führen nicht die Strafverfolgungsbehörden, sondern regelmäßig verschiedene Behörden und private Einrichtungen Suchläufe in den eigenen Dateien für Strafverfolgungszwecke durch. Nach diesen Suchläufen wird ein gefundener Datensatz in einer gesonderten Ergebnisdatei abgespeichert. Nur die Ergebnisdateien werden von den Strafverfolgungsbehörden eingesehen und miteinander oder mit Dateien abgeglichen, die bereits zu Strafverfolgungszwecken angelegt sind. Dabei ist grundrechtlich nicht nur zu bedenken, dass die auf dem Ergebnisband abgespeicherten Daten eine Kontextänderung erfahren, sondern auch, dass die von verschiedenen Behörden und privaten Einrichtungen durchgeführten Suchläufe in keinem Zusammenhang mit der eigentlichen Zwecksetzung der Datenspeicherung stehen. Außerdem besteht bei der Rasterfahndung für die herausgerasterten Personen die Gefahr, dass deren personenbezogene Daten zu einem partiellen oder vollständigen Persönlichkeitsbild zusammengefügt werden, sogar ohne Wissen der Betroffenen. Diese Möglichkeit löst einen psychischen Anpassungsdruck in Richtung der als „normal“ vermuteten Verhaltensmuster aus.

Bei der negativen Rasterfahndung gleichen die Strafverfolgungsbehörden demgegenüber die verschiedenen Dateien ab, um Personendaten aus einer Fremd- oder einer Ausgangsdatei, die zu Strafverfolgungszwecken

angelegt ist, zu löschen. Die Strafverfolgungsbehörden sehen nur die Ausgangsdatei ein, weil die Abgleichdateien beim Abgleich lediglich dazu genutzt werden, Daten aus dem Ausgangsdatenbestand zu löschen. Es entsteht hier jedoch eine Missbrauchsgefahr, weil die Abgleichdateien immerhin den Strafverfolgungsbehörden zur Verfügung gestellt werden. Bei der negativen Rasterfahndung mit einer Fremddatei als Ausgangsdatei wird die Ausgangsdatei aus ihrem ursprünglichen Kontext herausgelöst und in den polizeilichen Fahndungskontext überführt, während bei der negativen Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist, die Ausgangsdatei keine Zweckänderung erfährt.

Wenn eine Rasterfahndungsanordnung seitens des Ermittlungsrichters ergangen ist, läuft die Rasterfahndung in folgenden Schritten ab:

Zunächst wird eine Suchanfrage zur Recherche in den Datenbeständen öffentlicher und nichtöffentlicher Stellen mit Hilfe von Rastern für den konkreten Einzelfall (§ 98a Abs. 1 S. 5 StPO) unter Verwendung logischer Verknüpfungen zur Erstellung eines bestimmten Verdächtigenprofils formuliert. Anhand dieser Suchanfrage werden die Datenbestände nach bestimmten zuvor aufgestellten Kriterien durchsucht. Diejenigen Informationen, die mit der Suchanfrage übereinstimmen (Treffer), werden selektiert und in eine separate Datei (Report) ausgesondert und dort gespeichert. Bereits in diesem Stadium sind die Daten derjenigen, die mit den Rastern nicht übereinstimmen, im Wege der negativen Rasterfahndung auszufiltern. Übrig bleiben die Daten derer, die im Wege der positiven Rasterfahndung unter das Raster fallen und somit dem Verdächtigenprofil entsprechen. Die gesonderte Datei wird durch den Gewahrsamsinhaber an die Strafverfolgungsbehörden übermittelt. Nach § 98a Abs. 2 StPO ist die speichernde Stelle dazu verpflichtet, die erforderlichen Daten auszusondern und den Strafverfolgungsbehörden zu übermitteln. Über die Aussonderungs- und Herausgabepflicht hinaus hat die Speicherstelle auf Anforderung der Staatsanwaltschaft die Abgleichstelle zu unterstützen. Als Unterstützungshandlung gilt hierbei jede geeignete und zumutbare Hilfe, wobei insbesondere Bedienungshinweise, Passwortfreigabe, aktive Mitwirkung von Personal sowie die Nutzung von Programmen und Hardware der Speicherstelle in Betracht kommen.[194] Die so ausgesonderten und übermittelten Daten werden sodann bei den Strafverfolgungsbehörden mit anderen Daten maschinell abgeglichen. Beim Abgleich werden anhand (weiterer) Raster entweder positiv Personen festgestellt, die diesen Rastern entsprechen, oder negativ die Personen ausgesondert, die zwar das

194 *Greven*, KK-StPO, § 98a Rn. 27.

Verdächtigenprofil, nicht aber die Raster erfüllen. Sollte die durchgeführte Rasterung einen Tatverdacht ergeben, da einzelne Personen die Raster erfüllen, wird diesem mit den üblichen Ermittlungsmethoden weiter nachgegangen.

2. Abgleichbare Daten

Der Gesetzgeber hat bei der gesetzlichen Formulierung der Rasterfahndung die Art, den Inhalt und den Umfang der zu verwendenden Daten nicht näher umschrieben, sondern vielmehr den unpräzisen Begriff „personenbezogene Daten" gewählt. Diese Daten können von verschiedenen Speicherstellen angefordert und mit anderen Daten maschinell abgeglichen werden können. Der Gesetzgeber scheint also eine pauschale Erlaubnis zur Verarbeitung personenbezogener Daten zu geben.[195]

Die unpräzise Formulierung dürfte auf der Tatsache beruhen, dass es schwierig ist, bereits in der gesetzlichen Regelung zu beurteilen, welche Informationen über eine Person im Einzelfall aufklärungsrelevant sein können. Angesichts des Risikos einer zu extensiven Auslegung des Begriffs „personenbezogene Daten" und der Gefahr, dass mangels der Eingrenzung der personenbezogenen Daten durch die Verwendung von sensiblen Daten bzw. die Verknüpfung von an sich betrachtet vielleicht weniger sensibel erscheinenden Daten Persönlichkeitsbilder entstehen, ist ein Bemühen um Normenklarheit erforderlich.

3. Verwendung des Datenabgleiches

Angesichts der Gefahren, die mit einer Rasterfahndung verbunden sind, wird zweierlei Einschränkungen Rechnung getragen: zum einen der Einschränkung auf Straftaten von erheblicher Bedeutung, die durch den typisierenden Katalog ergänzt werden, und zum anderen dem Richtervorbehalt.

---

195 Vgl. die von *Riegel* und *Rogall* vorgeschlagenen Entwürfe: Die Übermittlung von Daten zu Rasterfahndungszwecken soll auf Namen, Anschrift und Geburtsdatum der betreffenden Personen beschränkt werden, mit Ergänzung um die Prüfungsmerkmale (*Riegel*, Rechtsprobleme der Rasterfahndung, ZRP 1980, 300, 306; *Rogall*, Moderne Fahndungsmethoden im Lichte eines gewandelten Grundrechtsverständnisses, GA 1985, 1, 20).

Eine besondere Fahndungsmethode der Polizei unter Einsatz von Computertechnologie, nämlich die Rasterfahndung mit polizeiexternen Dateien, darf nur bei Vorliegen zureichender tatsächlicher Anhaltspunkte für bestimmte Delikte eingesetzt werden, die in § 98a Abs. 1 Satz 1 StPO aufgeführt werden. Dies sind Straftaten „von erheblicher Bedeutung

1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 GVG),
3. auf dem Gebiet der gemeingefährlichen Straftaten,
4. gegen Leib oder Leben, die sexuelle Selbstbestimmung oder die persönliche Freiheit,
5. erwerbs- oder bandenmäßig oder
6. von einem Bandenmitglied oder in anderer Weise organisiert" begangen werden.

Mit Blick auf die Katalogtaten werden jedoch weder die den einzelnen Straftaten zuzuordnenden Gesetzesparagraphen bezeichnet, noch sind die gemeinsamen Merkmale der bezeichneten Straftaten erkennbar.[196] Außerdem ist die Bezeichnung „von erheblicher Bedeutung" problematisch. Denn was eine Straftat von erheblicher Bedeutung ist, lässt sich nur schwer bestimmen, und ob dieses Merkmal erfüllt ist, wird sich vielfach erst im Lauf der Ermittlungen ergeben. Diese Gesetzgebungstechnik oder die dabei verwendeten Begriffe könnten somit der Eingriffsintensität der Rasterfahndung nicht entsprechen und darüber hinaus gegen den Grundsatz der Normenklarheit verstoßen.

Die Rasterfahndung mit polizeiexternen Dateien darf nur durch das Gericht – bei Gefahr im Verzug auch durch die Staatsanwaltschaft – und nur dann angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters durch andere Maßnahmen erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die staatsanwaltschaftliche Eilanordnung bedarf der unverzüglichen richterlichen Bestätigung. Wird die Anordnung nicht binnen drei Tagen von dem Richter bestätigt, so tritt sie außer Kraft (§ 98b Abs. 1 S. 3 StPO). Der Richtervorbehalt ist eine wichtige verfahrensrechtliche Vorkehrung, um die Rechtsschutz- und Kontrollfunktion für Grundrechtseingriffsmaßnahmen auszuführen. Die Einschränkung von Grundrechten erfordern

196 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 115.

ein zwingendes Bedürfnis. Dieses ist bei einer Rasterfahndung jedoch nicht erkennbar. Eine Rasterfahndung benötigt eine gewisse Vorlaufzeit, weil die verschiedenen Speicherstellen daran teilnehmen müssen. Der Fall eines besonderen Eilbedürfnisses, das die Einholung einer richterlichen Entscheidung nicht zulassen würde, ist daher schwer vorstellbar.[197] Die richterliche Bestätigung innerhalb von drei Tagen ist ebenfalls bedenklich. Denn die Tatsache, dass die richterliche Bestätigung ausbleibt oder versagt wird, macht die Übermittlung und den Abgleich von Daten aufgrund staatsanwaltschaftlicher Anordnung nicht rechtswidrig. Dann entsteht das Problem der Verwertbarkeit der durch die Maßnahme erlangten Erkenntnisse. Eine Lösung dieses Problems kann nicht im Gesetz gefunden werden. Bestenfalls kann das Heranziehen der erlangten Beweismittel zur Beweisführung vom Tatrichter im Hauptverfahren abgelehnt werden.[198]

4. Aufbewahrungsdauer der Daten

Gemäß § 98b Abs. 3 Satz 1 StPO sind die erhaltenen Datenträger nach Beendigung des Abgleichs unverzüglich an die betreffenden Speicherstellen zurückzugeben. Personenbezogene Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden (§ 98b Abs. 3 Satz 2 StPO). Der Grund dafür, dass für das Löschen übertragener Daten ein späterer Zeitpunkt als für die Rückgabe der Datenträger gilt, ist der, dass die übertragenen Daten möglicherweise zur Beweisführung benötigt werden.[199] Durch die Löschung oder Rückgabe von Daten wird verhindert, dass Daten auf Vorrat gesammelt werden. Daher sind die Daten auf den erhaltenen Datenträgern unverzüglich, also *ohne eine nicht durch die Sachlage begründete Verzögerung*,[200] sofort nach der Beendigung des Abgleichs zurückzugeben und die Daten auf den übertragenen Datenträgern unver-

197 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 133.

198 *Schnarr*, Zur Verknüpfung von Richtervorbehalt, staatsanwaltlicher Eilanordnung und richterlicher Bestätigung, NStZ 1991, 209, 215.

199 Vgl. *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 135 f. m. w. N.

200 *Schmitt*, Strafprozessordnung, § 98b Rn. 6 unter Hinweis auf § 25 Rn. 8; vgl. die Legaldefinition in § 121 BGB: „ohne schuldhaftes Zögern".

züglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden. Die Daten sind damit spätestens mit rechtskräftigem Abschluss des Strafverfahrens zu löschen.[201] Eine Aufbewahrung über den gesetzlich normierten Zeitpunkt hinaus ist deshalb rechtswidrig, weil die weitere Aufbewahrung der Datenträger eine Aufrechterhaltung des Eingriffs in das informationelle Selbstbestimmungsrecht ohne die verfassungsrechtlich erforderliche gesetzliche Grundlage darstellt. Die Löschungspflicht gemäß § 98b Abs. 3 Satz 2 StPO ist gerade vor dem Hintergrund der Gefahren einer unbegrenzten Speicherung, Verwendung und Weitergabe von elektronischen Daten, die mit der modernen Datenverarbeitung verbunden sind, von besonderer Bedeutung.

Darüber hinaus ist zu bedenken, dass es keine Löschungs- oder Vernichtungsvorschrift für Daten gibt, die zwar aufgrund einer staatsanwaltschaftlichen Eilanordnung erlangt worden sind, danach jedoch gerichtlich nicht bestätigt wurden und damit außer Kraft treten.

5. Mitteilungspflicht

Bei der Rasterfahndung sind zwei Arten der Mitteilungspflicht mit geregelt: zum einen die Benachrichtigung der Betroffenen und zum anderen die Unterrichtung der für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz zuständigen Stelle.

§ 101 Abs. 4 Satz 1 Nr. 1 StPO statuiert die Pflicht zur nachträglichen Unterrichtung der Personen, gegen die nach Abgleich der Daten weitere Ermittlungen geführt wurden. Die weiteren Ermittlungen in diesem Sinn sind Ermittlungshandlungen herkömmlicher Art, wie die Vernehmung dieser Personen, Durchsuchungen, Nachforschungen in ihrem Umfeld oder die bloße Einholung von Auskünften über sie.[202] Somit fallen alle

201 Dagegen wird zum Teil die Auffassung vertreten, dass das Datenmaterial auch nach Urteilsrechtskraft für ein Wiederaufnahmeverfahren benötigt werden könnte und deshalb nicht zu vernichten ist(*Greven*, KK-StPO, § 98b Rn. 8 unter Hinweis auf *Schmitt*, Strafprozessordnung, § 101 Rn. 27). Dem ist jedoch entgegenzuhalten, dass allein die abstrakte Möglichkeit der Nützlichkeit von Daten in einem Wiederaufnahmeverfahren keine zeitlich unbegrenzte Aufrechterhaltung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung rechtfertigt (*Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 136 f.).

202 BT-Drs. 12/989, S. 38; *Erb*, LR-StPO, § 163d Rn. 81.

übrigen Betroffenen, deren personenbezogene Daten ebenfalls in die Rasterfahndung einbezogen waren, aus der Benachrichtigungspflicht heraus. Das beruht auf der Tatsache, dass Personen, die im Zuge einer Rasterfahndung von den Informationsverarbeitungsvorgängen betroffen sind, mit unterschiedlicher Intensität in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt werden. Diejenigen, die als Merkmalsträger nach mehreren Suchläufen herausgerastert wurden, sind stärker betroffen als diejenigen, deren Daten sich auf Datenträgern befinden, ohne zur Kenntnis genommen zu werden. Denn erst für denjenigen, der aus Datenträgern herausgefiltert wird, kommt es unmittelbar zu einer Gefährdung, während für alle übrigen nur die mittelbare Gefahr besteht, möglicherweise zur Kenntnis genommen zu werden.

Aber die personelle Beschränkung der Benachrichtigungspflicht auf diejenigen Merkmalsträger, gegen die weitere Ermittlungen geführt worden sind, geht zu weit, weil die Benachrichtigungspflicht nicht durch die Rasterfahndung an sich ausgelöst wird, sondern erst durch die dadurch veranlasste Vornahme weiterer Ermittlungen gegen diese Personen. Darüber hinaus entspricht die Beschränkung auch nicht dem Gebot des effektiven Rechtsschutzes. Für einen effektiven Rechtsschutz müssen die Bürger grundsätzlich Kenntnis davon haben, über welche sie betreffenden Informationen staatliche Stellen verfügen. In den Bereichen, in denen die Datenverarbeitung nicht offen aufgrund freiwillig gemachter Angaben betrieben wird, hängt diese Kenntnis ausschließlich von der Auskunftserteilung ab. Aus diesem Grund wird die Regelung der Benachrichtigungspflicht gefordert.

Die nachträgliche Benachrichtigung sollte daher grundsätzlich alle herausgerasterten Merkmalsträger einschließen. Sie sollte außerdem inhaltlich Folgendes enthalten: zunächst die Tatsache, dass eine Rasterfahndung angeordnet und durchgeführt wurde. Des Weiteren ist mitzuteilen, bei welcher Speicherstelle Daten ausgesondert, welche Prüfungsmerkmale gerastert wurden und welche Stelle im Besitz der Daten war oder noch ist.[203]

Die Benachrichtigung unterbleibt oder wird zurückgestellt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen oder sie den Untersuchungszweck, das Leben, die körperliche Unversehrtheit und die persönliche Freiheit einer Person und bedeutende

203 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 141; *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, S. 217 f.

Vermögenswerte gefährden könnte. Die Dauer der Benachrichtigungszurückstellung bestimmt das Gericht. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Die Benachrichtigung wird nachgeholt, sobald die Einschränkungsgründe wegfallen (§ 101 Abs. 4, 5 und 6 StPO).

Darüber hinaus ist gemäß § 98b Abs. 4 StPO nach Beendigung einer Maßnahme nach § 98a die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist. Denn der Einzelne kann überaus komplexe administrative Zusammenhänge sowie hochtechnische Verarbeitungsprozesse nur schwer durchschauen.[204] Aber die nachträgliche Kontrolle der zuständigen Stelle ist nicht umfangreich und reicht daher nicht aus. Zur effektiven Kontrolle des Datenschutzes sollten Vorabunterrichtung, Beratung und begleitende Kontrolle vorausgesetzt werden.[205]

III. Vorratsdatenspeicherung

1. Geschichtlicher Hintergrund

§ 12 FAG[206] regelte die Möglichkeit des Auskunftsverlangens über den Fernmeldeverkehr durch den Richter und bei Gefahr im Verzug auch

204 *Simitis*, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398, 403.

205 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 143.

206 Das Gesetz über Fernmeldeanlagen (FAG) wurde erstmals als Neubekanntmachung des Gesetzes über das Telegraphenwesen des Deutschen Reichs herausgegeben, 6. April 1892 (RGBl. S. 467), die weitere Neubekanntmachung vom 3. Juli 1989 (BGBl. I S. 1455). Zum 1. Januar 1998 trat das FAG überwiegend und zum 1. Januar 2002 vollends außer Kraft. Nachfolgeregelungen sind vor allem im Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120) enthalten.

durch die Staatsanwaltschaft.[207] Dabei legte § 5 TDSV[208] fest, welche Verbindungsdaten von Diensteanbietern – z. B. der Deutschen Telekom – gespeichert werden durften. Die folgenden Verbindungsdaten durften erhoben und verarbeitet werden: die Rufnummer oder die Kennung des anrufenden und des angerufenen Anschlusses, die personenbezogene Berechtigungskennung, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen und Kartenanschlüssen auch die Standortkennung (§ 5 Abs. 1 Nr. 1); Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhingen, die übermittelten Datenmengen (§ 5 Abs. 1 Nr. 2); die vom Kunden in Anspruch genommene Telekommunikationsdienstleistung (§ 5 Abs. 1 Nr. 3); die Endpunkte von festgeschalteten Verbindungen sowie deren Beginn und Ende nach Datum und Uhrzeit (§ 5 Abs. 1 Nr. 4).[209] Ein Problem lag hierbei darin, dass eine Anordnung zur Auskunft über diese Daten erfolglos sein konnte, da die Daten nur für einen durch das Gesetz nicht näher spezifizierten Zeitraum aufbewahrt wurden. Das heißt, die Strafverfolgungsbehörden konnten nur auf die zum Zeitpunkt der Erhebung noch beim Telekommunikationsanbieter gespeicherten Daten zurückgreifen. Da die Speicherdauer jedoch bei jedem Anbieter unterschiedlich war, war es dem Zufall überlassen, ob die Verkehrsdaten zum Zeitpunkt des Zugriffs noch vorhanden waren oder nicht. Dies konnte zu Schwierigkeiten bei der Strafverfolgung und gegebenenfalls zu erfolglosen Ermittlungen führen.

In diesem Zusammenhang hat der Wunsch der Strafverfolgungsbehörden nach Einführung einer Speicherung von Telekommunikationsdaten für Strafverfolgungszwecke auf EU-Ebene eine lange Geschichte. Diese Daten umfassen Verkehrsdaten, die nicht zu Abrechnungszwecken gespeichert werden müssen, Standortdaten sowie eindeutige Geräteidentifikationen. Die Speicherfrist geht dabei deutlich über die für reine Vertragszwecke zulässige Dauer hinaus, und die Speicherung wird weder durch Ver-

---

207 § 12 FAG: In strafrechtlichen Untersuchungen kann der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hat.

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

209 Die Vorschrift wurde später durch § 96 TKG ersetzt.

tragszwecke noch durch einen bestimmten Tatverdacht veranlasst. Sowohl in Deutschland als auch auf europäischer Ebene gab es seit langem Bemühungen, die Vorratsdatenspeicherung von Kommunikationsdaten einzuführen; alle Versuche waren jedoch gescheitert. Bereits im Jahre 1996 wurde in Deutschland der erste Versuch unternommen, eine Mindestspeicherfrist von Telekommunikationsdaten zu etablieren. Damit sollte vermieden werden, dass die von Strafverfolgungsbehörden angeforderten Daten nicht mehr vorhanden waren.[210] Dieser Versuch einer Gesetzgebung scheiterte an der Ablehnung der damaligen Bundesregierung, nach deren Auffassung eine Mindestspeicherfrist den verfassungsrechtlichen Geboten der Verhältnismäßigkeit, der Erforderlichkeit und der Zweckbindung widersprochen hätte.[211] Einen weiteren nennenswerten Versuch, eine Vorratsdatenspeicherung zur Diskussion zu stellen, gab es im Jahre 2000 im Rahmen der Innenministerkonferenz. Die Forderung nach Einführung der Vorratsdatenspeicherung wurde allerdings von den Datenschutzbeauftragten scharf kritisiert und anschließend abgelehnt.[212]

Die Einführung der Vorratsdatenspeicherung in Deutschland begann daher nicht auf nationaler, sondern auf europäischer Ebene. Als Reaktion auf die Zuganschläge am 11. März 2004 in Madrid und vor allem auf die Bombenanschläge vom 7. Juli 2005 auf U-Bahnen und einen Bus in London wurde nach dem bis zu diesem Zeitpunkt kürzesten Rechtsetzungsverfahren am 15. März 2006 die Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie) verabschiedet; sie trat zum 3. Mai 2006 in Kraft.[213] Gemäß Art. 15 Vorratsdatenspeicherungsrichtlinie waren die Mitgliedstaaten dazu verpflichtet, die Richtlinie bis zum 15. September 2007 und bezüglich der Internetdienste bis zum 15. März 2009 in nationales Recht umzusetzen. Die Richtlinie wurde demgemäß in Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007

210 BT-Drs. 13/4438, S. 23.
211 BT-Drs. 13/4438, S. 39.
212 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 150.
213 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.

in nationales Recht umgesetzt.[214] Hierbei wurden jedoch wiederkehrend verfassungsrechtliche Bedenken gegen die Vorratsdatenspeicherung geäußert, aufgrund derer es in der Folge zu einer rechtlichen Diskussion in Deutschland und auf europäischer Ebene kam. In der Folge wurde die Vorratsdatenspeicherung sowohl vom EuGH als auch vom Bundesverfassungsgericht jeweils für ungültig[215] oder für verfassungswidrig und nichtig erklärt.[216] Daraufhin wurde im Oktober 2014 ein neues Gesetz zur Vorratsdatenspeicherung in Deutschland verabschiedet, das am 18. Dezember 2015 in Kraft trat.[217] Doch selbst gegen das neue Gesetz, das den Anforderungen des Bundesverfassungsgerichts genügte, wurde erneut Verfassungsbeschwerde eingereicht.

a) Die Vorratsdatenspeicherungsrichtlinie auf europäischer Ebene

aa) Entstehungsgeschichte der Richtlinie

Das Recht auf Privatsphäre ist auf europäischer Ebene sowohl in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) als auch in Verträgen und Gesetzgebungen der EU verankert. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat den Geltungsbereich des Rechts auf Privatsphäre um die Feststellung erweitert, dass Artikel 8 der EMRK auch ein Recht auf Datenschutz gewährleistet, obwohl der EGMR im Rahmen der EMRK häufig einen Ermessensspielraum für die Mitgliedstaaten eröffnete, wenn das Recht auf Privatsphäre mit nationalen Sicherheitsbedenken in Konflikt geriet. Auf Ebene der Europäischen Union sind die Privatsphäre und personenbezogene Daten durch Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta) geschützt. In Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der durch den 2009 in Kraft getretenen Vertrag von Lissabon[218] eingeführt wurde, wird erneut darauf hingewiesen, dass „jede Person das Recht auf Schutz der sie betreffenden personen-

214 Das Gesetz trat am 1. Januar 2008 in Kraft. Es wurde mit eindeutiger Mehrheit angenommen; vgl. dazu *Orantek*, Die Vorratsdatenspeicherung in Deutschland, NJ 2010, 193, 199.
215 EuGH, C-293/12, 8. April 2014.
216 BVerfGE 125, 260.
217 Verkündung BGBl. 2015 I S. 2218.
218 Der Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft wurde

bezogenen Daten hat." Die Vorschrift ermächtigt den Unionsgesetzgeber zur Festlegung von Bestimmungen im Hinblick auf den Datenschutz. Die Einhaltung dieser Regeln unterliegt der Kontrolle unabhängiger Behörden.

Auf Ebene des Sekundärrechts wurde der Rahmen für den Datenschutz schrittweise durch die Richtlinie 95/46/EG zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten und zum freien Datenverkehr (Datenschutzrichtlinie) geschaffen.[219] Diese beschreibt Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der EU durch nationale Gesetze sichergestellt werden müssen. Vor allem für die Verarbeitung personenbezogener Daten besteht eine Anforderung der Richtlinie darin, dass die Datenerhebung in Relation zu dem Zweck, zu dem sie unternommen wird,[220] verhältnismäßig sein muss und dass sie im Allgemeinen vorbehaltlich der Zustimmung des Betroffenen ist.[221] Die Verarbeitung sensibler Daten ist grundsätzlich verboten.[222] Die Betroffenen sollen gemäß der Richtlinie über die Verarbeitung ihrer Daten informiert werden[223] und sie sind ermächtigt, Zugang zu ihren Daten zu erhalten und bei Bedarf die Berichtigung, Sperrung oder Löschung ihrer Daten zu verlangen.[224] In diesem Zusammenhang wurden die Verordnung 45/2001/EG[225] – die anders als eine Richtlinie, die durch die nationalen Parlamente erst in innerstaatliche Gesetze umgesetzt werden muss, unmittelbar nach ihrer Verabschiedung in den Mitgliedstaaten Geltung hat – und die Richtlinie 2002/58/EG[226] nacheinander

---

im ABl. 2007/C 306/01 veröffentlicht, zuletzt durch Abdruck der konsolidierten Textfassungen im ABl. 2012/C 326/01 bekanntgemacht.

219 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). Die Richtlinie wurde später durch die Verordnung (EU) 2016/679 am 25. Mai 2018 ersetzt.

220 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, Art. 6 (1).

221 a. a. O. Art. 7.

222 a. a. O. Art. 8 (1).

223 a. a. O. Art. 10.

224 a. a. O. Art. 12.

225 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.

226 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der

erlassen. Letztere aktualisiert die Grundsätze der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation und harmonisiert die Rechtsvorschriften der Mitgliedstaaten, um ein gleichwertiges Schutzniveau der Grundrechte und Grundfreiheiten sicherzustellen. Die Datenschutzrichtlinie wurde durch die Datenschutz-Grundverordnung ersetzt,[227] mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht wurden. Dadurch soll der Schutz personenbezogener Daten innerhalb der EU sichergestellt sowie der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Trotz dieser Bemühungen, die Regeln zur Verarbeitung personenbezogener Daten innerhalb der EU und ihrer Mitgliedstaaten zu vereinheitlichen, erlaubt der EU-Datenschutzrahmen bestimmte Ausnahmen, die die Mitgliedstaaten dazu ermächtigen, die in der Datenschutzrichtlinie angegebenen Rechte aus Gründen der nationalen Sicherheit einzuschränken. Aufgrund dieses außergewöhnlichen Ermessensspielraums führten einige EU-Mitgliedstaaten nach den Anschlägen vom 11. September 2001 Ausnahmen von den EU-Datenschutzvorschriften ein. Diese Fragmentierung der staatlichen Gesetzgebung hatte zur Folge, dass in unterschiedlichem Maße von den Datenschutzgrundsätzen der EU abgewichen und andere Regeln für die Vorratsdatenspeicherung von Daten durch Anbieter elektronischer Kommunikation festgelegt wurden. Mit dem Ziel, diese unterschiedlichen nationalen Gesetze miteinander in Einklang zu bringen, wurde im Jahr 2006 die Vorratsdatenspeicherungsrichtlinie[228] verabschiedet. Art. 1 Abs. 1 Vorratsdatenspeicherungsrichtlinie sieht die Verpflichtung der Mitgliedstaaten vor, bestimmte Daten, die von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder von Betreibern ei-

---

Privatsphäre in der elektronischen Kommunikation, 31. Juli 2002 (ABl. EG Nr. L 201 S. 37–47).

227 Die Richtlinie wurde 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 am 25. Mai 2018 ersetzt, um eine umfassende Wahrung des Datenschutzes zu garantieren und Mitgliedstaaten stärker in die Pflicht zu nehmen. Die Verordnung 2016/679 (Datenschutz-Grundverordnung) trat am 24. Mai 2016 in Kraft.

228 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.

nes öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, auf Vorrat zu speichern. Das Ziel dieser Richtlinie ist zum einen die Harmonisierung einzelner mitgliedstaatlicher Vorschriften und zum anderen die Sicherstellung des Umstands, dass die Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen. Gemäß Art. 4 der Richtlinie müssen die Mitgliedstaaten in nationalem Recht die Voraussetzungen für den Zugang zu diesen Daten entsprechend dem Notwendigkeits- und dem Verhältnismäßigkeitsgrundsatz sowie im Einklang mit den einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts und insbesondere der EMRK regeln. Die Richtlinie lässt den Mitgliedstaaten jedoch einen Ermessensspielraum bei der Festlegung der Bedingungen, die den Zugang zu den gespeicherten Daten rechtfertigen.

bb) Regelungen der Richtlinie

Die Richtlinie enthält 17 Vorschriften darüber, in welcher Weise konkrete Maßnahmen ergriffen werden dürfen. Als wesentlich können Art. 1, 5, 6, 7, 8 und 13 genannt werden. Art. 1 Vorratsdatenspeicherungsrichtlinie legt deutlich die Zielsetzung der Richtlinie fest, die zum einen in der Harmonisierung mitgliedstaatlicher Vorschriften über Vorratsdatenspeicherung und zum anderen in der Sicherstellung bestimmter Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten besteht. Hierbei kommen vornehmlich Terroranschläge und organisierte Kriminalität in Betracht. Darüber hinaus wird der Anwendungsbereich gemäß Art 1. Abs. 2 auf Verkehrs- und Standortdaten beschränkt; er erstreckt sich hingegen nicht auf den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden. In Art. 5 Abs. 1 Vorratsdatenspeicherungsrichtlinie sind die zu speichernden Daten zunächst nach Verwendungszwecken enumerativ geordnet. Als Verwendungszwecke werden die folgenden genannt:

1. Rückverfolgung und Identifizierung der Quelle einer Nachricht
2. Identifizierung des Adressaten einer Nachricht
3. Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung
4. Bestimmung der Art einer Nachrichtenübermittlung

5. Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern
6. Bestimmung des Standorts mobiler Geräte

Die zu speichernden Daten, die diesen Verwendungszwecken dienen können, werden sodann abschließend aufgelistet. Erfasst werden dabei Verkehrs- und Standortdaten und alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind.

Die oben genannten Daten sind gemäß Art. 6 Vorratsdatenspeicherungsrichtlinie mindestens sechs Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat zu speichern. Außerdem ist gemäß Art. 12 Vorratsdatenspeicherungsrichtlinie den Mitgliedstaaten die Möglichkeit beigemessen worden, die maximale Speicherfrist für einen begrenzten Zeitraum zu verlängern, sofern entsprechende Rechtfertigungsgründe vorliegen. Trifft die Kommission keine ausdrückliche Ablehnungsentscheidung, besteht für Mitgliedstaaten theoretisch der Raum, die Speicherfrist zwar für einen begrenzten, jedoch beliebigen Zeitraum zu verlängern. Unabhängig davon bleibt den Mitgliedstaaten bei der Wahl des Speicherzeitraums ein erheblicher Gestaltungsspielraum zwischen sechs und 24 Monaten. Um die Datensicherheit zu gewährleisten, verlangt Art. 7 Vorratsdatenspeicherungsrichtlinie ausdrücklich, dass geeignete technische und organisatorische Maßnahmen ergriffen werden sollen. Darüber hinaus ist auch die Löschpflicht nach dem Ablauf der Speicherfrist in Art. 7 Abs. d Vorratsdatenspeicherungsrichtlinie bestimmt.

Art. 8 Vorratsdatenspeicherungsrichtlinie fordert die Mitgliedstaaten dazu auf, die Daten so zu speichern, dass sie „unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können". Die Bestimmung der dabei erforderlichen Maßnahmen (die zur Anfrage befugten staatlichen Stellen, die Anfrage- und Weitergabenvoraussetzungen sowie die konkreten Verfahren) ist den Mitgliedstaaten überlassen, soweit die Anforderungen der Notwendigkeit und der Verhältnismäßigkeit eingehalten werden. Art. 13 Vorratsdatenspeicherungsrichtlinie verpflichtet die Mitgliedstaaten zudem dazu, über Rechtsbehelfe, Haftung und Sanktionen die Umsetzung sicherzustellen, gewährt ihnen bei deren Konkretisierung allerdings einen weiten Gestaltungsspielraum.

cc) Das Urteil des Europäischen Gerichtshofs

Unmittelbar nach der Verabschiedung der Vorratsdatenspeicherungsrichtlinie wurde von Irland eine Klage vor dem Europäischen Gerichtshof angestrengt. Die Klage bezog sich auf die Wahl der Rechtsgrundlage (Art. 95 EGV a. F., jetzt Art. 114 AEUV); es handelte sich also um eine rein formelle Rechtsfrage. Eine mögliche Verletzung der Grundrechte als Folge von mit der Vorratsdatenspeicherungsrichtlinie verbundenen Eingriffen in das Recht auf Privatsphäre wurde hingegen nicht adressiert. Obwohl die formelle Frage der Richtlinie auch rechtswissenschaftlich umstritten war, wies der Europäische Gerichtshof die Klage mit der Begründung ab, dass sich die Regelungen zur Vorratsdatenspeicherung

„unmittelbar auf das Funktionieren des Binnenmarkts auswirken[229] und die Vorratsdatenspeicherungsrichtlinie Tätigkeiten regelt, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind, damit sie die Diensteanbieter verpflichtet, die Daten, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet wurden, auf Vorrat zu speichern".[230]

Die Frage nach der Vereinbarkeit der Richtlinie mit den EU-Grundrechten wurde erst in der Vorabentscheidung behandelt, in der der irische *High Court* und der österreichische Verfassungsgerichtshof dem EuGH die Frage vorlegten, ob die Vorratsdatenspeicherung mit den EU-Grundrechten vereinbar sei. Der EuGH erklärte mit seinem Urteil vom 8. April 2014 die Vorratsdatenspeicherungsrichtlinie (VDS-RL 2006/24/EG) für ungültig, da sie in die durch die Europäischen Grundrechtecharta garantierten Grundrechte auf Achtung des Privat- und Familienlebens (Art. 7 GRC) und auf Schutz der personenbezogenen Daten (Art. 8 GRC) eingreift[231] und der Unionsgesetzgeber dabei die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit einhalten müsse.[232] Nach der Rechtsprechung des EuGH ist der mit der Vorratsdatenspeicherungsrichtlinie verbundene Eingriff in die oben genannten Grundrechte von großem Ausmaß und als besonders schwerwiegend anzusehen.[233] Da der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich

229 EuGH, C-301/06, 10.2.2009, Rn. 71.
230 EuGH, C-301/06, 10.2.2009, Rn. 82 f.
231 EuGH, C-293/12, 8.4.2014, Rn. 34 ff.
232 EuGH, C-293/12, 8.4.2014, Rn. 69.
233 EuGH, C-293/12, 8.4.2014, Rn. 37.

die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen,[234] wird von der Unionsregelung über die Vorratsdatenspeicherung gefordert, klare und präzise Regeln für ihre Tragweite und Anwendung festzulegen und einen wirksamen Schutz der personenbezogenen Daten vor Missbrauch, unberechtigtem Zugang und unberechtigter Nutzung sicherzustellen.[235]

In diesem Zusammenhang stellt die Vorratsdatenspeicherungsrichtlinie einen Eingriff in die in Art. 7 und 8 verankerten Grundrechte dar, der im Hinblick auf die Verhältnismäßigkeit deshalb nicht gerechtfertigt ist, weil in der Richtlinie keine Bestimmungen enthalten sind, die gewährleisten, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.[236] Die Richtlinie verpflichtet erstens dazu, in umfassender Weise die Daten aller Personen anlassunabhängig zu speichern, die elektronische Kommunikationsdienste nutzen.[237] Zweitens sieht die Richtlinie für einen Zugriff auf die Daten keine Einschränkung auf konkrete schwere Straftaten vor.[238] Abschließend liegt ein weiteres Problem in der Dauer der Vorratsdatenspeicherung begründet. Denn nach der Richtlinie sind die Daten ohne eine Unterscheidung bezüglich der Datenkategorien nach Maßgabe ihres etwaigen Nutzens oder anhand der betroffenen Personen für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern.[239] Der EuGH erklärte die EU-Richtlinie 2006/24/EG über die Vorratsdatenspeicherung für ungültig, weil die darin vorgeschriebene Verpflichtung von Telekommunikationsanbietern, die Daten ihrer Nutzer zu speichern, nicht auf das Notwendige beschränkt gewesen sei.

Auf der Ebene der EU wird zwar immer wieder die Forderung nach einer Wiedereinführung der Vorratsdatenspeicherung laut, jedoch besteht bis heute keine wirksame Vorschrift zur Vorratsdatenspeicherung. Während die Vorratsdatenspeicherungsrichtlinie nicht mehr in Kraft ist, ihre Umsetzungsgesetze in den Mitgliedstatten jedoch noch bestehen, gab es im Jahr 2016 zwei Vorabentscheidungsverfahren des EuGH, in denen dem Gerichtshof die Frage vorgelegt wurde, ob die nationalen Regelungen mit der EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) mit der Grundrechtecharta vereinbar seien. Die Grundlage

234 EuGH, C-293/12, 8.4.2014, Rn. 52.
235 EuGH, C-293/12, 8.4.2014, Rn. 54.
236 EuGH, C-293/12, 8.4.2014, Rn. 65.
237 EuGH, C-293/12, 8.4.2014, Rn. 58.
238 EuGH, C-293/12, 8.4.2014, Rn. 60.
239 EuGH, C-293/12, 8.4.2014, Rn. 63.

hierfür waren entsprechende Verfahren in Schweden und Großbritannien. In beiden Ländern sind Telekommunikationsunternehmen dazu verpflichtet, umfangreiche Verkehrs- und Standortdaten ihrer Nutzer systematisch auf Vorrat zu speichern und den Behörden zur Verfügung zu stellen. In den Vorabentscheidungsverfahren stellte der EuGH klar, dass eine nationale Regelung, die eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien zulässt, nicht mit dem Unionsrecht vereinbar sei.[240] Hiermit erteilte der EuGH einer allgemeinen Vorratsdatenspeicherung erneut eine deutliche Absage. Der Gerichtshof bestätigte zunächst, dass die Richtlinie 2002/58[241] den Mitgliedstaaten durchaus erlaubt, die grundsätzliche Verpflichtung zum Schutz der vertraulichen Kommunikation selbst auszugestalten und mit Ausnahmen zu versehen. Diese Ausnahmen dürften jedoch nicht zur Regel werden.[242] Nach der ständigen Rechtsprechung des EuGH seien die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige zu beschränken.[243] Außerdem wurden in Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte besonders hohe Anforderungen an die Rechtfertigung durch eine nationale Regelung gestellt, die die Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu Zwecken der Kriminalitätsbekämpfung vorsieht. Die Vorratsdatenspeicherung könne also allein zur Bekämpfung schwerer Straftaten herangezogen werden.[244] Zu diesem Zweck erlaube die Datenschutzrichtlinie eine gezielte Vorratsspeicherung von Daten, sofern diese hinsichtlich der Art der Daten, der betroffenen Kommunikationsmittel sowie der betroffenen Personen und der Dauer der Speicherung auf das absolut Notwendige beschränkt sei. Immerhin wurde festgestellt, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben hätten, mit Europarecht nicht vereinbar ist.

Im Anschluss daran hat der EuGH im Jahr 2020 zwei neue Urteile gesprochen.[245] Er hat hier zwar im Prinzip die im Jahr 2016 aufgestellten

240 EuGH, C-203/15, C-698/15, 21.12.2016.

241 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 (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 31. Juli 2002.

242 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 88 und 89.

243 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 96.

244 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 102 und 103.

245 EuGH, C-623/17, 6.10.2020 sowie EuGH, C-511/18, C-512/18 und C-520/18, 6.10.2020.

strengen Vorgaben an die Rechtmäßigkeit der Vorratsdatenspeicherung aufrechterhalten, jedoch Ausnahmen vom Verbot der Vorratsdatenspeicherung geschaffen. Die möglichen Ausnahmen wurden in einem Katalog in Ansatz gebracht und konkretisiert:

- Im Falle der gegenwärtigen oder vorhersehbaren ernsthaften Bedrohung der nationalen Sicherheit oder zur Bekämpfung schwerer Straftaten dürfen die Mitgliedstaaten per Gesetz die allgemeine und unterschiedslose Aufbewahrung von Verkehrs- und Standortdaten für einen auf das unbedingt erforderliche Maß beschränkten Zeitraum vorsehen. Dieser Zeitraum kann bei fortbestehender Bedrohung verlängert werden.
- Ein Gericht oder eine unabhängige Verwaltungsbehörde muss diese Maßnahmen jeweils überprüfen.
- Auch sei eine gezielte, zeitlich auf das unbedingt Notwendige beschränkte Speicherung von Verkehrs- und Standortdaten erlaubt, die auf der Grundlage objektiver und nicht diskriminierender Faktoren nach Maßgabe der betroffenen Personengruppen oder anhand eines geografischen Kriteriums begrenzt ist.
- Ebenso steht es den Mitgliedstaaten offen, eine allgemeine und unterschiedslose, wenn auch auf das unbedingt notwendige Maß beschränkte Vorratsspeicherung von IP-Adressen oder sogar eine allgemeine und unterschiedslose Vorratsspeicherung nur von Daten vorzunehmen, die sich auf die Identität der Telekommunikationsnutzer beziehen – hier sogar ohne Fristbindung.
- Schließlich hält der EuGH auch Regelungen zur Echtzeiterhebung von unter anderem Verkehrs- und Standortdaten für unionsrechtskonform, sofern diese Erhebung auf Personen beschränkt ist, bezüglich derer der begründete Verdacht besteht, dass sie in der einen oder anderen Weise an terroristischen Aktivitäten beteiligt sind, und wenn diese Datenerhebung einer vorherigen Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegt. In dringenden Fällen hat die Überprüfung unverzüglich zu erfolgen.

b) Das deutsche Umsetzungsgesetz

Die Vorratsdatenspeicherungsrichtlinie wurde in Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007 umgesetzt. Dies führte zu Änderungen des TKG, der StPO, des BKAG und

des JVEG. Der neu eingeführte § 113a TKG a. F.[246] verpflichtete die Anbieter öffentlich zugänglicher Telekommunikationsdienste (Abs. 1 Satz 1) dazu, Verkehrsdaten sechs Monate lang zu speichern, damit Auskunftsersuche der berechtigten Stellen unverzüglich beantwortet werden können (Abs. 9). Die Absätze 2 bis 4 sahen eine Vorratsdatenspeicherungspflicht der Anbieter von öffentlich zugänglichen Telefondiensten, Diensten elektronischer Post und Internetzugangsdiensten mit jeweils zu speichernden Datenkategorien vor. Inhaltsdaten waren dabei gemäß Abs. 8 von der Speicherverpflichtung ausgenommen. Zudem wurden gemäß § 113a Abs. 7 TKG die Betreiber von Mobilfunknetzen dazu verpflichtet, Daten über die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie ihre Hauptstrahlrichtung vorzuhalten. Betreffend die Qualität und den Schutz der gespeicherten Daten verlangte Abs. 10, die im Bereich der Telekommunikation erforderliche Sorgfaltspflicht zu beachten. Die im Rahmen der Vorratsdatenspeicherung gespeicherten Daten waren innerhalb eines Monats nach Ablauf der Frist zu löschen (Abs. 11).

Der § 113b TKG a. F. bestimmte die Zwecke, für die die nach § 113a gespeicherten Daten verwendet werden dürfen: zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes. Darüber hinaus enthielt der Artikel die Verlangens- und Übermittlungsvoraussetzungen der Daten.

Die Ermächtigungsgrundlage zur Verwendung der Daten im Rahmen der Strafverfolgung wurde mit § 100g StPO a. F. geschaffen. Es handelt sich um eine Erhebungsberechtigung der Daten. Dabei wurden die Voraussetzungen eines Zugriffs auf die Daten geregelt. Die Berechtigung lag vor, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer entweder 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat oder 2. eine Straftat mittels Telekommunikation begangen hat und der Zugriff für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes erforderlich ist. Außerdem ermächtigt § 20m BKAG dazu, auf die gemäß § 113a TKG a. F. gespeicherten Daten zuzugreifen.

246 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 dem 01. Januar 2008.

Die Umsetzung der Richtlinie in nationales Recht der EU-Mitgliedstaaten brachte in Ländern, die mit fortgeschrittenen nationalen Standards für den Schutz der Privatsphäre ausgestattet waren, eine Reihe verfassungsrechtlicher Herausforderungen mit sich. Die verfassungsrechtlichen Bedenken gegen das Umsetzungsgesetz wurden in der Literatur vor sowie nach der Einführung der Vorratsdatenspeicherung immer wieder hervorgehoben. In Übereinstimmung mit diesen Bedenken wurden zahlreiche Verfassungsbeschwerden eingereicht.[247] Denn der Bundesverfassungsgerichtshof entschied stets, dass das Recht auf informationelle Selbstbestimmung ein Grundrecht darstelle, das nach dem deutschen Grundgesetz geschützt sei.[248] Das Bundesverfassungsgericht beschloss im März 2010, also erst zwei Jahre nach der Einführung der Vorratsdatenspeicherung, über vielzählige Verfassungsbeschwerden. Nach seinem Urteil stellen die Vorschriften zur Vorratsdatenspeicherung einen Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG dar. Dieser gewährleistet das Fernmeldegeheimnis, das die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt. Folglich liege in der an die Telekommunikationsunternehmen gerichteten Anordnung, Telekommunikationsdaten zu erheben, zu speichern und an eine staatliche Stelle zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG vor.[249]

Die Vorratsdatenspeicherung sei zwar nicht schlechthin mit dem Grundgesetz unvereinbar[250] und auch nicht von vornherein unverhältnismäßig im engeren Sinne,[251] jedoch entsprächen die Regelungen zur Datensicherheit, zu den Zwecken und zur Transparenz der Datenverwendung sowie zum Rechtsschutz nicht den verfassungsrechtlichen Anforderungen.[252] Angesichts des Umfangs und der potenziellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände bedürfe es der gesetzlichen Gewährleistung besonders hoher Standards der Datensicherheit, also eng eingeschränkter sowie konkreter gesetzlicher Regelungen über die Voraussetzungen für die Datenverwendung und deren Umfang

247 Insgesamt legten 34.443 Bürger Verfassungsbeschwerde ein, vgl. *Krempl*, 34.443 Klageschriften gegen die Vorratsdatenspeicherung, heise online v. 29. Februar 2008, abrufbar unter: http://www.heise.de/-185285.html.

248 Siehe zum Beispiel BVerfGE 1, 6 (Mikrozensusurteil); BVerfGE 65, 1 (Volkszählungsurteil).

249 BVerfGE 125, 260 (309 ff.).

250 BVerfGE 125, 260 (316).

251 BVerfGE 125, 260 (318).

252 BVerfGE 125, 260 (347).

sowie hinreichender Vorkehrungen, die der Gesetzgeber zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen trifft.

Das Bundesverfassungsgericht erklärte somit die Regelungen zur Vorratsdatenspeicherung für verfassungswidrig und insoweit für nichtig. Der Gerichtshof hat also ausdrücklich auf eine Entscheidung gegen die Gültigkeit der Richtlinie über die Vorratsdatenspeicherung verzichtet und lediglich die innerstaatliche Gesetzgebung dazu aufgefordert, nationale Bestimmungen einzuführen, die die organisatorischen und technischen Schutzvorkehrungen für die Privatsphäre und für personenbezogene Daten in bestimmten Bereichen erhöhen.

c) Erneute Verabschiedung 2015

Nach der Entscheidung des Bundesverfassungsgerichts erklärten die deutsche Regierung und die Fraktionen der CDU/CSU und der SPD am Anfang des Jahres 2015 die Erforderlichkeit der Wiedereinführung der Vorratsdatenspeicherung. Daran anschließend legten beide Fraktionen dem Bundestag einen „Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“[253] vor. Obwohl Deutschland wegen der Entscheidung des EuGH nicht zur Umsetzung der Vorratsdatenspeicherungsrichtlinie verpflichtet ist, stimmte der Bundestag im Oktober 2015 für den Gesetzesentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, der am 16. Oktober 2015 vom Bundestag ohne wesentliche Änderungen beschlossen wurde. Am 6. November 2015 stimmte der Bundesrat dem Gesetz zu, am 10. Dezember 2015 wurde es vom Bundespräsidenten unterzeichnet und am 17. Dezember 2015 im Bundesgesetzblatt veröffentlicht. Damit wurde die Vorratsdatenspeicherung in Deutschland wiedereingeführt. Mit diesem Gesetz wurden einige Vorschriften vornehmlich in TKG und der StPO geändert und einige Vorgaben in das TKG und die StPO neu eingefügt.

Die wichtigste Änderung beim Gesetz zur Wiedereinführung der Vorratsdatenspeicherung besteht darin, dass der Gesetzgeber gemäß den Anforderungen des Bundesverfassungsgerichts hinsichtlich der Datensicherheit, des Zwecks sowie der Transparenz der Datenverwendung und des Rechtsschutzes die entsprechenden Regelungen zusammengestellt hat. Da-

253 BT-Drs. 18/5088; BT-Drs. 18/5171.

für wurden nicht nur die Straftaten, die die Datenerhebung ermöglichen, konkret ausgestaltet, sondern in §§ 113c bis 113g TKG auch die Vorkehrungen zur Datensicherheit und zur Transparenz der Datenverwendung getroffen. Im Detail wurden Regelungen zur Datenübermittlung nach § 113c TKG, zur Gewährleistung der Datensicherheit nach § 113d TKG, zur Verpflichtung der Protokollierung nach § 113e TKG, über den Anforderungskatalog zur Datensicherheit und Datenqualität nach § 113f TKG sowie zum Sicherheitskonzept nach § 113g TKG mit der Neuregelung des Gesetzes zur Vorratsdatenspeicherung geschaffen.

In der Literatur wurden gegen die Rechtmäßigkeit dieser neuen Regelungen vor allem in Bezug auf die Vereinbarkeit des § 113b TKG mit dem Unionsrecht allerdings schon früh Bedenken angemeldet.[254] Außerdem wurden gegen die wiedereingeführte Vorratsdatenspeicherung[255] wiederum mehrere Verfassungsbeschwerden eingereicht, die erste bereits am 18. Dezember 2015, also nur wenige Tage nach der Verabschiedung des neuen Vorratsdatenspeicherungsgesetzes.[256] Seitdem wurden kontinuierlich weitere Verfassungsbeschwerden gegen das Gesetz eingelegt.[257] Darüber hinaus wurde vom Internetverband Eco zusammen mit dem Münchener Internetprovider SpaceNet AG eine Klage vor dem Verwaltungsgericht Köln eingereicht. Die Klage richtete sich an das Verwaltungsgericht, weil vor dem Verwaltungsgericht, anders als bei Verfassungsbeschwerden, bei denen ein beschränkter Prüfungsrahmen angelegt würde, das gesamte

254 *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 538; *Derksen*, Unionsrechtskonforme Spielräume für anlasslose Speicherung von Verkehrsdaten?, NVwZ 2017, 1005.

255 Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 51, ausgegeben zu Bonn am 17. Dezember 2015.

256 1 BvR 3156/15.

257 1 BvR 17/16: Das Gesetz wurde hier deswegen kritisiert, weil die „anlasslos vorsorgliche Speicherung von Telekommunikationsdaten aller Bürger auf Grund ihrer Streuweite und Intensität einen ganz erheblichen Eingriff in das Fernmeldegeheimnis und den Schutz der Persönlichkeit bedeute."; 1 BvR 141/16; 1 BvR 229/16: Es wurde behauptet, dass die anlasslose Datenspeicherung bei den schrecklichen Anschlägen in Frankreich wirkungslos war; 1 BvR 2683/16: Hier wurde inhaltlich insbesondere der Punkt der Überwachungsgesamtrechnung aufgegriffen; 1 BvR 2840/16: Die Beschwerde führt den Punkt der Überwachungsgesamtrechnung weiter und warnt vor Gefahren, dass moderne Kommunikationsmittel wie Handys aufgrund der Vorratsdatenspeicherung zu elektronischen Fußfesseln würden. Die Beschwerde wurde ohne Begründung abgelehnt.

maßgebliche Recht berücksichtigt werden kann, also auch die seit 2016 geltende Rechtsprechung des EuGH.[258] Dabei wurde zugleich ein Eilantrag gestellt, der allerdings zunächst mit Beschluss vom 25. Januar 2017 abgelehnt wurde.[259] Gegen den Beschluss wurde nachfolgend erfolgreich Beschwerde vor dem Oberverwaltungsgericht für das Land Nordrhein-Westfalen eingelegt.[260] Das Oberverwaltungsgericht bestätigte damit die Unvereinbarkeit der deutschen Gesetzgebung mit dem Unionsrecht, speziell mit dem Art. 15 Abs. 1 der Richtlinie 2002/58[261] und die Verletzung der durch Art. 16 der Charta der Grundrechte der Europäischen Union geschützten unternehmerischen Freiheit der Antragstellerin.[262] Mit dem Beschluss wurde dem Eilantrag stattgegeben. Eine abschließende Klärung der grundlegenden verfassungsrechtlichen und unionsrechtlichen Fragestellungen sei allein in einem Hauptsacheverfahren möglich.[263] In der Folge setzte die Bundesnetzagentur die Pflicht zur Vorratsdatenspeicherung bis zur Entscheidung einer Klage im Hauptsacheverfahren aus.[264] Das Verwaltungsgericht Köln stellte danach in seiner Entscheidung fest, dass der nach § 113a TKG Verpflichtete gemäß § 113b TKG gerade nicht dazu verpflichtet ist, solche Daten gemäß § 113a TKG zu speichern. Die Entscheidung wurde damit begründet, dass die genannte Pflicht nicht mit Europarecht, speziell dem Art. 15 Abs. 1 der Richtlinie 2002/58, vereinbar sei. Da der EuGH feststellte, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben hätten, nicht mit Europarecht vereinbar sei,

258 SpaceNet und eco klagen gegen Vorratsdatenspeicherung. In: Süddeutsche Zeitung, 9. Mai 2017, abgerufen am 2. Februar 2019.
259 VG Köln, 9 L 1009/16, Beschluss am 25. Januar 2017.
260 OVG NRW, 13 B 238/17, Beschluss am 22. Juni 2017.
261 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 – Datenschutzrichtlinie für elektronische Kommunikation – (ABl. L 201, S. 37), zuletzt geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und Rates vom 25. November 2009 (ABl. L 337, S. 11) im Lichte der Grundrechte aus Art. 7, 8 und 11 sowie Artikel 52 Abs. 1 der Charta der Grundrechte der Europäischen Union. Vgl. EuGH, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 – Tele2 Sverige AB und Watson.
262 OVG NRW, 13 B 238/17, Rn. 33.
263 OVG NRW, 13 B 238/17, Rn. 88.
264 *Holland*, Bundesnetzagentur setzt Vorratsdatenspeicherung aus, heise online v. 28. Juni 2017, abrufbar unter: https://www.heise.de/-3757527.html.

regelte das deutsche Gesetz in §§ 113a und 113b TKG dies nach Ansicht des VG Köln rechtswidrig.[265]

Rein formell gesehen war die Vorratsdatenspeicherung damit nicht abgeschafft, sondern lediglich ihre Umsetzung bis zur Schaffung der notwendigen Rechtssicherheit aufgeschoben.[266] Die Entscheidungen des Bundesverfassungsgerichts über die aktuellen Gesetze zur Vorratsdatenspeicherung bleiben abzuwarten. Das Gericht stellte die grundsätzliche Rechtmäßigkeit der Vorratsdatenspeicherung fest, bemängelte jedoch das Datenschutzniveau der Vorratsdatenspeicherungsgesetze a. F. und erklärte das Gesetz daher für nichtig. Das Bundesverfassungsgericht stellte in seiner Entscheidung zum Datenschutz fest, dass die Rechtmäßigkeit deutscher Gesetze, die nicht auf eine EU-Richtlinie zurückzuführen und nicht durch Unionsrecht determiniert sind, grundsätzlich nicht an Unionsrecht zu messen ist, und dass eine Vorlage an den EuGH damit grundsätzlich ausscheidet.[267] Das Gericht hat in seinem Beschluss vom 8. Juni 2016 eine Aussetzung des Vollzugs der §§ 113a und 113b TKG abgelehnt, da der in der bloßen Speicherung der Verkehrsdaten liegende Nachteil für Freiheit und Privatheit der Einzelnen erst durch einen Abruf der Daten zu einer irreparablen Grundrechtsbeeinträchtigung führen könne.[268] Auch sei eine Aussetzung des Vollzugs von §§ 100g, 101a und 101b StPO mit der Begründung nicht geboten, dass der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Verkehrsdaten i. S. d. § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht habe. Diese lassen das Gewicht der durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen.[269] Bis zur eventuellen Ungültigkeitserklärung des Bundesverfassungsgerichts bleiben die aktuellen Gesetze zur Vorratsdatenspeicherung jedenfalls gültig. Es ist folglich bedeutsam, den aktuellen rechtlichen Inhalt eingehend zu betrachten, damit man die Konstruktion der Gesetze und deren Datenschutzniveau einsehen und die eventuellen Bedenken einschätzen kann.

---

265 VG Köln, 9 K 7417/17, Rn. 87.

266 *Levenshtein*, Vorratsdatenspeicherung auf Eis gelegt, industr.com v. 29. Juni 2017, abrufbar unter https://www.industr.com/-2296251.

267 BVerfGE 125, 260 (306 f.).

268 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240, Rn. 26.

269 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240, Rn. 20 und 22.

2. Aktuelle Rechtslage

Vom Schutz des Fernmeldegeheimnisses sind nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation erfasst. Das Recht auf Fernmeldegeheimnis verhindert, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten mit Überwachung rechnen müssen.[270] § 100g StPO enthält dabei Eingriffsermächtigungen zugunsten der Strafverfolgungsbehörden. Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015[271] bildet den rechtlichen Rahmen der neuen Vorratsdatenspeicherung. Es handelt sich dabei um ein „Doppeltürmodell",[272] das die konkreten Verantwortlichkeiten und Voraussetzungen mit einem Zweischritt in zwei verschiedene Gesetze aufspaltet: auf der einen Seite steht die Aufnahme eines Gesetzes über die Erhebung, Speicherung und Übermittlung ins TKG (Speicherpflicht und Bestimmung der Verantwortlichen, Art der zu speichernden Daten, Speicherdauer und Übermittlungsberechtigung) sowie auf der anderen Seite die Aufnahme eines Gesetzes über die Datenerhebung in die StPO (Zugriffsvoraussetzungen für den Abruf durch die Strafverfolgungsbehörden). Hiermit wurden die §§ 113a–g TKG neu eingeführt und der § 100g StPO geändert. Im Folgenden soll die aktuelle Rechtslage unter der neu eingeführten Vorratsdatenspeicherung untersucht werden. Um den Sinn der Einführung der Vorratsdatenspeicherung richtig zu erfassen, ist es zunächst notwendig, die Definition der Begriffe „Bestandsdaten" und „Verkehrsdaten" zu verdeutlichen. Des Weiteren ist zu erklären, welche Daten vor der Einführung der Vorratsdatenspeicherung gespeichert und unter welchen Voraussetzungen diese zu Ermittlungszwecken verwendet werden durften. Anschließend sollen die Vorschriften zur Vorratsdatenspeicherung vorgestellt, die Änderungen nach der Einführung der Vorratsdatenspeicherung konkret analysiert und die Datenspeicherung und -verwendung vor und nach der Neueinführung der Vorratsdatenspeicherung miteinander verglichen werden.

Die Rechtsgrundlagen der Speicherung, Verarbeitung und Nutzung personenbezogener Daten durch die Telekommunikationsdiensteanbieter sollen wie folgt skizziert werden: Nach dem Bundesdatenschutzgesetz

---

270 BVerfGE 100, 313 (359).
271 BGBl. I 2015, S. 2218, in Kraft seit dem 18. Dezember 2015.
272 *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 113.

(BDSG), das bezweckt, den Einzelnen vor einer Beeinträchtigung in seinem Persönlichkeitsrecht durch den Umgang mit seinen personenbezogenen Daten zu schützen, sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten. Sie sind nur auf Basis eines Erlaubnistatbestandes – auf Grundlage eines Erlaubnistatbestandes im BDSG, einer anderen Rechtsvorschrift oder einer Einwilligung des Betroffenen – zulässig.[273] Das BDSG fordert außerdem Datenvermeidung und -sparsamkeit.[274] Die Grundidee ist, dass bei der Datenverarbeitung nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind.[275]

Auf dieser Rechtsgrundlage sind §§ 95–98 TKG für die Datenerhebung und -verwendung von Telekommunikationsunternehmen einschlägig; ihre Ausnahmen bilden §§ 111–113 TKG. Daten, die nach dem TKG durch die Telekommunikationsdiensteanbieter gespeichert und verwendet werden können, lassen sich in Bestandsdaten und Verkehrsdaten (auch als Verbindungsdaten bezeichnet) unterteilen. Bestandsdaten sind nach § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, während es sich nach § 3 Nr. 30 TKG um Verkehrsdaten handelt, wenn Daten bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Standortdaten bilden einen Unterfall von Verkehrsdaten.

Bestandsdaten dürfen ursprünglich nach § 95 TKG nur erhoben und verwendet werden, soweit dies zur Vertragserfüllung erforderlich ist. Die Erhebung und die Verwendung von Bestandsdaten dürfen also nicht erlaubt werden, wenn dies nicht für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erforderlich ist. § 111 TKG bildet jedoch eine bedeutende Ausnahme, nach der Anbie-

273 § 4 BDSG.

274 § 3a BDSG: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."

275 Das Konzept wurde gesetzlich erstmals in § 3 Abs. 4 TDDSG im Juli 1997 normiert: „Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen."

ter, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken und dabei Rufnummern oder andere Anschlusskennungen vergeben, für die Auskunftsverfahren nach §§ 112 und 113 TKG bestimmte Informationen zu erheben und unverzüglich zu speichern haben.[276] Es handelt sich dabei um eine Speicherpflicht der Anbieter von Telefondiensten, Mobilfunktelefonen und Diensten elektronischer Postfächer.[277] Nach § 111 TKG sind die folgenden Bestandsdaten auch dann zu erheben und zu speichern, wenn sie für betriebliche Zwecke nicht erforderlich sind:

1. Rufnummer (stattdessen die Kennungen der elektronischen Postfächer bei Diensten des elektronischen Postfaches),
2. Name und Anschrift des Anschlussinhabers (statt des Anschlussinhabers des Inhabers des elektronischen Postfachs bei elektronischen Postfachdiensten),
3. das Geburtsdatum,
4. die Anschrift des Anschlusses bei Festnetzanschlüssen bzw. die Gerätenummer des überlassenen Mobilfunktelefons,
5. das Datum des Vertragsbeginns sowie
6. die bisher noch nicht erhobenen Daten, sofern dem Anbieter eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

Auf gespeicherte Bestandsdaten darf im automatisierten Verfahren nach §§ 111, 112 TKG (dann nur auf die in § 111 Abs. 1 TKG genannten Daten) oder im Rahmen eines manuellen Auskunftsverfahrens nach § 113 TKG zugegriffen werden. §§ 112, 113 TKG bestimmen jeweils das automatisierte oder manuelle Auskunftsverfahren einschließlich der ersuchenden Stellen und der Ersuchungsformen. Dabei ist nach § 113 Abs. 5 TKG dafür Sorge

---

276 Vgl. *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministerium der Justiz, S. 21: „Der Begriff der ‚kleinen Vorratsdatenspeicherung' bietet sich an, da auch hier Daten auf Vorrat gespeichert werden, die für die eigentlichen Zwecke der Anbieter nicht erforderlich sind, die aber die Verfolgung von Ordnungswidrigkeiten nach dem TKG oder dem UWG ermöglichen sollen oder die für die Erledigung der Auskunftsersuchen der in § 112 Abs. 2 TKG genannten Stellen benötigt werden."

277 An den Daten, die bei elektronischen Postfachdiensten zu speichern sind, wird Kritik geübt, dass es sich um Telemedienbestandsdaten handele, so dass die Vorschrift grundsätzlich im falschen Gesetz enthalten und zudem durch die Verweisungstechnik auch nicht besonders normenklar sei; vgl. *Brunst*, Anonymität im Internet, S. 396 m. w. N.

zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in § 113 Abs. 2 TKG genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird. Eine Strafverfolgungsbehörde darf nach § 100j Abs. 1 Satz 1 StPO Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangen. Die Zugriffsregelung in der StPO (§ 100j StPO) wird zu einer Übermittlungspflicht für Telekommunikationsdiensteanbieter (§ 113 Abs. 4 TKG) konkretisiert. Wird Auskunft über Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, verlangt, darf dies nach § 100j Abs. 3 Satz 1 StPO nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Es besteht bei Gefahr im Verzug die Möglichkeit, die Anordnung auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen mit einer Nachholung der gerichtlichen Entscheidung zu treffen (§ 100j Abs. 3 Satz 2 und 3 StPO). Über die Auskunftserteilung ist die betroffene Person mit Ausnahme des Vorliegens einer Unterbleibens- oder Zurückstellungsvoraussetzung der Benachrichtigung zu benachrichtigen (§ 100j Abs. 4 StPO).

§ 96 TKG bildet einen Erlaubnistatbestand der Erhebung und der Verwendung von Verkehrsdaten. Es setzt die Erforderlichkeit zu den im 2. Abschnitt des TKG genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen voraus. Nach § 96 TKG dürfen die folgenden Verkehrsdaten erhoben werden:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. der Beginn und das Ende der jeweiligen Verbindung, die übermittelten Datenmengen, soweit die Entgelte davon abhängen,
3. der vom Nutzer in Anspruch genommene Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende und – soweit Entgelte davon abhängen – die übermittelten Datenmengen sowie
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Nach §§ 96, 97 TKG werden die Verkehrsdaten erhoben und verwendet, um einen technisch korrekten Verbindungsaufbau zu ermöglichen und die notwendigen Grundlagen für eine korrekte Entgeltermittlung und

-abrechnung zu schaffen. Die Abrechnungsdaten dürfen bis sechs Monate nach Versendung der Rechnung gespeichert werden, für die Abrechnung nicht erforderliche Daten hingegen sind unverzüglich zu löschen (§ 97 Abs. 3 TKG). Standortdaten als ein Unterfall von Verkehrsdaten dürfen außerdem nach § 98 TKG 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. Auf die Verkehrsdaten darf auf Grundlage des § 100g StPO zugegriffen werden. Vor der Vorratsdatenspeicherung durfte aber auf die nach §§ 96, 97 TKG gespeicherten Verkehrsdaten nur zugegriffen werden, soweit die Daten zum Zeitpunkt eines Auskunftsersuchens noch vorhanden waren.[278] Denn es bestand damals keine Regelung über Datenspeicherungs- und Datenübermittlungspflichten.

Auf dieser Rechtsgrundlage kommt es vor, dass Telekommunikationsdiensteanbieter unabhängig von §§ 96, 97 und 98 TKG nach der Vorratsdatenspeicherung (§§ 113a–g TKG) verpflichtet sind, die darin genannten Verkehrsdaten zu speichern und unter bestimmten Voraussetzungen an eine befugte Stelle zu übermitteln. Im Folgenden soll näher darauf eingegangen werden, wer welche Verkehrsdaten für welche Dauer nach §§ 113a–g TKG i. V. m. § 100g StPO zu speichern hat und unter welchen Voraussetzungen die Strafverfolgungsbehörden zu Ermittlungszwecken auf diese Daten zugreifen dürfen. Dabei soll die Eingriffsintensität der Vorratsdatenspeicherung untersucht und anschließend bewertet werden, ob es Regelungen für flankierende Maßnahmen gibt, die die Eingriffsintensität der Vorratsdatenspeicherung mildern sollen, und ob diese Regelungen hinreichend sind.

a) Zu speichernde Daten

Es sind Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, die im Rahmen der Vorratsdatenspeicherung dazu verpflichtet sind, bestimmte Verkehrsdaten für die unverzügliche Beantwortung auf Auskunftsersuchen der berechtigten Stellen zu speichern (§ 113a Abs. 1 Satz 1 TKG). Dies sind Telekommunikationsdiensteunternehmen i. S. d. § 3 Nr. 6 lit. a) TKG, also nicht bloß bei der Übermittlung von Daten

278 § 100g StPO a. F. Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001, BGBl. 2001, I. Nr. 73, S. 3879.

mitwirkende Unternehmen – etwa Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen (Hotspots in Hotels, Restaurants und Cafés).[279] Es handelt sich dabei vielmehr um Erbringer öffentlich zugänglicher Telefon- sowie Internetzugangsdienste. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, aber nicht alle der nach Maßgabe der §§ 113b bis 113g TKG zu speichernden Daten selbst erzeugt oder verarbeitet, hat sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß § 113b TKG von einem anderen gespeichert werden, und er hat der Bundesnetzagentur auf deren Verlangen hin unverzüglich mitzuteilen, wer diese Daten speichert (§ 113a Abs. 1 Satz 2 TKG).

Die jeweils bei den unterschiedlichen Telekommunikationsdiensten zu speichernden Daten regelt § 113b Abs. 2 Satz 1 TKG.

Bei den Erbringern von Telefondiensten sind die folgenden Daten zu speichern:

1. Die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. Datum und Uhrzeit von Beginn und Ende der Verbindung,
3. Angaben zu dem genutzten Dienst,
4. bei mobilen Telefondiensten die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss (IMSI), die internationale Kennung des anrufenden und des angerufenen Endgerätes (IMEI) sowie Datum und Uhrzeit der ersten Aktivierung des Dienstes, wenn Dienste im Voraus bezahlt wurden,
5. bei Internet-Telefondiensten auch die IP-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht und für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe. Das heißt, die Speicherpflicht wird mit § 113b Abs. 2 Satz 2 Nr. 2 TKG auf nicht entgegengenommene oder erfolglose Anrufe ausgedehnt. Bei der Übermittlung einer Nachricht sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

279 Erbringer zeichnen sich dadurch aus, dass den Kunden regelmäßig ein eigener, in der Regel auf unbestimmte Dauer angelegter Telekommunikationsanschluss zur selbständigen Verwendung überlassen wird, vgl. BT-Drs. 18/5088, S. 37.

Als eine bemerkenswerte Regelung muss § 113b Abs. 3 Nr. 1 TKG bezeichnet werden, der insbesondere die Pflicht zur Speicherung der dynamischen IP-Adresse für Erbringer öffentlich zugänglicher Internetzugänge regelt. Dynamische IP-Adressen, die sowohl nach Einschätzung des EuGH als auch nach der des BGH als personenbezogene Daten gelten und folglich besonders zu schützen sind,[280] müssen von den Telekommunikationsanbietern im Sinne der Vorratsdatenspeicherung gespeichert werden. Für Bestandsdatenauskünfte zu dynamischen IP-Adressen darf auf nach § 113b TKG gespeicherte Verkehrsdaten zurückgegriffen werden. Die Speicherung der dynamischen IP-Adresse eröffnet neue Möglichkeiten für die Verfolgungsbehörden im Rahmen der Ermittlung von Straftätern.[281] Bei den Erbringern von Internetzugangsdiensten sind die folgenden Daten zu speichern:

1. Die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung sowie
3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse.

Laut Gesetzgeber sollen die „eindeutige Kennung des Anschlusses" sowie die „zugewiesene Benutzerkennung" der Praxis die Rückverfolgung und Identifizierung der Quelle eines Kommunikationsvorgangs besser ermöglichen.[282] Die Gesetzesbegründung schweigt sich jedoch darüber aus, was diese Begrifflichkeiten bedeuten, die neben der dynamischen IP-Adresse beiordnend geregelt sind.

Im Fall der Nutzung mobiler Telefondienste oder der mobilen Nutzung von öffentlich zugänglichen Internetzugangsdiensten sind darüber hinaus zusätzlich auch Standortdaten bei Beginn aller Mobiltelefonate sowie einer

280 EuGH, C-582/14, 19.10.2016; BGH, VI ZR 135/13, 16.05.2017.

281 Trotz enormer praktischer Wichtigkeit dynamischer IP-Adressen im Zusammenhang mit Cybercrime (vgl. den Abschlussbericht BKA 2011 – Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu „Mindestspeicherfristen", S. 5) wehrten sich Dienstunternehmen teilweise auch explizit gegen die Abfrage der dynamischen IP-Adresse. Dies geschah unter Verweis auf die ungeklärte Rechtsgrundlage (vgl. *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ, 2016, 113, 116 m. w. N.), weil das Dienstunternehmen die IP-Adressen nicht für Abrechnungszwecke bei der heutigen Verbreitung von Flatrate-Tarifen benötigt.

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

mobilen Internetnutzung, also die konkreten Bezeichnungen der Funkzellen, zu speichern.

Der Kommunikationsinhalt, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen nicht gespeichert werden (§ 113b Abs. 5 TKG). Wird auch der Inhalt bei einer Kurz-, Multimedia- oder ähnlichen Nachricht gespeichert, muss die ganze Nachricht von Speicherungsgegenständen ausgenommen werden.[283] Die Daten, die nach der Vorratsdatenspeicherung durch die Erbringer öffentlich zugänglicher Telekommunikationsdiente für Endnutzer gespeichert werden müssen, greifen weit über den Speicherumfang vor der Vorratsdatenspeicherung hinaus. Der Telekommunikationsanbieter ist daher dazu verpflichtet, eine zeitlich längere und datenmäßig umfangreichere Speicherung vorhandener Daten vorzunehmen als dies abrechnungstechnisch erforderlich wäre. Dies führt zu einer relativ langen Speicherung einer enormen Menge an Daten getrennt von §§ 95–98 TKG.[284]

Tabelle 1: Synopse der grundsätzlich abfragbaren Datenarten gem. §§ 96 und 113a TKG[285]

§ 96 TKG	**§ 113b TKG**
Abs. 1 Satz 1 Nr. 1: die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung personenbezogene Berechtigungskennungen die Kartennummer bei Verwendung von Kundenkarten	Abs. 2 Satz 1 Nr. 1: – die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses Abs. 2 Satz 1 Nr. 4: bei mobilen Telefondiensten – die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss

283 *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 535.

284 Zum Vergleich der gemäß § 96 TKG zu speichernden Daten mit den gemäß § 113a TKG zu speichernden Daten siehe Tabelle 1.

285 Vgl. *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-

	– die internationale Kennung des anrufenden und des angerufenen Endgerätes Abs. 2 Satz 1 Nr. 5: im Fall von Internet-Telefondiensten – auch die *Internetprotokoll-Adressen* des anrufenden und des angerufenen Anschlusses – zugewiesene *Benutzerkennungen* Abs. 3 Nr. 1: im Fall von Internetzugangsdiensten – die dem Teilnehmer für eine Internetnutzung zugewiesene *Internetprotokoll-Adresse* Abs. 3 Nr. 2: im Fall von Internetzugangsdiensten – eine *eindeutige Kennung* des Anschlusses, über den die Internetnutzung erfolgt – eine zugewiesene *Benutzerkennung*
Abs. 1 Satz 1 Nr. 2: den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit Abs. 1 Satz 1 Nr. 4: die Endpunkte von festgeschalteten Verbindungen und deren Beginn und Ende nach Datum und Uhrzeit	Abs. 2 Satz 1 Nr. 2: – Datum und Uhrzeit von Beginn und Ende der Verbindung Abs. 2 Satz 1 Nr. 4 c): bei im Voraus bezahlter mobiler Telefondienste – Datum und Uhrzeit der ersten Aktivierung des Dienstes Abs. 2 Satz 2 Nr. 2: – *Datum und Uhrzeit von unbeantworteten* oder wegen eines Eingriffs

Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 29.

	des Netzwerkmanagements *erfolglosen Anrufen* Abs. 3 Nr. 3: im Fall von Internetzugangsdiensten – Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der jeweils geltenden Zeitzone.
Abs. 1 Satz 1 Nr. 3: den vom Nutzer in Anspruch genommenen Telekommunikationsdienst	Abs. 2 Satz 1 Nr. 3: – Angaben zum genutzten Telefondienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können
Abs. 1 Satz 1 Nr. 2: soweit die Entgelte davon abhängen, *die übermittelten Datenmengen* Abs. 1 Satz 1 Nr. 4: soweit die Entgelte davon abhängen, *die übermittelten Datenmengen*	
Abs. 1 Satz 1 Nr. 5: sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten	Abs. 2 Satz 2 Nr. 1: bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht *– die Zeitpunkte der Versendung und des Empfangs der Nachricht*
Abs. 1 Satz 1 Nr. 1: bei mobilen Anschlüssen auch die Standortdaten	Abs. 4 Satz 1 und 2: – bei mobilen Telefondiensten die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt werden – im Fall der mobilen Nutzung öffentlich zugänglicher Internetzugangsdienste die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle

§ 113b Abs. 6 TKG bestimmt hingegen auch die Daten, die nach § 113b TKG nicht gespeichert werden dürfen. Nach der Entscheidung des Bundesverfassungsgerichts, der zufolge es verfassungsrechtlich geboten ist, zumindest für einen engen Kreis auf besondere Vertraulichkeit angewiesener Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen,[286] sieht § 113b Abs. 6 TKG vor, dass Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zugrunde liegen, nicht im Sinne der Vorratsdatenspeicherung gespeichert werden dürfen. Demgegenüber sind die Daten derer, die anderen als den oben genannten Verschwiegenheitsverpflichtungen unterliegen, zu speichern. Nach § 100g Abs. 4 StPO ist die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO, auch in Verbindung mit Abs. 3 Satz 2, die sich gegen eine der in § 53 Abs. 1 Satz 1 Nr. 1 bis 5 genannten Personen – z. B. Geistliche, Verteidiger des Beschuldigten, Rechtsanwälte – richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden.

Das TKG erfordert keinen Anlass zur Speicherung der in § 113b genannten Daten, sondern sieht die vorrätige Speicherung von Verkehrsdaten *aller* Personen vor, um das Vorhandensein der erforderlichen Daten für eventuelle Anfragen sicherzustellen. Konsequenterweise macht § 113b TKG die Speicherung der hier genannten Verkehrsdaten nicht davon abhängig, ob ein Zusammenhang mit schweren Straftaten besteht bzw. ob die Daten geeignet sind, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Zweckbeschränkung besteht ausschließlich für die Verwendung der Daten gemäß § 113c TKG. Der Europäische Gerichtshof erteilt einer anlasslosen Speicherung von Daten, ohne dass jene Personen einen Anlass dazu gegeben haben, also eine Absage.[287] Nach der Datenschutzrichtlinie 2002/58 ist eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien nicht mit Unionsrecht vereinbar.[288] In diesem Zusammenhang hat das OVG Münster im Wege der einstweiligen Anordnung festgestellt, dass der dort klagende Internetzugangsdiensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens nicht dazu verpflichtet ist, die in § 113b Abs. 3 TKG genannten Verkehrsdaten zu speichern, weil diese Pflicht nicht mit

286 BVerfGE 125, 260 (334).
287 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 105.
288 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 108.

Unionsrecht vereinbar ist.[289] Trotz der Entscheidung des EuGH werden in Deutschland im Rahmen der Vorratsdatenspeicherung bestimmte Verkehrsdaten aller Personen anlasslos gespeichert. Insoweit baut der deutsche Gesetzgeber nicht darauf auf, dass der EuGH die eine oder andere Variante der Vorratsdatenspeicherung für unzulässig erklärt, sondern dass in der Entscheidung des EuGH die Gründe, die die Richtlinie zur Vorratsdatenspeicherung und eine entsprechende nationalstaatliche Umsetzung grundrechtswidrig machen würden, *in Summe* aufgezählt werden.[290] Der Gesetzgeber hält weiterhin an der Anlasslosigkeit der Speicherung fest, wobei er gleichzeitig verschiedene Forderungen umsetzt: Nicht alle verfügbaren Daten werden gespeichert (z. B. nicht die URL oder die Inhaltsdaten); eine Zweckverwendung nach § 113c TKG darf nur bei Verdacht besonders schwerer Straftaten erfolgen.[291] Es ist umstritten, ob die Eingriffsintensität der anlasslosen Speicherung einer Vielzahl von Daten durch die anderen Faktoren, also durch strenge Abrufmechanismen, gemindert werden kann.[292]

b) Zugriff auf Daten

Der Gesetzgeber wollte die Eingriffsintensität der anlasslosen Speicherung von Daten durch strenge Abrufmechanismen flankieren. Eine anlasslose Speicherung rechtfertigt sich vor allem über die enge Zweckbegrenzung des § 113c TKG zur Verfolgung besonders schwerer Straftaten im Rahmen der Ermittlung. Die nach § 113b TKG gespeicherten Daten dürfen nur für die drei folgenden Zwecke verwendet werden (§ 113c TKG): Erstens dürfen die Speicherungsverpflichteten die Daten an eine Strafverfolgungsbehörde übermitteln, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt. Dazu dient § 100g StPO als eine Ermächtigungsgrundlage. Zweitens

289 OVG NRW, 13 B 238/17, Beschluss am 22. Juni 2017.

290 Der Gesetzgeber spricht insoweit von einer „Vielzahl von Kritikpunkten, die in ihrer Gesamtbetrachtung die Unverhältnismäßigkeit bedeuteten“ und einer „Kombination“ von langer Speicherdauer ohne Differenzierung nach Datenart, vgl. BT-Drs. 18/5088, S. 23.

291 *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 115.

292 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.

dürfen die Daten an eine Gefahrenabwehrbehörde der Länder übermittelt werden. Die Übermittlung soll sich dabei aus einer gesetzlichen Bestimmung begründen, die der Behörde eine Erhebung der in § 113b TKG genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt. Der Erbringer öffentlich zugänglicher Telekommunikationsdienste darf schließlich die Daten zum Ersuchen der Bestandsdaten über eine IP-Adresse gemäß § 113 Abs. 1 Satz 3 TKG verwenden.[293] Eine Verwendung für andere Zwecke als die oben genannten ist nach § 113c Abs. 2 TKG explizit verboten. Es soll angesichts des Forschungsziels dieser Arbeit nachfolgend nur in die Verwendung des Strafverfolgungszweckes Einblick genommen werden. Dabei ermächtigt § 100g StPO die Strafverfolgungsbehörden mit dem bestimmten Straftatbezug unter einigen Voraussetzungen, Verkehrsdaten zu erheben.

§ 100g StPO unterscheidet mehrere Arten von Auskünften: § 100g Abs. 1 Satz 1 regelt die allgemeine Auskunft über die gemäß § 96 TKG gespeicherten Daten zur Aufklärung einer Straftat von erheblicher Bedeutung bzw. mittels Telekommunikation. § 100g Abs. 1 Satz 3 StPO betrifft speziell die Erhebung von Standortdaten als einer Sonderform von Verkehrsdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit, die unabhängig von der Vorratsdatenspeicherung gespeichert werden – weil die Vorratsdatenspeicherung auf den Zugriff auf die bereits beim Anbieter vorsorglich gespeicherten Daten abzielt. § 100g Abs. 2 StPO normiert den strafprozessualen Zugriff auf die gemäß § 113b TKG gespeicherten Verkehrsdaten (Vorratsdatenspeicherung) und § 100g Abs. 3 StPO gestaltet schließlich eine Funkzellenabfrage, also die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten.

Die unabhängig von der Vorratsdatenspeicherung nach § 96 TKG gespeicherten Verkehrsdaten dürfen nur dann erhoben werden, wenn bestimmte Tatsachen einen Verdacht begründen, dass eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat (Verdacht auf schwere Straftaten, die eine Telekommunikationsüberwachung auslösen können) oder eine Straftat mittels Telekommunikation begangen wurde, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Für die Straftat mittels Telekommunikation wird gefordert, dass die Erforschung des Sach-

293 BVerfGE 125, 260 (340 f.); dazu kritisch *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich in der Vorratsdatenspeicherung, S. 13 ff.

verhalts auf andere Weise aussichtslos wäre. Für den Verdacht bezüglich einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Abs. 2 StPO bezeichneten Straftat (Straftatenkatalog) oder einer Straftat mittels Telekommunikation ist zur Erhebung von Verkehrsdaten die Erforderlichkeit und die Verhältnismäßigkeit vorauszusetzen. Für die Erhebung von Verkehrsdaten beim Verdacht einer Straftat mittels Telekommunikation wird außerdem die Subsidiarität der Aussichtslosigkeit auf andere Weise gefordert. Die Erhebung von Standortdaten darf nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur zum Ziel der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes des Beschuldigten geschehen. Dies beschränkt sich zudem auf den Fall des § 100g Abs. 1 Satz 1 Nr. 1 StPO, also darauf, dass bestimmte Tatsachen einen Verdacht begründen, dass jemand eine Straftat von auch im Einzelfall erheblicher Bedeutung begangen hat.

Die nach § 113b TKG im Rahmen der Vorratsdatenspeicherung gespeicherten Daten dürfen gemäß § 100g Abs. 2 StPO unter relativ strengen Voraussetzungen erhoben werden.[294] Bei der Erhebung von Verkehrsdaten gemäß Art. 100g Abs. 2 StPO wird davon ausgegangen, dass die Daten tatsächlich gespeichert wurden, sodass nur die Verkehrsdaten der Vergangenheit erfasst werden. Für die Erhebung zukünftig anfallender Verkehrsdaten oder zur Erhebung in Echtzeit ist diese Vorschrift hingegen nicht einschlägig. Gegenstand der Auskunft nach Abs. 2 sind die Verbindungsdaten nach § 113b Abs. 2 TKG bezüglich Telefondiensten, diejenigen nach § 113b Abs. 3 TKG bezüglich Internetzugangsdiensten und die Standortdaten nach § 113b Abs. 4 TKG bezüglich Funkzellen.[295] Retrograde Standortdaten dürfen nach Ablauf der Überleitungsvorschrift des § 12 EGStPO zum 29. Juli 2017 nur auf Grundlage von Abs. 2 i. V. m. § 113b TKG erhoben werden.[296] Da die Speicherverpflichtung nach den §§ 113b bis 113e und 113g spätestens ab dem 1. Juli 2017 zu erfüllen sind, dürfen die nach § 96 Abs. 1 Satz 1 Nr. 1 TKG gespeicherten Standortdaten auf der Grundlage des § 100g Abs. 1 a. F. erhoben werden, damit in der Zwischenzeit ein Abruf gespeicherter Standortdaten möglich bleibt.

Für die Erhebung der nach Vorratsdatenspeicherung gespeicherten Daten genügt ein einfacher Verdacht einer besonders schweren Straftat im Sinne des Abs. 2 Satz 2. Den Tatverdacht müssen aber bestimmte Tatsa-

294 Über die unterschiedlichen Voraussetzungen je nach der Datenart siehe unten Tabelle 2.

295 Vgl. *Bär*, BeckOK-TKG, § 113b, Rn. 5 ff., 15, 16 ff.

296 BGH, Ermittlungsrichter, 03.08.2017 – 1 BGs 237/17.

chen begründen.[297] Dieser muss also objektivierbar und konkret auf den Einzelfall bezogen sein.[298] Mit Blick auf das Gewicht des Grundrechtseingriffs durch den Zugriff auf die nach § 113b TKG gespeicherten Daten muss sich der Verdacht auf eine hinreichende Tatsachenbasis stützen und mehr als nur unerheblich sein.[299] Für die Erhebung dieser Daten schließt § 100g Abs. 2 StPO einen bestimmten Straftatenkatalog an. Nur wenn ein Verdacht begründet wird, dass eine der in § 100g Abs. 2 StPO aufgezählten Straftaten begangen wurde und die Tat auch im Einzelfall besonders schwer wiegt, dürfen die nach § 113b TKG gespeicherten Daten erhoben werden. Der Katalog ist dabei abschließender Natur. Im Deliktskatalog in Abs. 2 Satz 2 spiegelt sich die Erforderlichkeit der Ermittlung über den Zugriff auf die Vorratsdaten. Der Gesetzgeber hat im Hinblick auf die hohe Grundrechtsrelevanz des Abrufs verpflichtend gespeicherter Daten den Katalog im Vergleich zu dem in § 100a Abs. 2 Satz 2 deutlich reduziert.[300] Dieser Katalog stößt wegen seines Umfangs aber oft auf Kritik: Einerseits seien manche Deliktsbereiche vom Katalog des § 100g Abs. 2 Satz 2 nicht erfasst, obwohl polizeiliche Strukturermittlungen ohne Vorratsdatenspeicherung kaum sinnvoll durchgeführt werden können, z. B. im Bereich der Organisierten Kriminalität der gewerbsmäßige Betrug gemäß § 263 Abs. 3 Satz 2 Nr. 1 StGB.[301] Andererseits seien einige Delikte konsequenterweise aus dem Katalog des Absatzes 2 Satz 2 zu streichen, weil für die Delikte kaum eine kriminalistische Notwendigkeit des Zugriffs auf die Vorratsdaten besteht, wie etwa beim besonders schweren Fall des Landfriedensbruchs nach § 125a StGB.[302] Es wird außerdem der Vorwurf erhoben, dass der Bezug auf die im Katalog des Absatzes 2 Satz 2 aufgeführten Grundtatbestände zu Beginn eines Ermittlungsverfahrens in der Regel nicht festgestellt wird und sich auch die Möglichkeit eines (besonders) schweren Falls erst im Laufe des Ermittlungsverfahrens herausstellen kann;

297 Vgl. BVerfGE 107, 299; *Bruns*, KK-StPO, § 100a Rn. 30; *Hauck*, LR-StPO, § 100a Rn. 42.

298 *Hauck*, LR-StPO, § 100g Rn. 11.

299 BGH, NStZ-RR 2016, 346, Rn. 9.

300 BT-Drs. 18/5088, S. 32.

301 *Hauck*, LR-StPO, § 100g Rn. 48. Ebenso für eine maßvolle Erweiterung des Katalogs Münch ZRP 2015 130; *Herrmann*, Vorratsdatenspeicherung ist notwendig, in: *Hanns Seidel Stiftung* (Hrsg.), Politische Studien Bd. 458 im Fokus „Frei oder Sicher? – brauchen wir die Vorratsdatenspeicherung?" 14 (17); ablehnend aber *Leutheusser-Schnarrenberger*, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, DuD 2014, 589, 590 f.

302 *Hauck*, LR-StPO, § 100g, 49; Deutscher Richterbund (Stellungnahme), 2 f.

obwohl Verkehrsdaten als Ermittlungsansatz vor allem zu Beginn eines Ermittlungsverfahrens von großer Bedeutung sind.[303]

Wie in § 100a StPO ist der Einsatz dieser Maßnahme in § 100g Abs. 2 nur zulässig, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Im Vergleich mit den Erfolgsaussichten anderer Maßnahmen ist bei gleichen Voraussetzungen die schonendere Maßnahme zu ergreifen.

Außerdem erfordern die Auskünfte nach Abs. 2, dass die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Bei staatlichen Grundrechtseingriffen ist ungeachtet der vom Gesetz vorgesehenen generellen Eingriffsvoraussetzungen die Überprüfung der verfassungsrechtlichen Verhältnismäßigkeit grundsätzlich vorausgesetzt. § 100g Abs. 2 erwähnt trotz des allgemeinen Grundsatzes der Verhältnismäßigkeit zusätzlich ein angemessenes Verhältnis zur Bedeutung der Sache. Die Bedeutung dieser Klausel erklärt der Gesetzgeber in seinem Gesetzesentwurf jedoch nicht. Die Klausel ist als eine zweite, gesonderte Verhältnismäßigkeitsprüfung im Licht der Anforderungen des EuGH zu verstehen, wonach der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen.[304] Bei der Angemessenheitsprüfung im Rahmen der ursprünglichen Verhältnismäßigkeitsprüfung ist eine Abwägung sämtlicher Vor- und Nachteile der Maßnahme vorzunehmen. Eine Maßnahme ist also nur dann verhältnismäßig im engeren Sinn, wenn die Nachteile, die mit der Maßnahme verbunden sind, nicht völlig außer Verhältnis zu den Vorteilen stehen, die sie bewirkt. In der Klausel des angemessenen Verhältnisses zur Bedeutung der Sache ist daher eine Garantie zu sehen, die bei der hohen Eingriffsintensität einer vorrätigen Speicherung personenbezogener Daten vieler Personen einen wirksamen Schutz dieser Daten vor Missbrauch sowie vor jedem unbefugten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglicht.[305] Es lässt sich feststellen, dass den möglichen Bedenken hinsichtlich der hohen Eingriffsintensität der Maßnahme, des drohenden Vertrauensverlusts in die

303 *Hauck*, LR-StPO, § 100g, 50.
304 EuGH, Urteil vom 8. April 2014 in den Rechtssachen C-293/12, C-594/12.
305 So *Schmitt*, Strafprozessordnung, § 100g Rn. 35; *Bär*, BeckOK-StPO, § 100g Rn. 18; *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terrorabwehr, S. 257.

Strafjustiz und der Missbrauchsanfälligkeit[306] mit der Verhältnismäßigkeit der Maßnahme in besonderem Maße begegnet wird.

§ 100g StPO enthält darüber hinaus in Abs. 3 eine Sonderregelung zu der Funkzellenanfrage. Bei einer solchen Abfrage werden alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren.[307] Die Maßnahme kommt in Betracht, wenn Kennungen nicht bekannt sind, aber Erkenntnisse dafür vorliegen, dass in bestimmten räumlichen Bereichen mit Hilfe des Mobilfunks Telekommunikation betrieben wurde, deren Daten für die Identifizierung noch unbekannter Täter[308] von Bedeutung sein könnten. Da Gegenstand dieser Maßnahme alle Verkehrsdaten sind, die in einer bestimmten Funkzelle angefallen sind, ist die Gefahr, dass Telekommunikationsdaten völlig unbeteiligter Personen erhoben werden, sehr groß. Der Gesetzgeber begegnet daher den vielen Bedenken[309] hinsichtlich der Verfassungsmäßigkeit, insbesondere der Verhältnismäßigkeit der Maßnahme, mit engen Voraussetzungen: Während bei Funkzellenabfragen[310] nach § 100g Abs. 3 StPO die Erhebung von nach § 96 Abs. 1 TKG gespeicherten Verkehrsdaten zulässig ist, wenn die Voraussetzungen des § Abs. 1 Satz 1 Nr. 1 StPO vorliegen, die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert ist, müssen für eine Erhebung der nach § 113b TKG gespeicherten Verkehrsdaten für eine Funkzellenabfrage die Voraussetzungen des § 100g Abs. 2 erfüllt sein. Beim Einsatz der Maßnahme ist ferner

306 *Zimmer*, Zugriff auf Internetzugangsdaten: Unter besonderer Berücksichtigung der Verhältnismäßigkeit einer verdachtsunabhängigen Vorratsdatenspeicherung, 2012, S. 195 ff.

307 BT-Drs. 18/5088, S. 32.

308 *Hilger*, Gesetzgebungsbericht: §§ 100g, 100h StPO, die Nachfolgeregelungen zu § 12 FAG, GA 2002, 228, 230; *Wohlers/Demko*, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241, 247.

309 Vgl. *Singelnstein*, Verhältnismäßigkeitsanforderungen für strafprozessuale Ermittlungsmaßnahmen – am Beispiel der neueren Praxis der Funkzellenabfrage, JZ 2012, 601, 601 ff. m. w. N.; *Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, 593, 602: „enorme Streubreite".

310 Die Funkzellenabfrage ist nach § 100g Abs. 3 Satz 1 StPO die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten und damit nicht auf die Erhebung von Standortdaten beschränkt (BT-Drs. 18/5088, S. 32).

davon auszugehen, dass überhaupt eine Verbindung zustande gekommen ist.[311]

Für den Zugriff auf die Daten, die der Anbieter der Telekommunikationsdienste gespeichert hat, werden grundsätzlich bestimmte Grundrechtseingriffsvoraussetzungen vorgesehen, etwa einfacher Verdacht einer Straftat von erheblicher Bedeutung bzw. einer besonders schweren Straftat, Subsidiaritätsklauseln und der Grundsatz der Verhältnismäßigkeit. Um die Daten, auf die die Strafverfolgungsbehörden zugreifen dürfen, zu erweitern, hat der Gesetzgeber die Zugriffsermächtigung verpflichtend gespeicherter Daten gemäß § 113b TKG eingeführt, wobei im Lichte der hohen Eingriffsintensität dieser Maßnahme die Voraussetzungen verstärkt wurden. So werden angesichts der schon weit im Vorfeld der Regelung vorgebrachten Bedenken und der Tatsache, dass die Maßnahme eine Vielzahl von Daten Unbeteiligter erfasst, zusätzlich eine Einschränkung auf die abschließenden Katalogtaten und eine besondere Verhältnismäßigkeitsprüfung gefordert.

§ 101a StPO, der unter dem neuen Vorratsdatenspeicherungsgesetz neu eingefügt wurde, regelt den Richtervorbehalt. Danach bedarf es für den Zugriff auf die Verkehrsdaten unter Berufung auf § 100g StPO grundsätzlich einer gerichtlichen Anordnung auf Antrag der Staatsanwaltschaft (§ 100b StPO). In den Fällen einer Auskunft über die nach § 96 TKG gespeicherten Daten besteht bei Gefahr im Verzug die Möglichkeit der Anordnung durch die Staatsanwaltschaft, wobei die Anordnung der Staatsanwaltschaft binnen drei Werktagen von einem Gericht bestätigt werden soll. Diese Möglichkeit wird in den Fällen des § 100g Abs. 2 StPO (Auskunft über die Vorratsdaten: Vorratsdatenspeicherung), auch in Verbindung mit § 100g Abs. 3 Satz 2, ausgeschlossen. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt (§ 100a Abs. 3 StPO). In der Entscheidung sind anzugeben: der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet; die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes; Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen.

311 Für die Auskunft über die Daten nur auf Bereitschaft geschalteter Endgeräte gilt § 100a bzw. § 100i StPO.

Die Verwendung personenbezogener Daten, die durch Maßnahmen nach § 100g Abs. 2 StPO, auch in Verbindung mit § 100g Abs. 3 Satz 2, erhoben wurden, muss unter Zweckbindung stehen. Diese Zweckbindung bestimmt § 101a Abs. 4 StPO. Die Daten dürfen also in anderen Strafverfahren zur Aufklärung einer Straftat, auf Grund derer eine Maßnahme nach § 100g Abs. 2, auch in Verbindung mit § 100g Abs. 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden. Ihre Übermittlung darf zu Zwecken der Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes geschehen.

Damit fordert § 100g StPO für die Erhebung der nach § 96 TKG gespeicherten Daten bei einem Verdacht für eine in § 100a bezeichnete Straftat auch im Einzelfall von erheblicher Bedeutung oder für eine Straftat mittels Telekommunikation die Erforderlichkeit der Maßnahme und die Verhältnismäßigkeit zwischen der Maßnahme und der Bedeutung der Sache. Für eine Datenanfrage bezüglich einer Straftat mittels Telekommunikation fügt das Gesetz jedoch die Anforderung „wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre" hinzu. Die Erhebung von Standortdaten kann nicht nur bei der Erforderlichkeit für die Erforschung des Sachverhalts, sondern auch bei der Erforderlichkeit für die Ermittlung des Aufenthaltsortes des Beschuldigten ergriffen werden. Für die Funkzellenanfrage wird darüber hinaus gefordert, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Im Gegensatz dazu wird die Erhebung der nach § 113b TKG gespeicherten Daten an engere Voraussetzungen geknüpft: wenn bestimmte Tatsachen den Verdacht für eine in § 100g Abs. 2 bezeichnete Straftat begründen und die Tat auch im Einzelfall besonders schwer wiegt und soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Trotz dieser Unterschiede in den Anforderungen haben die Maßnahmen nach § 100a und § 100g Abs. 1 bis 3 einige Gemeinsamkeiten. Für sämtliche Auskünfte nach § 100g ist der Anfangsverdacht einer bestimmten Straftat vorausgesetzt. Es genügt ein einfacher Verdacht, der auf bestimmten Tatsachen beruhen muss, also objektivierbar und konkret auf den

Einzelfall bezogen sein muss,[312] einer Straftat von erheblicher Bedeutung bzw. einer besonders schweren Straftat. Insofern entspricht die gesetzliche Regelung der in § 100a. Alle drei Auskunftsformen des § 100g fordern eine Subsidiarität, indem die Maßnahme für die Erforschung des Sachverhalts und/oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich sein muss oder die Erforschung bzw. Ermittlung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Mit den Subsidiaritätsvorschriften betont § 100g ebenso wie die Telekommunikationsüberwachung in § 100a den Verhältnismäßigkeitsgrundsatz noch einmal, weil der Eingriff schon rechtswidrig wäre, wenn der verfolgte Zweck mit für die Betroffenen weniger belastenden Mitteln erreichbar wäre.[313] Darüber hinaus gelten der Richtervorbehalt, die Benachrichtigungspflicht und die Anordnung nur gegen den Beschuldigten oder gegen Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt, ebenso wie in § 100a auch für die Auskunftsformen in § 100g.

Der Straftatkatalog nach § 100g Abs. 2 StPO ist aber angesichts der Eingriffsintensität enger als die Katalogtaten nach § 100a Abs. 2 gefasst. Nach der Entscheidung des Bundesverfassungsgerichts, die besagt, dass ein Datenabruf zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt und eine Generalklausel oder lediglich der Verweis auf Straftaten von erheblicher Bedeutung hingegen nicht ausreichen würden, hat der Gesetzgeber einen Katalog besonders schwerer Straftaten für die Erhebung der nach § 113b TKG gespeicherten Daten geschaffen.

Die Verfahren der Datenübermittlung, die auf Verlangen einer zuständigen Stelle erfolgen, bestimmen die Rechtsverordnung nach § 110 Abs. 2 TKG und die Technische Richtlinie nach § 110 Abs. 3 TKG (§ 113c TKG).

312 BT-Drs. 14/7008, S. 6; *Wohlers/Demko*, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241, 245.

313 BT-Drs. 14/7008, S. 7; BVerfGE 107, 299.

Tabelle 2: Voraussetzungen je nach gespeicherter Datenart

	Straftatbezug	Voraussetzungen
Die nach § 96 TKG gespeicherten Daten	Alt. 1: Verdacht auf eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	– soweit dies für die Erforschung des Sachverhaltes erforderlich ist und – die Erhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht.
	Alt. 2: Verdacht auf eine Straftat mittels Tele-kommunikation	– soweit dies für die Erforschung des Sachverhaltes erforderlich ist, – die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht und – die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.
Die nach § 113b gespeicherten Daten	Verdacht auf eine der in § 113b Abs. 2 Satz 2 bezeichneten *besonders schweren Straftaten*, die auch im Einzelfall besonders schwer wiegt	– soweit die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und – die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht.
künftig anfallende Standortdaten oder in Echtzeit	Verdacht für eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	soweit dies für die Erforschung des Sachverhaltes erforderlich ist

Funkzellenanfrage: alle in einer Funkzelle angefallenen Verkehrsdaten	Verdacht für eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	– soweit die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht und – die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.
§ 100a	Verdacht für eine in § 100g Abs. 2 StPO bezeichnete *schwere* Straftat	– wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthalts-ortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

c) Löschungspflicht

Im TKG ist nicht nur die Speicherungsermächtigung bestimmter Daten durch den Diensteanbieter für die unverzügliche Beantwortung von Auskunftsersuchen berechtigter Stellen geregelt. Vielmehr bestimmt es auch deutlich die Löschungspflicht dieser Daten zum Schutz personenbezogener Daten durch das Datensparsamkeitsprinzip entsprechend der verfassungsrechtlichen Verpflichtung, die Daten nach Ablauf der Höchstdauer der Speicherfrist zu löschen.[314] Während die alte Regelung zur Vorratsdatenspeicherung eine einheitliche Speicherdauer der Daten von sechs Monaten vorsah, fordert § 113b TKG n. F. zwei unterschiedliche Möglichkeiten der Speicherfrist der nach §§ 113a und b TKG gespeicherten Daten. Auf diese Weise berücksichtigt die Vorschrift die Unterschiede hinsichtlich Umfang und Bedeutung der durch die Vorratsdatenspeicherung geschaffenen Datenbestände. Daten nach § 113b Abs. 2 und 3 sind von Erbringern öffentlich zugänglicher Telefondienste sowie Internetzu-

314 BVerfGE 125, 260 (333).

gangsdienste für zehn Wochen zu speichern, Standortdaten nach Abs. 4 hingegen für vier Wochen. Die Löschung muss gemäß § 113b Abs. 9 TKG unverzüglich, spätestens jedoch innerhalb einer Woche nach Ablauf der Speicherfristen erfolgen. Dabei muss die Löschung irreversibel sein. Darunter versteht man, dass sichergestellt werden muss, dass auf den Speichermedien physikalisch keine Fragmente oder gar noch die gesamten Daten vorhanden sind und etwa mit technischen Mitteln wieder rekonstruiert werden können. Die irreversible Löschung der Daten muss daher nach dem Stand der Technik gewährleistet werden, weshalb dazu in den Anforderungskatalog nach § 113f entsprechende Regelungen aufzunehmen sein werden.[315] Die Löschung ist gemäß § 113e Abs. 1 Satz 1 aktenkundig zu machen.

Anders als bei der Rasterfahndung ist bei der Vorratsdatenspeicherung die Löschung oder die Rückgabe der vom Diensteanbieter übermittelten Daten nicht vorgesehen. Der Grund hierfür liegt darin, dass für die Verwendung der nach § 100g StPO i. V. m. § 113b TKG gewonnenen Daten eine enge Zweckbegrenzung vorgesehen ist. Dabei stellt § 113c Abs. 1 Nr. 1 und 2 TKG die Voraussetzung der Datenübermittlung dar und § 113c Abs. 2 TKG schließt die Datenverwendung für andere als die in § 113c Abs. 1 TKG genannten Zwecke ausdrücklich aus. In diesem Zusammenhang muss eine hinreichende Erörterung der Eignung der Maßnahme zur Ermittlung im Anordnungsbeschluss angegeben sein.

d) Mitteilungspflicht

Nach § 101a Abs. 6 StPO sind die Beteiligten der betroffenen Telekommunikation grundsätzlich von der Erhebung der Verkehrsdaten nach § 100g StPO zu benachrichtigen, weil § 100g grundsätzlich eine offene Ermittlungsmaßnahme darstellt.[316] Da Verkehrsdaten in der Praxis regelmäßig bereits zu einem frühen Zeitpunkt erhoben werden, zu dem die Ermittlungen noch heimlich geführt werden, ist allerdings davon auszugehen, dass der offene Zugriff die Ausnahme bleiben wird.[317] Im Hinblick auf den Inhalt und die Zuständigkeit für die Benachrichtigung gelten nach Abs. 6 Satz 2 Halbsatz 1 die Regelungen des § 101 Abs. 4 Satz 2 bis 5 und Abs. 5 bis 7 entsprechend. Nach § 101 Abs. 7 StPO ist auf die Möglichkeit

315 *Bär*, BeckOK-TKG, § 113b TKG Rn. 26.
316 BT-Drs. 18/5088, S. 36.
317 *Gercke*, HK-StPO, § 101a Rn. 25 m. w. N.

nachträglichen Rechtsschutzes und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung muss sich insbesondere auf die Anordnung und Durchführung einschließlich der Dauer und des Umfangs der Maßnahme erstrecken. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen (§ 101 Abs. 4 Satz 3 StPO). Die Benachrichtigung kann zurückgestellt werden, soweit sie den Untersuchungszweck gefährden würde (§ 101 Abs. 5 Satz 1 StPO). Das Unterbleiben oder die Zurückstellung der Benachrichtigung bedarf dabei der Anordnung des zuständigen Gerichts (§ 101a Abs. 6 Satz 2 Nr. 1 und 2 StPO). Die Zurückstellung der Benachrichtigung ist erstmalig auf höchstens zwölf Monate zu befristen und kann durch das Gericht verlängert werden. Das Gericht kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden (§ 101 Abs. 6 StPO). Insoweit bedarf es einer Begründung im Einzelfall.[318]

318 BT-Drs. 18/5088, S. 36.