Der Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsdaten

Zugleich eine Anmerkung zum Urteil des 2. Senats des Bundesverfassungsgerichts vom 2. März 2006 – 2 BvR 2099/04

Von Wiss. Assistentin Dr. **Janique Brüning**,
Hamburg*

I. Einleitung

Straftäter verwenden in zunehmendem Maße moderne Kommunikationstechnologien bei der Planung und Begehung von Straftaten. Für die Strafverfolgungsbehörden besteht daher ein erhebliches Bedürfnis im Rahmen ihrer Ermittlungstätigkeit auf die entsprechenden Kommunikationsdaten zugreifen zu können. Von besonderem Interesse sind dabei die sog. Verbindungsdaten, die zwar nicht den Kommunikationsinhalt wiedergeben, jedoch Aufschluss über die einzelnen Kommunikationsvorgänge und gegebenenfalls über den Aufenthaltsort des Kommunikationsteilnehmers geben können.¹

Das BVerfG hat sich in jüngerer Zeit (4. Februar 2005 und 2. März 2006) zweimal mit der rechtlichen Bewertung des Zugriffs auf sog. Verbindungsdaten befasst. Zentraler Entscheidungsgegenstand war jeweils die Frage, ob die bei einem Kommunikationsteilnehmer gespeicherten Verbindungsdaten in den Schutzbereich des Fernmeldegeheimnisses i.S.d. Art. 10 Abs. 1 GG fallen. Die Beantwortung dieser Frage ist für die Effektivität der strafrechtlichen Ermittlungspraxis von erheblicher Tragweite. Ursache hierfür ist, dass Ermächtigungen für Eingriffe in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis gem. Art. 10 Abs. 2 GG einer gesetzlichen Grundlage bedürfen, die die Grenzen des Eingriffs festlegt.² In der StPO sind nur zwei entsprechende Ermächtigungsgrundlagen i.S.d. Art. 10 Abs. 2 StPO normiert: Die §§ 100a, 100b StPO legitimieren die Überwachung und Aufzeichnung der Telekommunikation, wohingegen die §§ 100g, 100h StPO eine Ermächtigungsgrundlage für die Erlangung von Auskünften der Telekommunikationsanbieter über Verbindungsdaten darstellen. Beide strafprozessualen Grundrechtseingriffe verlangen als Eingriffsvoraussetzung eine Straftat von erheblicher Bedeutung³ und unterliegen einem Richtervorbehalt. Liegt Gefahr im Verzug vor, so besteht lediglich für die Staatsanwaltschaft eine Anordnungskompetenz, nicht hingegen für ihre Ermittlungspersonen.

* Die Verf. ist wissenschaftliche Assistentin an der Bucerius Law School am Lehrstuhl von Prof. Dr. *Frank Saliger*. Für wertvolle Hinweise dankt sie Herrn RiAG *Marc Wenske*.

¹ *Gusy*, NStZ 2003, 399 (400). Allerdings nimmt auch die Bedeutung „kommunikationsunabhängiger“ Daten in Strafverfahren zu. Dies gilt vor allem für Wirtschafts- und Strafverfahren, bei denen regelmäßig große Datenbestände als Beweismittel zu sichern sind, vgl. *Kemper*, NStZ 2005, 538.

² BVerfG NJW 2004, 2213 (2215).

³ Nach § 100g Abs. 1 S. 1 2. Fall StPO ist sogar als Eingriffsvoraussetzung ausreichend, wenn der Verdacht besteht, dass die Straftat mittels eines Endgerätes begangen wurde.

Stellt der Zugriff auf die Kommunikationsdaten, die sich im Herrschaftsbereich des Kommunikationsteilnehmers befinden, einen Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis dar, so müssen die soeben dargestellten Voraussetzungen erfüllt sein, insbesondere muss regelmäßig eine Straftat von erheblicher Bedeutung gegeben sein. Ist der Zugriff hingegen kein Eingriff in das Fernmeldegeheimnis, so bedarf es für diesen Zugriff keiner Ermächtigungsgrundlage, die die Anforderungen des Art. 10 Abs. 2 GG wahrt. Diese rechtliche Wertung entspricht der in der strafrechtlichen Ermittlungspraxis vorherrschenden Ansicht. Dies hat zur Folge, dass die Vorschriften der Sicherstellung bzw. Beschlagnahme gem. § 94 StPO bei einem Zugriff auf die beim Kommunikationsteilnehmer gespeicherten Kommunikationsdaten in Anspruch genommen werden.⁴ § 94 Abs. 2 StPO lässt – im Gegensatz zu den §§ 100a, 100b bzw. §§ 100g, 100h StPO – lediglich einen einfachen Tatverdacht als Eingriffsvoraussetzung ausreichen. Zwar steht auch die Beschlagnahme gem. § 98 Abs. 1 StPO unter einem Richtervorbehalt. Bei Gefahr im Verzug sind allerdings – anders als bei den §§ 100a, 100b bzw. §§ 100g, 100h StPO – neben der Staatsanwaltschaft auch ihre Ermittlungspersonen gem. § 152 GVG anordnungsbefugt.

Vor dem Hintergrund dieser Rechtsfolgen wandte sich die 3. Kammer des 2. Senats am 4. Februar 2005 gegen die bis dahin geltende Ermittlungspraxis und erklärte, dass die im Herrschaftsbereich des Beschuldigten aufgefundenen Verbindungsdaten als Einzelverbindungsdaten in Rechnungen oder als gespeicherte Daten im Mobiltelefon in den Schutzbereich des Art. 10 Abs. 1 GG fallen, und forderte als Eingriffsvoraussetzung für einen Zugriff auf diese Daten eine Straftat von erheblicher Bedeutung.⁵ Das hier zu besprechende Urteil des 2. Senats vom 2. März 2006 hält an dieser Rechtsauffassung nicht mehr fest.

II. Die Entscheidung des BVerfG

Hintergrund der aktuellen Senatsentscheidung ist folgender Sachverhalt: Eine Richterin wendet sich mit ihrer Verfassungsbeschwerde gegen die wegen des Verdachts der Verletzung von Dienstgeheimnissen durchgeführte Durchsuchung ihrer Privatwohnung und ihres Dienstzimmers sowie gegen die Beschlagnahme ihres Computers und Mobiltelefons. Ihr wurde zur Last gelegt, Informationen aus einem Ermittlungs-

⁴ Vgl. dazu *Bär*, in: *Wabnitz/Janowsky* (Hrsg.), *Handbuch des Wirtschafts- und Strafstrafrechts*, 2. Aufl. 2004, 25. Kap., Rn. 36 ff.; *Nack*, in: *Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz*, 5. Aufl. 2003, § 94 Rn. 4.

⁵ BVerfG NJW 2005, 1637 (1639).

verfahren bezüglich „terroristischer“ Straftaten an einen befreundeten Journalisten weitergegeben zu haben, der diese später veröffentlichte. Nachdem das AG Karlsruhe den Antrag der Staatsanwaltschaft auf Erlass eines entsprechenden Durchsuchungsbeschlusses zunächst mangels Tatverdachts negativ beschied, erließ das LG Karlsruhe auf Beschwerde der Staatsanwaltschaft fünf Monate später (!) den Durchsuchungsbeschluss. Das erhoffte Ermittlungsergebnis, mittels der Sicherstellung und Auswertung der Verbindungsdaten nachweisen zu können, dass die beschwerdeführende Richterin in dem tatrelevanten Zeitraum Kontakt zu dem befreundeten Journalisten hatte, wurde nicht erreicht. Entsprechende Verbindungsdaten wurden nicht gefunden. Da das LG Karlsruhe einen Antrag auf (nachträgliche) Feststellung der Rechtswidrigkeit der Strafverfolgungsmaßnahmen abgelehnt hat, erhebt die Richterin nunmehr erfolgreich Verfassungsbeschwerde.

Nachdem die Kammerentscheidung vom Februar 2005 im Schrifttum auf massive Kritik gestoßen war,⁶ geht der *Senat* in Beantwortung der Grundsatzfrage des Urteils nunmehr einstimmig davon aus, dass der Zugriff auf die in einem Computer gespeicherten Daten sowie auf die Einzelverbindungsdaten eines Mobiltelefons keinen Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis darstellt. Zwar konstatiert der *Senat* zunächst, dass der Schutzbereich des Fernmeldegeheimnisses auch die näheren Umstände des Fernmeldevorgangs umfasse, der Schutz also grundsätzlich nicht aufhöre, wenn der Kommunikationsvorgang beendet sei. Gleichwohl erstrecke sich der Schutzbereich des Art. 10 Abs. 1 GG nicht auf solche Daten, die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeichert seien. In diesem Fall bestehe die spezifische Gefahr des räumlich distanzierter Kommunikationsvorgangs nicht, da der Kommunikationsteilnehmer, die im eigenen Herrschaftsbereich gespeicherten Daten beherrsche und Vorkehrungen gegen den ungewollten Zugriff Dritter – einschließlich des Staates – treffen könne.⁷ Zwar merkt das BVerfG an, dass eine endgültige Löschung der gespeicherten Daten regelmäßig nicht ohne eine spezielle Software möglich sei. Diesen Bedenken begegnen die Richter allerdings mit dem Argument, dass dem Kommunikationsteilnehmer jedenfalls die Möglichkeit der physischen Zerstörung eröffnet sei.⁸ Im Übrigen komme es auch nicht darauf an, ob der Kommunikationsteilnehmer die endgültige Löschung herbeiführen könne. Denn für die Bestimmung des Schutzbereiches von Art. 10 Abs. 1 GG – vor allem in Abgrenzung zu Art. 2 Abs. 1 GG – sei vielmehr die Vergleichbarkeit mit den sonst in der Privatsphäre gespeicherten Daten maßgeblich.⁹ In beiden Fällen seien die spezifischen Risiken, die aufgrund der Einwirkungsmöglichkeiten während des Übertragungsvorgangs bestünden, nicht gegeben, so dass es

eines Schutzes für die im Herrschaftsbereich gespeicherten Daten durch Art. 10 Abs. 1 GG nicht bedürfe.

Allerdings nimmt das BVerfG an, dass die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Daten nicht ausschließlich durch das in Art. 13 Abs. 1 GG normierte Recht auf Unverletzlichkeit der Wohnung geschützt werden, sondern darüber hinaus vom Schutz des Rechts auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erfasst seien. Das Recht auf informationelle Selbstbestimmung könne selbstständig als unbenanntes Freiheitsrecht neben den speziellen Grundrechten Anwendung finden, wenn nur eine partielle Überschneidung mit dem Schutzbereich eines speziellen Freiheitsrechts vorliege.¹⁰ Werde auf personenbezogene Kommunikationsdaten in der Wohnung des Betroffenen zugegriffen, so erschöpfe sich der Eingriff nicht in der Überwindung der räumlichen Grenzen der Privatsphäre. Vielmehr erfahre die Maßnahme aufgrund des Zugriffs auf die Kommunikationsdaten eine weitere grundrechtsrelevante Qualität.¹¹ Durch die zunehmende Digitalisierung der persönlichen Kommunikation und der Abwicklung von Alltagsgeschäften würden vermehrt Verbindungsdaten anfallen. Auf diese Weise erhöhe sich der Aussagegehalt der Verbindungsdaten, so dass im Ergebnis Rückschlüsse möglich seien, die an die Qualität eines Persönlichkeitsprofils heranreichten.¹² Das Recht auf informationelle Selbstbestimmung stehe aus diesem Grund in einem Ergänzungsverhältnis zu Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.¹³ „Damit wird der besonderen Schutzwürdigkeit der Telekommunikationsumstände Rechnung getragen und die Vertraulichkeit räumlich distanzierter Kommunikation auch nach Beendigung des Übertragungsvorgangs gewahrt.“¹⁴

Ferner stellt das BVerfG klar, dass die §§ 94 ff. StPO eine hinreichende Ermächtigungsgrundlage für die Sicherstellung und Beschlagnahme von Datenträgern und den hierauf enthaltenen Daten darstellen. Der 2. *Senat* nimmt dabei Bezug auf seinen Beschluss vom 12. April 2005¹⁵. Die §§ 94 ff. StPO verwirklichten die verfassungsrechtlichen Vorgaben, die an eine gesetzliche Eingriffsermächtigung für eine Beschränkung des Rechts auf informationelle Selbstbestimmung zu stellen seien. Das Gebot der Normenklarheit und das Prinzip der Verhältnismäßigkeit seien gewahrt. Zwar seien die §§ 94 ff. StPO ursprünglich für Eingriffe in körperliche Gegenstände konzipiert worden. Aufgrund der Normierung der §§ 98a ff. StPO sei jedoch deutlich geworden, dass der Gesetzgeber nunmehr grundsätzlich von der Beschlagnahmefähigkeit von Daten ausgehe. Im Übrigen gestatte der Wortsinn des § 94 StPO eine Einbeziehung nicht-körperlicher Gegenstände. Schließlich bestimme die Ermächtigungsgrundlage den Verwendungszweck der erhobenen Daten bereichsspezifisch und präzise. Dies ergebe sich aus dem Normzusammen-

⁶ Bär, MMR 2005, 523 ff.; Götz, Kriminalistik 2005, 300 ff.; Hauschild, NStZ 2005, 339 ff.; R. Günther, NStZ 2005, 485 ff.

⁷ BVerfG ZIS 2006, 243 ff. Rn. 73.

⁸ BVerfG ZIS 2006 (Fn. 7) Rn. 78.

⁹ BVerfG ZIS 2006 (Fn. 7) Rn. 79.

¹⁰ BVerfG ZIS 2006 (Fn. 7) Rn. 84.

¹¹ BVerfG ZIS 2006 (Fn. 7) Rn. 84.

¹² BVerfG ZIS 2006 (Fn. 7) Rn. 91.

¹³ BVerfG ZIS 2006 (Fn. 7) Rn. 88.

¹⁴ BVerfG ZIS 2006 (Fn. 7) Rn. 89.

¹⁵ BVerfG NJW 2005, 1917 ff.

hang, in den die §§ 94 ff. StPO eingebettet seien (§§ 152 Abs. 2, 155 Abs. 1, 160, 170, 244 Abs. 2, 264 StPO).

Ferner verlange auch der Verhältnismäßigkeitsgrundsatz nach Ansicht des BVerfG keine über die §§ 94 ff. StPO hinausgehenden speziellen Voraussetzungen. Insbesondere sei keine Straftat von erheblicher Bedeutung als Eingriffsvoraussetzung zu fordern. Dies begründet das BVerfG damit, dass die „in der Ermittlungspraxis erfahrenen Auskunftspersonen“ in der mündlichen Verhandlung erklärt hätten, dass in der Praxis auch ein Bedürfnis bestünde, auf Verbindungsdaten zuzugreifen, wenn – anders als die §§ 100g, 100h StPO es verlangen – keine Straftat von erheblicher Bedeutung verfolgt würden.¹⁶

Schließlich fehle es bei einem Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten an der Heimlichkeit der Maßnahme. Auch insoweit sei es zur Wahrung des Verhältnismäßigkeitsgrundsatzes nicht erforderlich, die Beschlagnahme generell auf Ermittlungen zu beschränken, die sich auf Straftaten von erheblicher Bedeutung erstrecken. Denn aufgrund der Offenheit des Eingriffs habe der Betroffene die Möglichkeit, bereits während der Vollstreckung der Maßnahme entgegenzutreten.¹⁷ Somit entfalle auch das Risiko – wie es grundsätzlich bei heimlichen Maßnahmen bestehe – an der Inanspruchnahme von Rechtsschutz faktisch gehindert zu sein.¹⁸

Im vorliegenden Fall nimmt das BVerfG jedoch an, dass die Eingriffe in die Unverletzlichkeit der Wohnung und das Recht auf informationelle Selbstbestimmung unverhältnismäßig und daher nicht gerechtfertigt waren. Insbesondere hätte bei der Verhältnismäßigkeitsabwägung berücksichtigt werden müssen, dass es sich bei den Daten um solche handle, die außerhalb der Sphäre des Betroffenen in den Schutzbereich des Art. 10 Abs. 1 GG fielen.¹⁹ Im Übrigen hätten der äußerst geringe Tatverdacht und die – angesichts der zwischenzeitlich verstrichenen Zeit – geringeren Auffindungswahrscheinlichkeit nicht ausreichend Beachtung gefunden.²⁰

III. Kritische Würdigung

Im Folgenden sind die Ausführungen des BVerfG kritisch zu beleuchten. Dabei ist in einem ersten Schritt zu hinterfragen, ob die Ausführungen zum Schutzbereich des Art. 10 Abs. 1 GG im vollen Umfang zu überzeugen vermögen (1.). In einem zweiten Schritt ist die Frage aufzuwerfen, inwieweit das Recht auf informationelle Selbstbestimmung durch einen Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsdaten betroffen ist (2.). In einem letzten Schritt ist zu erörtern, welche Anforderungen an die Rechtfertigung eines Eingriffs in die informationelle Selbstbestimmung zu stellen sind. Dabei stellt sich insbesondere die Frage, ob die §§ 94 ff. StPO den Anforderungen gerecht werden, die an eine Ermächtigungsgrundlage für einen Zugriff auf die im Herrschaftsbereich des Kommu-

nikationsteilnehmers gespeicherten Kommunikationsdaten zu stellen sind (3.).

1. Das Fernmeldegeheimnis i.S.d. Art. 10 Abs. 1 GG

Die fundamentale Frage der vorliegenden Entscheidung ist, ob die bei einem Kommunikationsteilnehmer gespeicherten Verbindungsdaten in den Schutzbereich des durch Art. 10 Abs. 1 GG geschützten Fernmeldegeheimnisses fallen. Dies hat das BVerfG im Ergebnis zu Recht verneint, ohne dabei allerdings auf den abweichenden Kammerbeschluss vom 4. Februar 2005 einzugehen.

Der Schutzbereich des Art. 10 Abs. 1 GG umfasst nicht nur den Inhalt der Kommunikation, sondern darüber hinaus auch Kommunikationsumstände. Dazu zählen etwa Informationen, ob, wann und wie oft welche Personen bzw. Endrichtungen im Wege der Telekommunikation in Verbindung standen.²¹ Das Grundrecht soll also die Vertraulichkeit der freien Kommunikation und damit die freie Entfaltung der Persönlichkeit durch einen privaten vor der Öffentlichkeit abgeschirmten Austausch von Informationen gewährleisten.²² Durch diese grundrechtliche Verbürgung soll vermieden werden, dass der telekommunikative Meinungs- und Informationsaustausch unterbleibt, weil die Beteiligten befürchten, dass staatliche Stellen Zugriff auf den Kommunikationsverkehr nehmen und dadurch Kenntnisse über Kommunikationsbeziehungen oder -inhalte gewinnen.²³

Art. 10 Abs. 1 GG schützt sämtliche mit Hilfe der Kommunikationstechnik übermittelten Informationen, wobei unerheblich ist, welche Kommunikationstechniken zum Einsatz kommen²⁴ und wer Betreiber der Übertragungs- und Vermittlungseinrichtung ist.²⁵ Dabei stellt Art. 10 Abs. 1 GG ein sog. dynamisches Grundrecht dar, d.h. es ist entwicklungs offen und umfasst nicht nur die bei Entstehung des Gesetzes bekannten Arten der Nachrichtenübermittlung, sondern auch moderne Übertragungstechniken.

Durch den Schutz des Fernmeldegeheimnisses soll gerade den spezifischen Gefahren begegnet werden, die aus dem durch Dritte geleisteten Übermittlungsvorgang resultieren.²⁶ Der Grundrechtsschutz des Art. 10 Abs. 1 GG beschränkt sich dabei nicht nur auf die Dauer des Kommunikationsvorgangs. Vielmehr kann der Schutz des Fernmeldegeheimnisses hinsichtlich der Kommunikationsumstände bereits vor Beginn eines Telefongesprächs bestehen, z.B. wenn das Telefonat nicht zustande kam, aber gleichwohl Verbindungsdaten gespeichert wurden. Ebenso ist der Schutzbereich des Art. 10 Abs. 1 GG nach Ende des Kommunikationsvorgangs einschlägig, wenn etwa durch die Übermittlung kommunika-

²¹ BVerfG NJW 2003, 1787 (1788).

²² BVerfG NJW 2005, 2603 (2612).

²³ BVerfG NJW 2003, 1787 (1789).

²⁴ Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, 8. Aufl. 2006, Art. 10 Rn. 4; Krüger/Pagenkopf, in: Sachs, Grundgesetz, 3. Aufl. 2006, Art. 10 Rn. 14.

²⁵ BVerfG NJW 2002, 3619 (3620); Janz, JuS 2003, 1063 (1064).

²⁶ BVerfG NJW 2003, 1787 (1789); Gusy, JuS 1986, 89 (90).

¹⁶ BVerfG ZIS 2006 (Fn. 7) Rn. 103.

¹⁷ BVerfG ZIS 2006 (Fn. 7) Rn. 106.

¹⁸ BVerfG ZIS 2006 (Fn. 7) Rn. 108.

¹⁹ BVerfG ZIS 2006 (Fn. 7) Rn. 118.

²⁰ BVerfG ZIS 2006 (Fn. 7) Rn. 127.

onsbezogene Daten beim Telekommunikationsunternehmen gespeichert wurden.²⁷

Insoweit ist unstrittig, dass ein Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis gegeben ist, wenn staatliche Behörden Kenntnis über die Kommunikationsumstände der Kommunikationsteilnehmer von Telekommunikationsunternehmen erlangen.

Problematisch ist allerdings, wie sich der Umstand auswirkt, dass die Strafverfolgungsbehörden – wie vorliegend – ihre Kenntnisse über die Einzelheiten der Telekommunikationsumstände nicht von einem Kommunikationsunternehmen erlangen, sondern vielmehr im Herrschaftsbereich der Betroffenen erwerben.

Zunächst ist festzustellen, dass die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten im selben Umfang Aufschluss über die Umstände der durch Art. 10 Abs. 1 GG geschützten Kommunikationsumstände geben wie solche Daten, die bei einem Telekommunikationsunternehmen gespeichert sind. Dabei könnte der Schluss nahe liegen, dass alle Verbindungsdaten, unabhängig von ihrem Speicherort im gleichen Umfang schutzbedürftig sind und daher gleichermaßen dem Schutzbereich des Art. 10 Abs. 1 GG unterfallen.²⁸

Gleichwohl ist zu berücksichtigen, dass Art. 10 Abs. 1 GG gerade solche Gefahren zu verhindern sucht, die dadurch entstehen, dass die Kommunikationsteilnehmer nicht am selben Ort, sondern mittels Einsatzes moderner Technologien durch Einschaltung fremder Übermittler kommunizieren. Geschützt werden soll allein der Umstand, dass Dritte aufgrund des schlichten Kommunikationsvorgangs Informationen über den Kommunikationsinhalt oder über die Kommunikationsumstände erlangen können. Art. 10 Abs. 1 schafft insoweit lediglich einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit, der durch die Nutzung der Telekommunikationsvorrichtungen Dritter entsteht.²⁹ Diese spezifische Gefahr des räumlich distanzierten Kommunikationsvorgangs realisiert sich bei einem Zugriff auf Verbindungsdaten, die in der Sphäre des Kommunikationsteilnehmers gespeichert sind, aber gerade nicht.

Verdient diese Feststellung des BVerfG in vollem Umfang Zustimmung, so vermögen jedoch die Ausführungen des *Senats*, hinsichtlich der Beherrschbarkeit der Daten in der Privatsphäre eines Telekommunikationsnutzers nicht zu überzeugen. Die These, der Kommunikationsteilnehmer beherrsche die in seiner Sphäre gespeicherten Daten und könne sich vor unerwünschten Zugriffen Dritter, einschließlich der staatlichen Behörden, schützen, ist – wie das BVerfG letztlich selbst einräumt – kein taugliches Kriterium, diesen Daten den Schutz des Art. 10 Abs. 1 GG zu verwehren. Denn faktisch verfügt der Bürger über keine endgültige Löschungsmöglichkeit der Daten. Auch die vom BVerfG ins Feld geführte physische Zerstörungsmöglichkeit führt nicht zwingend eine Vernichtung der gespeicherten Verbindungsdaten herbei. Darüber hinaus dürfte sich die „Option“ einer

physischen Zerstörung jedenfalls für die Fälle als unpraktikabel erweisen, in denen der Datenträger nicht im Eigentum des Kommunikationsteilnehmers steht, wie etwa der PC am Arbeitsplatz.

Außerdem ist zu beachten, dass die Beherrschbarkeit der Daten voraussetzt, dass der Kommunikationsteilnehmer von ihrer Existenz weiß. Aufgrund der rapiden Entwicklung der Informationstechnologie und der damit verbundenen steigenden Menge anfallender Daten verliert der Kommunikationsteilnehmer schnell den Überblick über die sich in seinem Herrschaftsbereich ansammelnden Daten. Wer aber nicht weiß, dass Daten in seiner Privatsphäre gespeichert werden, kann diese auch nicht beherrschen.

Dennoch stehen die in der Privatsphäre des Kommunikationsteilnehmers gespeicherten Daten potentiell zur Disposition des Betroffenen. Allerdings lässt sich dieses Potential zur Löschung der Daten nur in seltenen Fällen realisieren. Dies gilt auch für einen vom BVerfG angesprochenen Schutz durch Passwörter, da diese oftmals durch Dritte – auch von Staatsorganen – entschlüsselt werden können. Der Unterschied zwischen den beim Kommunikationsteilnehmer und den beim Kommunikationsunternehmen gespeicherten Verbindungsdaten besteht also nicht in der *faktischen* Beherrschbarkeit, sondern allenfalls in einer – grundsätzlich nicht nutzbaren – *potentiellen* Beherrschbarkeit der Daten.

Zustimmung verdient hingegen die Begründung des BVerfG, soweit es auf die Vergleichbarkeit der gespeicherten Verbindungsdaten mit den übrigen im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Daten abstellt. Zwar ist dieser Argumentation des BVerfG zunächst entgegenzuhalten, dass sich aus anderen in der Privatsphäre gespeicherten Daten nicht im selben Umfang Rückschlüsse auf Kommunikationsumstände ziehen lassen wie sie aus den Verbindungsdaten gezogen werden können. So lässt sich etwa dem in einem Mobiltelefon gespeicherten Rufnummernverzeichnis nur entnehmen, dass der Inhaber des Mobiltelefons grundsätzlich telefonischen Kontakt zu der entsprechenden Person hat. Erkenntnisse über Zeit, Anzahl, Ort und Dauer der Gespräche lassen sich hingegen nur aus den Kommunikationsdaten gewinnen. Gleichwohl ist zu konstatieren, dass die Möglichkeit der Kenntnisnahme der in den Kommunikationsdaten enthaltenen Kommunikationsumständen bei einem Zugriff im Herrschaftsbereich des Kommunikationsteilnehmers nicht auf dem technischen Risiko des Übermittlungsvorgangs beruht. Genaugenommen ist also nicht die inhaltliche Vergleichbarkeit mit den anderen in der Privatsphäre gespeicherten Daten der entscheidende Gesichtspunkt dafür, dass die im Herrschaftsbereich gespeicherten Verbindungsdaten aus dem Schutzbereich des Art. 10 Abs. 1 GG fallen. Maßgeblich ist vielmehr allein der Umstand, dass das Risiko, dass Dritte aufgrund des technischen Übermittlungsvorgangs Informationen über den Kommunikationsinhalt oder über die Kommunikationsumstände erlangen können, nicht gegeben ist. Insoweit besteht also nur eine Vergleichbarkeit des Zugriffsrisikos.

²⁷ Gusy, NStZ 2003, 399 (401).

²⁸ Vgl. BVerfG NJW 2005, 1637 (1639).

²⁹ Sankol, MMR 2006, 361 (364).

2. Das Recht auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Bei der Prüfung des Rechts auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG stellt das BVerfG vorliegend zu Recht fest, dass dieses Grundrecht neben Art. 13 Abs. 1 GG Anwendung findet, d.h. ein Vorrang des Art. 13 Abs. 1 GG als spezielles Freiheitsrecht nicht besteht.

Zutreffend betont das BVerfG, dass sich der Eingriff bei einem Zugriff auf Verbindungsdaten im Herrschaftsbereich des Kommunikationsteilnehmers nicht allein auf das Eindringen der Strafverfolgungsbehörde in die räumliche Privatsphäre des Betroffenen beschränkt. Denn bei den Verbindungsdaten handelt es sich um personenbezogene Daten, die unabhängig vom Zugriffsort einen erheblichen Aussagegehalt aufweisen und Rückschlüsse zulassen, die „an die Qualität eines Persönlichkeitsprofils heranreichen“³⁰, wobei der Betroffene die Richtigkeit dieses Persönlichkeitsprofils nicht kontrollieren kann.³¹ Der Eingriff weist damit einen engen Bezug zur Menschenwürde i.S.d. Art. 1 Abs. 1 GG auf.

Vor dem Hintergrund dieses gravierenden Eingriffs in die Privatsphäre ist es für den Betroffenen irrelevant, *wo* die Ermittlungsbehörden die personenbezogenen Informationen über ihn erlangen: beim Kommunikationsteilnehmer oder beim Kommunikationsunternehmen. Die Ermittlungsbehörden gewinnen jeweils dieselben Erkenntnisse; und zwar wer mit wem wann, wo, wie oft und wie lange mittels Telekommunikationstechnologie in Verbindung stand. Das Recht auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG trägt insoweit dem Umstand Rechnung, dass sich auch aus der nicht übermittlungsbedingten Kenntnisnahme der Verbindungsdaten Informationen über Kommunikationsumstände gewinnen lassen und sie daher auch nach Beendigung des Übermittlungsvorgangs eines besonderen Schutzes bedürfen. Maßgeblich für die Schutzbedürftigkeit der Daten ist also letztlich nicht der Umstand, *wo* auf diese Daten zugegriffen wird, sondern allein *dass* ein Zugriff auf diese Daten erfolgt. Aus diesem Grund ist es begrüßenswert, dass das BVerfG Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vorliegend als Ausdruck einer Ergänzungsfunktion zu Art. 10 Abs. 1 GG versteht.

3. Die Rechtfertigung des Eingriffs in das Recht auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Sind die Ausführungen zum Schutzbereich des Rechts auf informationelle Selbstbestimmung uneingeschränkt begrüßenswert, so gilt dies nicht für die Überlegungen des *Senats* zur Rechtfertigung dieses Grundrechtseingriffs.

Bei der Erörterung der Frage, unter welchen Voraussetzungen der Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt ist, hebt das BVerfG hervor: „Die Verhältnismäßigkeitsprüfung muss dem Umstand Rechnung

tragen, dass es sich um Daten handelt, die außerhalb der Sphäre des Betroffenen unter dem besonderen Schutz des Fernmeldegeheimnisses stehen und denen im Herrschaftsbereich des Betroffenen ein ergänzender Schutz durch das Recht auf informationelle Selbstbestimmung zuteil wird.“³² Diesen strengen Verhältnismäßigkeitsmaßstab legt das BVerfG jedoch erst im Rahmen der Einzelfallabwägung an. Weniger streng sind dagegen die Anforderungen, die das BVerfG an eine gesetzliche Ermächtigungsgrundlage stellt, die einen Eingriff in das Recht auf informationelle Selbstbestimmung legitimiert, soweit auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten zugegriffen wird. Hier lässt das BVerfG die „weichen“ Voraussetzungen des § 94 StPO ausreichen. Diese Feststellungen des BVerfG sind jedoch durchgreifenden Bedenken ausgesetzt. Denn es bestehen erhebliche Zweifel, ob die §§ 94 ff. StPO ein ausreichendes Schutzniveau für den Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten bieten.³³

Gem. § 94 Abs. 2 StPO wird eine Beschlagnahme angeordnet, wenn der betreffende Gegenstand, der sich im Gewahrsam einer Person befindet, nicht freiwillig herausgegeben wird. Voraussetzung ist der einfache Verdacht einer Straftat i.S.d. § 152 Abs. 2 StPO, der sich nicht gegen eine bestimmte Person richten muss. Weiterhin ist der Verhältnismäßigkeitsgrundsatz zu beachten, d.h. die Maßnahme muss in einem angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen. Schließlich muss der beschlagnahmte Gegenstand einen potentiellen Beweiswert aufweisen und für die Ermittlungen als Beweisgegenstand von Bedeutung sein. Gem. § 98 Abs. 1 StPO ist die Anordnung der Beschlagnahme zwar einem Richter vorbehalten. Bei Gefahr im Verzug sind jedoch sowohl die Staatsanwaltschaft als auch ihre Ermittlungspersonen anordnungsbefugt.

Die Beschlagnahme fordert demnach lediglich die materiellen Mindestvoraussetzungen, die wenigstens bei jedem strafprozessualen Grundrechtseingriff vorliegen müssen: einen einfachen tatbezogenen Tatverdacht, die Einhaltung des Verhältnismäßigkeitsgrundsatzes und eine Beweisbedeutung. Auch hinsichtlich der formellen Anforderungen gelten lediglich Mindeststandards: Zwar gilt grundsätzlich der Richtervorbehalt, bei Gefahr im Verzug sind aber grundsätzlich sowohl die Staatsanwaltschaft als auch deren Ermittlungspersonen zur Anordnung befugt.

Diese Mindeststandards sind allerdings nicht ausreichend für eine gesetzliche Ermächtigung, die einen Zugriff auf Verbindungsdaten legitimiert, auch wenn diese (nur) im

³⁰ So auch das BVerfG für die in der Privatsphäre gespeicherten Daten, BVerfG ZIS 2006 (Fn. 7) Rn. 91.

³¹ BVerfG NJW 1984, 419 ff. (Rn. 147).

³² BVerfG ZIS 2006 (Fn. 7) Rn. 118; vgl. auch *Jahn*, JuS 2006, 491, 492.

³³ Die Frage, ob §§ 94 ff. StPO grundsätzlich auf die Sicherstellung und Beschlagnahme von *unkörperlichen* Gegenständen anzuwenden ist, wäre einen eigenständigen Beitrag wert und soll daher an dieser Stelle nicht erörtert werden. Vgl. zu dieser Problematik BVerfG NJW 2005, 1917 ff.; *Kemper*, NStZ 2005, 538 ff.; *T. Böckenförde*, Die Ermittlung im Netz, 2003, S. 275 ff.

Herrschaftsbereich des Kommunikationsteilnehmers gespeichert wurden und daher nicht mehr in den Schutzbereich des Art. 10 Abs. 1 GG fallen.

Der *1. Senat* des BVerfG hat in seinem Urteil vom 12. März 2003 festgestellt, dass die Erhebung von Verbindungsdaten nur bei einem Verdacht wegen einer Straftat von erheblicher Bedeutung gerechtfertigt sei. Diesen Straftaten messe der Gesetzgeber allgemein ein besonderes Gewicht zu. Damit werde dem Umstand Rechnung getragen, dass die Offenlegung der Verbindungsdaten ein detailliertes Bild über Kommunikationsvorgänge ermögliche.³⁴ Der *1. Senat* hat das Erfordernis einer Straftat von erheblicher Bedeutung also nicht an den Art. 10 Abs. 1 GG charakterisierenden Umstand der Gefahr einer räumlich distanzierter Kommunikation geknüpft, sondern daran, dass sich faktisch aus der Auswertung der Verbindungsdaten Erkenntnisse gewinnen lassen, die an die Qualität eines Persönlichkeitsprofils heranreichen. Genau diese Erkenntnisse lassen sich aber auch durch die Offenlegung der im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten gewinnen.³⁵

Ist aber die persönlichkeitsbezogene Intensität des Eingriffs der maßgebliche Grund für die Normierung einer Straftat von erheblicher Bedeutung als Eingriffsvoraussetzung, so stellt sich die Frage, aus welchem Grund das BVerfG vorliegend auf dieses Erfordernis verzichtet.

Die Tatsache, dass der Eingriff nach §§ 100g, 100h heimlich erfolgt, die Beschlagnahme gem. § 94 Abs. 2 StPO hingegen eine offene Maßnahme darstellt, rechtfertigt das unterschiedliche Schutzniveau nicht. Die vom BVerfG vorgetragene Argumentation, dass sich der Eingriff nach § 100g StPO aufgrund der Heimlichkeit ohne vorherige Anhörung des Betroffenen vollziehe und der Betroffene daher frühestens nach Vollzug der Maßnahme Rechtsschutz begehren könne, vermag eine zusätzliche Schwere des heimlichen Eingriffs im Gegensatz zu offenen Maßnahmen nicht zu begründen. Diese Ansicht berücksichtigt nicht, dass grundsätzlich keine strafprozessuale beweissichernde Maßnahme einem Beschuldigten gegenüber zuvor angekündigt wird. Das Problem des mangelnden vorbeugenden Rechtsschutzes ist demnach kein die heimlichen Maßnahmen kennzeichnender Umstand, sondern vielmehr ein alle strafprozessualen Grundrechtseingriffe auszeichnendes Moment. Denn der Sinn dieser Eingriffe besteht ja gerade darin, dass sie überraschend erfolgen, um zu verhindern, dass der Erfolg der Maßnahme durch Beseitigung von Beweismitteln vereitelt wird. Bei geheimen Maßnahmen besteht zwar grundsätzlich die erhöhte Notwendigkeit, dass der Betroffene *bei Durchführung der Maßnahme* nichts davon weiß, da der Erfolg der Maßnahmen maßgeblich davon abhängt, dass die Betroffenen sich unbeobachtet fühlen, etwa bei Abhörmaßnahmen. Dieser die heimlichen strafprozessualen Grundrechtseingriffe kennzeichnende Umstand fehlt aber bei der Maßnahme nach §§ 100g, 100h StPO. Entscheidend ist hier nicht, dass sich der Betroffene *zum Zeitpunkt des Zugriffs* auf die Daten unbeobachtet fühlt. Maßgeblich ist vielmehr, dass der Betroffene *zum Zeitpunkt der Speicherung*

der Daten ahnungslos ist. Zu diesem Zeitpunkt befindet sich der Betroffene in einer Situation vermeintlicher Vertraulichkeit und rechnet nicht damit, dass zu einem späteren Zeitpunkt auf die Verbindungsdaten in seiner Privatsphäre oder beim Kommunikationsunternehmen zugegriffen wird.

Die fehlende Offenheit des Zugriffs i.S.d. §§ 100g, 100h StPO vermag also die Behauptung, der Eingriff wiege schwerer, nicht zu stützen.

Die unbestrittene Tatsache, dass für die Strafverfolgungsbehörden ein erhebliches Bedürfnis besteht, auf die beim Kommunikationsteilnehmer gespeicherten Daten auch bei der Verfolgung von weniger erheblichen Straftaten zugreifen zu können, ist ferner kein Grund, um das Schutzniveau der Eingriffsvoraussetzungen absenken zu können. Der Wunsch nach effektiven Strafverfolgungsmöglichkeiten vermag ihre Legitimität noch nicht zu begründen. Ferner ließe sich mit dieser Argumentation jede Eingriffsbeschränkung verhindern, da jede Verschärfung der Eingriffsvoraussetzungen einer Effektivierung der Strafverfolgung entgegenstünde.

Letztlich führt eine Zugriffslegitimation auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Daten unter den Voraussetzungen des § 94 StPO zu einer Umgehung der in den §§ 100g, 100h StPO verlangten Voraussetzungen.³⁶ Wenn beide strafprozessualen Grundrechtseingriffe zum gleichen Ziel führen und an die eine Maßnahme wesentlich geringere Voraussetzungen gestellt werden als an die andere, so besteht die Gefahr, dass die Strafverfolgungsbehörden die strengen Voraussetzungen der §§ 100g, 100h StPO unterlaufen.

Abschließend sei noch angemerkt, dass das BVerfG zwar die Geringfügigkeit der zu ermittelnden Straftat als einen abwägungsrelevanten Gesichtspunkt erachtet,³⁷ gleichwohl an keiner Stelle des Urteils in die Abwägung mit einfließen lässt, dass die in Rede stehende Straftat – die Verletzung von Dienstgeheimnissen gem. § 353b Abs. 1 StGB – eine Höchststrafe von einem Jahr Freiheitsstrafe aufweist und mithin einen niedrigeren Unrechtsgehalt besitzt als die Sachbeschädigung i.S.d. § 303 Abs. 1 StGB (Höchststrafe von zwei Jahren Freiheitsstrafe). Dies lässt befürchten, dass die Schwere der Tat im Ergebnis überhaupt keine Berücksichtigung gefunden hat.

IV. Fazit

Der Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten stellt keinen Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis dar. Allerdings wird durch einen solchen Zugriff in das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingegriffen. Dabei bietet § 94 Abs. 2 StPO – mit seinen weiten Eingriffsvoraussetzungen – als Ermächtigungsgrundlage für einen Zugriff auf die in der Privatsphäre gespeicherten Verbindungsdaten kein ausreichendes Schutzniveau. Der Gesetzgeber ist daher gefordert, eine der Eingriffsintensität Rechnung tragende Er-

³⁴ BVerfG NJW 2003, 1787, 1791.

³⁵ Vgl. BVerfG ZIS 2006 (Fn. 7) Rn. 91.

³⁶ Vgl. auch Volk, Grundkurs StPO, 5. Aufl. 2006, § 10 Rn. 47a.

³⁷ BVerfG ZIS 2006 (Fn. 7), Rn. 119.

mächtigungsgrundlage zu schaffen, die – um zumindest Bagatelldelikte generell auszuschließen – jedenfalls eine „Straftat von Bedeutung“ voraussetzt und einen bestimmten täterbezogenen Tatverdacht verlangt.

Entscheidungen zu Besprechungsaufsätzen

Wohnungsdurchsuchung zur Ermittlung von Kommunikationsdaten – Verdacht der Verletzung von Dienstgeheimnissen

GG Art. 1 Abs. 1, 2 Abs. 1, 10 Abs. 1, 13; StPO §§ 94 ff., 102 ff.; StGB § 353b Abs. 1

1. Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten werden nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt.

2. §§ 94 ff. und §§ 102 ff. StPO genügen den verfassungsrechtlichen Anforderungen auch hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten und entsprechen der vor allem für das Recht auf informationelle Selbstbestimmung geltenden Vorgabe, wonach der Gesetzgeber den Verwendungszweck der erhobenen Daten bereichsspezifisch, präzise und für den Betroffenen erkennbar bestimmen muss. Dem wird durch die strenge Begrenzung aller Maßnahmen auf den Ermittlungszweck Genüge getan (vgl. Beschluss des Zweiten Senats des Bundesverfassungsgerichts vom 12. April 2005 – 2 BvR 1027/02).

3. Beim Zugriff auf die bei dem Betroffenen gespeicherten Verbindungsdaten ist auf deren erhöhte Schutzwürdigkeit Rücksicht zu nehmen. Die Verhältnismäßigkeitsprüfung muss dem Umstand Rechnung tragen, dass es sich um Daten handelt, die außerhalb der Sphäre des Betroffenen unter dem besonderen Schutz des Fernmeldegeheimnisses stehen und denen im Herrschaftsbereich des Betroffenen ein ergänzender Schutz durch das Recht auf informationelle Selbstbestimmung zuteil wird.

BVerfG, Urt. v. 2.3.2006 – 2 BvR 2099/04

Sachverhalt:

A.

#1

Dem Verfahren liegt die Verfassungsbeschwerde einer Richterinnen am Amtsgericht zu Grunde, die sich gegen die Anordnung der Durchsuchung ihrer Wohnung wegen des Verdachts der Verletzung von Dienstgeheimnissen wendet. Die Durchsuchung diene dazu, Kommunikationsverbindungsdaten auf

dem Personalcomputer und dem Mobiltelefon der Beschwerdeführerin zu ermitteln, die einen Nachweis für Kontakte mit einem Reporter hätten ergeben können.

I.

#2

Die Durchsuchung bei dem Beschuldigten ist in § 102 StPO geregelt. Die Vorschrift lautet:

#3

§ 102 StPO

#4

Bei dem, welcher als Täter oder Teilnehmer einer Straftat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist, kann eine Durchsuchung der Wohnung und anderer Räume sowie seiner Person und der ihm gehörenden Sachen sowohl zum Zweck seiner Ergreifung als auch dann vorgenommen werden, wenn zu vermuten ist, dass die Durchsuchung zur Auffindung von Beweismitteln führen werde.

#5

Die materiellen Voraussetzungen der Sicherstellung und Beschlagnahme von Beweisgegenständen, die im Rahmen einer Durchsuchung näher konkretisiert werden, regelt § 94 StPO.

#6

Diese Vorschrift lautet:

#7

§ 94 StPO

#8

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.

#9

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.

#10

(3) ...

#11

Nach § 100g und § 100h StPO können die Ermittlungsbehörden Anbieter von Telekommunikationsdienstleistungen für Auskünfte über bestimmte Kommunikationsverbindungsdaten in Anspruch nehmen. Um welche Verbindungsdaten es sich dabei im Einzelnen handelt, geht aus § 100g Abs. 3 StPO hervor. § 100g Abs. 1 StPO begrenzt den Kreis der Delikte, die Anlass für eine solche Maßnahme sein können, auf Straftaten von erheblicher Bedeutung, vor allem solche im Sinne des § 100a StPO, sowie Straftaten, die mittels einer