KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Masterarbeit von

Lea Emelie Effelsberg

Strafprozessuale Datenbeschlagnahme *de lege lata*
Gehen die Beschuldigtenrechte im Zeitalter von *Big Data* unter?

Universität zu Köln
Fachbereich Rechtswissenschaft/ Recht der Digitalisierung (LL.M.)
Gutachterin: Prof. Dr. Dr. Frauke Rostalski
Abgabedatum: 18.6.2025

Inhaltsverzeichnis

I. Einführung

Smartphones sind aus der modernen Gesellschaft nicht mehr wegzudenken. Längst stellen sie nicht nur ein reines Medium zum Telefonieren dar, sondern verbinden sämtliche Lebensbereiche wie Arbeit, Dating, Banking, Einkauf, Gesundheit und soziale Kontakte.[1] Vielfach ermöglicht das Smartphone die Speicherung von Bank-, Fahr- oder Ausweiskarten im Wallet, von zahlreichen Bildern und Videos in der Galerie sowie die Verknüpfung all dessen über Soziale Medien wie WhatsApp, Instagram und Co. Damit stellt das Smartphone in der heutigen Gesellschaft ein zentrales Mittel zur Selbstverwirklichung dar und dient als das Trägermedium eigener, mitunter sehr persönlicher digitaler Daten, wie beispielsweise Soziale Netzwerk-Accounts, Handynummern, E-Mail-Adressen oder Passwörter.[2] Schnell kann man so über das Smartphone zum Beispiel in Erfahrung bringen, wie eine Person in Verhältnis zu anderen Personen steht, wie es um den Gesundheitszustand des Nutzers steht und welche persönlichen Interessen und Neigungen aus der aktiven Nutzung hervorgehen.

Daneben zeigt sich eine Tendenz dahingehend, dass Smartphones und das Internet zunehmend eine wichtigere Rolle in puncto Kriminalität spielen – nicht nur als reines Kommunikationsmittel, sondern auch als Tatmittel.[3] Angesichts dessen war es nur eine Frage der Zeit, wann das Smartphone und die darauf befindlichen digitalen Daten in den Fokus der Ermittlungsbehörden als „Beweismittel" geraten. Dass eine Beschlagnahme eben jener digitalen Daten für den Betroffenen eine enorme Belastung darstellt, erscheint mit Blick auf die Bedeutung für sein gesellschaftliches Leben außer Frage.

Die Frage ist jedoch: Wie weit reichen die strafprozessualen Befugnisse der Ermittlungsbehörden hinsichtlich dieser Daten? Zwei jüngst ergangene Entscheidungen des *OLG Bremen*[4] und des *BGH*[5] deuten eine verheißungsvolle Tendenz an. Nach den Ausführungen des *OLG Bremen* sei die Anwendung unmittelbaren Zwangs in Form von Auflegen eines Fingers auf den Fingerabdrucksensor des Telefons unter Heranziehung des § 81b StPO strafprozessual zulässig. Gleichwohl sei der Zugriff auf die im Mobiltelefon gespeicherten Daten und deren Verwendung im Strafverfahren nach den Bestimmungen der §§ 94, 110 StPO zu beurteilen.[6] Der *BGH* wies zudem auf die besonders schwerwiegende Eingriffsintensität des Zugriffs auf die digital gespeicherten Daten hin.[7]

Die vorliegende Bearbeitung möchte daher angesichts der Aktualität der Thematik den Fokus auf die derzeitigen Zugriffsmöglichkeiten der Ermittlungsbehörden auf digitale Daten des Beschuldigten im Rahmen des § 94 StPO legen. Es gilt zunächst zu klären, inwieweit digitale Daten überhaupt dem Anwendungsbereich des § 94 StPO unterfallen und welche weiteren Voraussetzungen im Kontext der Datenbeschlagnahme *de lege lata* zu beachten sind. Anschließend sollen die sich hieraus ergebenden aktuellen Ermittlungsbefugnisse den Rechtsschutzmöglichkeiten des Beschuldigten gegenübergestellt werden, um sodann im weiteren Verlauf kritisch zu hinterfragen und zu prüfen, inwieweit den verfassungsrechtlich verankerten Beschuldigtenrechten im Rahmen des § 94 StPO mit Blick auf die Sensibilität von Daten hinreichend Rechnung getragen wird oder ob diesbezüglich gesetzgeberischer

1 vgl. *Neuhaus/Artkämper/Weise*, Kriminaltechnik und Beweisführung im Strafverfahren, 2. Aufl. (2024), Rn. 202.
2 Im Einzelnen *Neuhaus/Artkämper/Weise*, Rn. 202.
3 Insbesondere als Tatmittel bei Betrugsdelikten vgl. Bundesministerium des Innern und der Heimat, PKS 2023, S. 17, 22 f., online abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2023.pdf?blob=publication- File&v=4; S. 17, 22 f. (zuletzt abgerufen am 20.5.2025); *Neuhaus/Artkämper/Weise*, Rn. 200, 202; zur Benennung einiger Anwendungsfelder vgl. *Wernert*, Internetkriminalität, 4. Aufl. (2021), S. 142 ff.
4 *OLG Bremen*, BeckRS 2025, 295.
5 *BGH*, BeckRS 2025, 9876.
6 *OLG Bremen*, BeckRS 2025, 295 Rn. 13; *BGH*, BeckRS 2025, 9876 Rn. 42.
7 *BGH*, BeckRS 2025, 9876 Rn. 33.

Handlungsbedarf besteht.[8]
In Abgrenzung hierzu setzt sich die Bearbeitung nicht mit der näheren Differenzierung zwischen Sicherstellung und Beschlagnahme als solcher auseinander. Weitergehende Problematiken im Zusammenhang mit grenzüberschreitenden Sachverhalten und europarechtlichen Vorgaben bleiben angesichts ihres Umfangs in der vorliegenden Bearbeitung unberücksichtigt. Angesichts der Vielgestaltigkeit der Datenbeschlagnahme[9] wird im Ausgangspunkt auf die Konstellation der Mitnahme des Datenträgers (hier: das Smartphone) und die anschließende Erstellung eines Datenduplikats abgestellt, sodass im Zentrum der Bearbeitung die nähere Auseinandersetzung mit der offenen Ermittlungsmaßnahme nach § 94 Abs. 1, 2 StPO steht.

II. Einordnung von digitalen Daten im Kontext der Beschlagnahmeregelung i.S.d. § 94 Abs. 1, 2 StPO

Zu Beginn ist zu klären, inwieweit digitale Daten dem Anwendungsbereich der Befugnisnorm des § 94 Abs. 1, 2 StPO unterfallen.

1. Begriff der digitalen Daten

Dazu ist zunächst näher zu erörtern, was sich hinter dem Datenbegriff verbirgt. Auffallend ist, dass der Begriff der Daten in der Strafprozessordnung in einigen Regelungen zwar zugrunde gelegt wird, dieser jedoch keiner Legaldefinition unterworfen wurde. Lediglich bei § 98a Abs. 1 StPO findet insofern eine nähere Konkretisierung statt, als dass es sich dort um personenbezogene Daten handeln muss.
Systematisch betrachtet lässt jedoch die Formulierung des § 98c S. 1 StPO, der einen Abgleich von personenbezogenen Daten mit „anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten“ gestattet, den Umkehrschluss zu, dass sich die Regelungen der Strafprozessordnung nicht nur auf rein personenbezogene, sondern sämtliche Daten im Bezug auf die Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr beziehen. Der Begriff scheint damit jedenfalls weit zu verstehen sein.
Nach dem Grundsatz der Einheit der Rechtsordnung[10] könnte indes auf die Legaldefinition des § 202a Abs. 2 StGB abgestellt werden. Hiernach sind „Daten […] solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.“ Eine Begrenzung auf rein personenbezogene Daten findet hier ebenfalls keine Grundlage,[11] was für ein Verständnis der weiten Auslegung des Datenbegriffs spricht. Aus der Legaldefinition des § 202a Abs. 2 StGB lässt sich jedoch nichts Näheres hinsichtlich des Datenbegriffes als solchem entnehmen, sondern lediglich dessen Speicherungs- und Übertragungsform.

8 So *El-Ghazi*, NJW-Beil 2024, 46 (49), zust. *Beukelmann*, NJW-Spezial 2024, 696; *Cornelius*, NJW 2024, 2725 (2727 f.); *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, 62. EL (Juni 2024), StPO, Teil 19.3 Rn. 91 ff., a.A. *Krause*, ZRP 2025, 17 (19).
9 Zur sinnvollen Differenzierung zwischen Mitnahme des Datenträgers als solchem, der Mitnahme des Datenträgers und dem anschließenden Kopieren des Datensatzes sowie der sofortigen Kopie des Datensatzes vgl. *Bell*, Beschlagnahme und Akteneinsicht bei elektronischen Medien, 2016, S. 13 ff., 66 ff., 146 ff.
10 Ausführlich zum Grundsatz *Helm*, in: NK-ASStrafR, 2021, StGB, Einl. Rn. 2 ff.
11 Für ein weites Verständnis vgl. *Hilgendorf*, in: LK-StGB, Bd. 10, 13. Aufl. (2023), § 202a Rn. 8 f.; *Eisele*, in: TK-StGB, 31. Aufl. (2025), § 202a Rn. 3; *Anstötz*, in: Fischer, StGB, 72. Aufl. (2025), § 202a Rn. 3.

Es bietet sich daher an, den Datenbegriff klarstellender zu formulieren: Daten sind digital gespeicherte Informationen,[12] die auf einem Datenträger[13] mittels Nullen und Einsen als Zahlenfolgen[14] dargestellt werden, deren Bedeutung aber ohne entsprechende Abstraktion[15] nicht ohne Weiteres menschlich wahrnehmbar ist und die sich durch ihre nichtkörperliche Form kennzeichnen.[16]

2. Digitale Daten als Beschlagnahmegegenstand i.S.d. § 94 Abs. 1, 2 StPO

Da der Datenbegriff nun näher erläutert wurde, sollte sich damit auseinandergesetzt werden, inwieweit sich der Datenbegriff in den Kontext der Beschlagnahmeregelung des § 94 StPO einordnen lässt. Dies wirft angesichts der „besonderen" Form von Daten Fragen auf. Hierzu sind im Folgenden die juristischen Auslegungsmethoden heranzuziehen.

a) Wortlaut

Als beschlagnahmefähig gelten dem ausdrücklichen Wortlaut des Normtextes und des Normtitels nach zunächst einmal „Gegenstände zu Beweiszwecken". Gemeint sind damit unbewegliche und bewegliche Sachen, wie körperliche Gegenstände.[17] Hierunter fallen neben Schriftstücken und Akten auch Speichermedien,[18] etwa Mobiltelefone[19] oder andere Datenträger.[20] Von Interesse für die Ermittlungsbehörden wird jedoch in erster Linie nicht der Datenträger sein, sondern der hierauf verkörperte Informationswert,[21] also die Daten.
Fraglich ist daher, ob nicht die Daten als solche ohne ihren verkörperten Datenträger den Beschlagnahmevorschriften unterliegen. Da digitale Daten im Ausgangspunkt zu den nichtkörperlichen Gegenständen zählen,[22] standen zahlreiche Stimmen in der Literatur[23] dem zu Recht kritisch gegenüber.
In der Vergangenheit stellte die Rechtsprechung ausdrücklich klar, dass es dem Wortsinn der Norm nicht entgegenstehe, als beschlagnahmefähigen Gegenstand auch unkörperliche Gegenstände – wie digitale Daten[24] als solche – zu verstehen. Zwar legt eine solche Auslegung auf den ersten Blick einen Widerspruch in der Bewertung von nichtkörperlichen Gegenständen nahe, da bei anderen nichtkörperlichen Gegenständen, z.B. Forderungen oder andere Rechte, bei denen eine unmittelbare Verwendung zu Beweiszwecken nicht möglich ist,[25] eine Beschlagnahme nach § 94 StPO ausscheidet. Hier kann jedoch entgegengehalten werden, dass ein Rückgriff auf die Kopie

12 *Blechschmitt*, MMR 2018, 361 (364), vgl. auch *Wohlers/Singelnstein*, in: SK-StPO, Bd. 2, 6. Aufl. (2023), § 94 Rn. 25; zum technischen Datenbegriff vgl. *Kargl*, in: NK-StGB, 6. Aufl. (2023), § 202a Rn. 12.
13 *LG Hamburg*, StV 2015, 161 (163).
14 *Gumm/Sommer*, Informatik, 2016, S. 12.
15 *Gumm/Sommer*, Informatik, 2016, S. 5.
16 *Fährmann*, MMR 2020, 228 (229).
17 *Hauschild*, in: MüKo-StPO, Bd. 1, 2. Aufl. (2023), § 94 Rn. 12; *Löffelmann*, in: AK-StPO, 2. Aufl. (2010), § 94 Rn. 3.
18 *Hauschild*, in: MüKo-StPO, § 94 Rn. 12; vgl. auch *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 4.
19 *Greven*, in: KK-StPO, 9. Aufl. (2023), § 94 Rn. 4.
20 *Wohlers/Singelnstein*, in: SK-StPO, § 94 Rn. 23, 27; *Gercke*, in: HK-StPO, 7. Aufl. (2023), § 94 Rn. 19.
21 Vgl. *Wohlers/Singelnstein*, in: SK-StPO, § 94 Rn. 26.
22 *Hauschild*, in: MüKo-StPO, § 94 Rn. 12 f.; vgl. auch *Menges*, in: LR-StPO, Bd. 3/1, 27. Aufl. (2019), § 94 Rn. 14; *Gercke*, in: HK-StPO, § 94 Rn. 18.
23 Kritisch etwa *Wohlers/Singelnstein*, in: SK-StPO, § 94 Rn. 27 ff.; *Gercke*, in: HK-StPO, § 94 Rn. 18; *Löffelmann*, in: AK-StPO, § 94 Rn. 3; wohl aber zustimmend *Menges*, in: LR-StPO, § 94 Rn. 14.
24 BVerfGE 113, 29 (50); BVerfGE 124, 43 (61); jüngst anschließend *BGH,* BeckRS 2025, 9876 Rn. 44 m.w.N.; a.A. *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. (2017), § 34 Rn. 4 („Elektronische Daten sind keine Gegenstände und unterliegen daher als solche nicht der Beschlagnahme"); nunmehr zust. *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. (2022), § 34 Rn. 4.
25 Vgl. zur Differenzierung zwischen „nichtkörperlichen und unkörperlichen Gegenständen" *Hauschild*, in: MüKo-StPO, § 94 Rn. 12; vgl. ansonsten *Greven*, in: KK-StPO, § 94 Rn. 3.

von Daten gegenüber der Mitnahme des Datenträgers als mildere Maßnahme[26] zwangsläufig geboten erscheint und sich eine andere Argumentation folglich Schwierigkeiten ausgesetzt sehen muss. Nicht entscheidend für die Beschlagnahmefähigkeit ist somit die Körperlichkeit eines Gegenstandes.[27]

b) Historie

Historisch lässt sich dieser Standpunkt zwar nicht untermauern, da der historische Gesetzgeber in der ursprünglichen Fassung der Norm nicht bedacht haben kann, dass Informationen auch einmal in nichtkörperlicher Form vorliegen könnten.[28] Dass sich strafprozessuale Eingriffsbefugnisse auch auf Maßnahmen außerhalb des jeweiligen Technikstandes im Zeitpunkt der Normierung erstrecken können, scheint jedoch kein Einzelfall, sondern zumeist „gebilligte Praxis“[29] der Gerichte. Dies entspricht auch dem Bedürfnis, bei der Auslegung von Ermittlungsbefugnissen die technischen Fortschritte einbeziehen zu können.[30]

c) Systematik

Systematisch ist erkennbar, dass dem Gesetzgeber die Bedeutung von Daten für die Strafverfolgung bewusst ist. Dies deutet sich z.B. in den §§ 98a-98c StPO an,[31] welche einen maschinellen Abgleich mit personenbezogenen Daten gestatten. Ferner streitet die mehrmals an die Bedürfnisse der Digitalisierung angepasste Vorschrift des § 110 StPO[32] als Vorstufe zur Beschlagnahme für eine einheitliche Handhabung der zu sichernden Gegenstände. Für den Beschuldigten kann es wertungstechnisch keinen Unterschied machen, ob die Daten zur vorläufigen Sicherstellung oder zur Beschlagnahme mitgenommen werden.[33]

d) Telos

Vielmehr entspricht es dem Normzweck, dass auch digitale Daten den Beschlagnahmevorschriften unterliegen. Diese dienen im Wesentlichen der Wahrheitsfindung und der Beweis- bzw. Verfahrenssicherung.[34] Folglich ist die Beschlagnahmefähigkeit nicht pauschal anhand einer gattungsrechtlichen Einordnung zu beurteilen, sondern stets anhand des Normzwecks.
Hinsichtlich des Beitrags zur Wahrheitsfindung lässt sich hier folgendes Beispiel anführen: Endet ein Streit zwischen zwei Personen in einer tödlichen Auseinandersetzung inmitten eines Feldes, ohne dass es Zeugen gäbe oder sonstige Spuren zurückgelassen werden, weil es etwa an jenem Tag regnete, so bietet das Bewegungsprofil eines

26 Vgl. *Menges*, in: LR-StPO, § 94 Rn. 28; *Wohlers/Singelnstein*, in: SK- StPO, § 94 Rn. 27.
27 *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 3.
28 So auch BVerfGE 113, 29 (50).
29 So *BGH*, BeckRS 2025, 9876 Rn. 40.
30 Zur sogenannten Technikoffenheit *Roggan*, NJW 2015, 1995.
31 BVerfGE 113, 29 (50); vgl. auch zur Gesetzesbegründung BT-Drs. 12/989, S. 36.
32 Zuletzt mit Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25.6.2021 (BGBl. I, S. 2099, 2102); erstmalige *Aufnahme* des Datenbegriffes mit Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (G-SIG: 1601943) vom 21.12.2007 (BGBl. I, S. 3198, 3204).
33 Überzeugend *Jäger/Wohlers*, in: SK-StPO, § 110 Rn. 2.
34 Vgl. *Gercke*, in: HK-StPO, Vorb. § 94 Rn. 3; *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 1; *Brodowski*, in: BeckOK-IT-Recht, 18. Ed. (1.10.2024), § 94 StPO Rn. 1; *Hauschild*, in: MüKo-StPO, § 94 Rn. 1.

Smartphones nach Möglichkeit einen Hinweis auf den Täter. Hierbei ist anzumerken, dass ein Täter im Regelfall Datenspuren[35] bei nahezu jedem Delikt hinterlassen wird. Die Förderung der Wahrheitsfindung ist daher nicht von der Hand zu weisen und eröffnet neue Erkenntnismöglichkeiten, was sich auch durch die gemeinsame Regelung des grenzüberschreitenden Zugriffs auf Computerdaten im Übereinkommen über Cyberkriminalität[36] andeutet. Eine erweiternde Auslegung des Begriffs der „Gegenstände" iSd § 94 StPO erscheint daher geboten.

e) Zwischenergebnis: Digitale Daten erfasst

Es ist festzuhalten, dass unter den Anwendungsbereich der Beschlagnahme auch digitale Daten unterfallen dürften, dies jedoch nach derzeitiger Rechtslage nicht hinreichend gesetzlich zum Ausdruck kommt.[37] Wünschenswert wäre ein klarstellender Hinweis durch die Gesetzgebung.[38] Exemplarisch stellt die Bearbeitung im weiteren Verlauf einen Entwurf für eine mögliche Neugestaltung des § 94 StPO unter Berücksichtigung der Datenbeschlagnahme vor.

III. Sich hieraus ergebende Zugriffsmöglichkeiten auf digitale Daten durch die Ermittlungsbehörden

Lässt man die Datenbeschlagnahme nach den Vorschriften der StPO entsprechend der Rechtsprechung zu, so ist kritisch zu reflektieren, welche Befugnisse damit den Ermittlungsbehörden eingeräumt werden.

1. Erheblicher Ermessensspielraum

Zwar hat der Gesetzgeber nach dem Wortlaut des § 94 Abs. 1 StPO („Gegenstände […] sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.") den Ermittlungsbehörden hinsichtlich des „Ob" der Beschlagnahme kein Ermessen eingeräumt. Gleichwohl sollte man an dieser Stelle hervorheben, dass den Ermittlungsbehörden in der konkreten Ausgestaltung der Durchführung der Beschlagnahme dennoch ein nicht nur unerheblicher Ermessensspielraum[39] zukommt.
Begrenzungen im Handlungsspielraum ergeben sich insoweit durch den Ermittlungszweck und dem Verhältnismäßigkeitsgrundsatz.[40] Damit besteht zumindest ein „Eckpunktekonzept" für die Durchführung, welche sich vornehmlich nach den Vorgaben der Rechtsprechung konkretisiert. Die Ermittlungsbehörden haben bei ihrer Tätigkeit die Grundsätze der richterlichen Rechtsprechung zwar zu beachten, können hierbei jedoch im Einzelfall abweichen.[41] Beispielsweise befindet die Ermittlungsbehörde im eigenen Ermessen darüber, ob sie als mildere Maßnahme der Beschlagnahme ein Auskunftsverlangen[42] an öffentliche Institutionen oder ein Herausgabeverlangen

35 Zum Begriff der Datenspuren *Bär*, in: Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl. (2025), 30. Kap. Rn. 120.
36 Vgl. Art. 32 der Cybercrime Convention.
37 Unter dem Hinweis, dass die Besonderheiten der elektronischen Daten nicht hinreichend in der StPO berücksichtigt werden *Warken*, NZWiSt 2017, 449.
38 So auch bezüglich der Definition unterschiedlicher Datenklassen *Warken*, NZWiSt 2017, 449 (456).
39 Andeutend *Schlothauer*, in: Münchener Anwaltshandbuch Strafverteidigung, 3. Aufl. (2022), § 3 Rn. 110; hinsichtlich der Datenerhebung und des Datenumfangs ebenfalls zust. *BGH*, BeckRS 2025, 9876 Rn. 46.
40 Vgl. *BGH*, BeckRS 2025, 9876 Rn. 46.
41 Nach *BGH*, BeckRS 2025, BeckRS 2025, 9876 Rn. 46 unter Verweis auf BVerfGE 113, 29 (51) findet eine weitergehende Eingrenzung wegen der Vielgestaltigkeit möglicher Sachverhalte gerade nicht statt.
42 *Hauschild*, in: MüKo-StPO, § 94 Rn. 26.

nach § 95 StPO[43] stellt. Gleiches gilt für die Frage, ob eine vorläufige Sicherstellung in Betracht kommt, wie die Maßnahme konkret durchgeführt wird und wie lange sie andauert.[44] Damit können die Ermittlungsbehörden selbst nach pflichtgemäßem Ermessen einschätzen, ob alternative Maßnahmen genügen und ob diese auch gleich effektiv sind.[45]

Dieser Handlungsspielraum ist nicht zu unterschätzen, da dies zwar anerkennenswerterweise auch eine hinreichende Einzelfallgerechtigkeit ermöglicht, aber zum anderen eine nicht nur unerhebliche Missbrauchsgefahr birgt, da eine inhaltliche Ermessenskontrolle durch die Gerichte insoweit nicht stattfindet.[46]

2. Anwendung unmittelbaren Zwangs

Wie sich der weite Ermessensspielraum in der Praxis auswirkt, zeigt Folgendes: Die Sicherstellung von Daten auf einem verschlüsselten Endgerät hatte bislang die Ermittlungsbeamten stets vor Schwierigkeiten gestellt. So ist der Beschuldigte aufgrund des Nemo-Tenetur- Grundsatzes[47] nicht dazu verpflichtet, etwaige Passwörter den Ermittlungsbehörden mitzuteilen.[48] Bei normalen Passwort-Barrieren bestehen allerdings häufig alternative Möglichkeiten zur Entschlüsselung, wie etwa das kryptographische Verfahren oder Kenntniserlangung des Passworts dank Übermittlung durch Telekommunikationsdienstleister gemäß § 100j Abs. 1, 3 StPO.[49]

Bislang lag die Schwierigkeit von Verschlüsselungsmechanismen auf den biometrischen Verschlüsselungen. Indes scheint diese Problematik angesichts der vergangenen Entscheidungen des *OLG Bremen*[50] und jüngst des *BGH*[51] nunmehr rein theoretischer Natur, da hiernach die Entsperrung eines Mobiltelefons durch Auflegen des Fingers des Beschuldigten – auch mittels unmittelbaren Zwangs auf Basis von § 81b Abs. 1 StPO – strafprozessual zulässig sei. Im Ergebnis scheint es wortwörtlich nicht mehr in der Hand des Beschuldigten zu liegen, ob die Ermittlungsbeamten Zugriff auf die persönlichen Daten erlangen oder nicht.

Zu Recht wurde in der Vergangenheit starke Kritik geäußert, insbesondere dahingehend, dass so der Weg geebnet werde, die Erstellung von Kommunikations-, Bewegungs- und Persönlichkeitsprofilen durch den nachgelagerten Datenzugriff zu ermöglichen.[52] Diese einstige Problematik im Umgang mit Daten auf verschlüsselten Datenträgern wird sich so daher stärker von der Praxis auf die gerichtliche Auseinandersetzung verlagern. Umso wichtiger ist es daher zu fragen, ob die strafprozessualen Vorschriften der StPO *de lege lata* im Falle eines rechtswidrigen Vorgehens durch die Ermittlungsbeamten dem Beschuldigten ausreichende Rechtsbehelfe zur Seite stellen.

43 *Engelhart*, in: NK-StPO, § 94 Rn. 22.
44 Vgl. *Greven*, in: KK-StPO, § 94 Rn. 4b.
45 *Engelhart*, in: NK-StPO, § 94 Rn. 22.
46 Unter dem Hinweis, dass eine eigene Bewertung des Ermittlungsrichters hinsichtlich des erforderlichen und verhältnismäßigen Umfangs nicht erfolgt, vgl. *BGH*, NStZ 2021, 623 Rn. 18.
47 Ausführlich *Rogall*, in: FS Beulke, 2015, S. 973 ff.; *Wegner*, in: FS Ignor, S. 853 ff.
48 *Martini/Möslein/Rostalski*, Recht der Digitalisierung, 2023, § 12 Rn. 43; *Jahn/Brodowski*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren, 2023, S. 67 (76).
49 *Martini/Möslein/Rostalski*, Recht der Digitalisierung, § 12 Rn. 43.
50 *OLG Bremen*, BeckRS 2025, 295.
51 *BGH*, BeckRS 2025, 9876.
52 *Wegner*, in: FS Ignor, S. 853 ff.; *OLG Bremen*, NJW 2025, 847; m. krit. Anm. *El-Ghazi*, NJW 2025, 847 (850).

3. Einbeziehung Dritter zur Datenauswertung

Hervorzuheben ist schließlich, dass Ermittlungsbehörden in der Praxis oft selbst aufgrund personeller Engpässe nicht (vollständig) die Auswertungsarbeit von *Big Data*-Verfahren vollbringen können. Naheliegend erscheint die Hinzuziehung von IT-Spezialisten, wobei es sich hierbei vornehmlich um private Unternehmen als Wirtschaftsakteure[53] handelt. Vielfach werden diese von der Staatsanwaltschaft als Sachverständige i.S.d. § 73 StPO eingesetzt, ohne dass es hierbei einer eingehenden Prüfung hinsichtlich der Qualifikation des Gutachters bedürfe.[54] Ein solches Vorgehen in der Praxis erscheint angesichts der (noch aufzuzeigenden) Grundrechtsrelevanz dieser Tätigkeit äußerst bedenklich und birgt die Gefahr, dass bei der Auswertung „Inhalte meist isoliert und nicht kontextbezogen bewertet werden."[55] Auch ließe dies den Schluss zu, dass „Sachbeweise selektiv in das Verfahren eingeführt werden"[56] könnten.

4. Zwischenfazit: Weite Eingriffsmöglichkeiten in die digitalen Daten des Betroffenen

Festzuhalten ist, dass den Ermittlungsbehörden unter dem derzeitigen Regelungskonzept der Beschlagnahme weitreichende Eingriffsmöglichkeiten zugestanden werden. Angesichts dessen erscheint eine fachliche Expertise, eine vollständige Dokumentation des Vorgehens sowie die Sicherstellung der Integrität und Authentizität digitaler Daten als Beweismittel zwingend geboten.[57]

IV. Welche Rolle spielen die Beschuldigtenrechte bei der Datenbeschlagnahme (noch)?

Im weiteren Verlauf ist zu klären, welche Beschuldigtenrechte durch die Datenbeschlagnahme betroffen werden und inwieweit diese mit Blick auf die vorangegangenen Darstellungen zu den weitgehenden Eingriffsmöglichkeiten durch die Ermittlungsbehörden nach dem geltenden Recht ausreichenden Schutz genießen. An dieser Stelle wird neben dem klassischen Grundrechtskatalog auf einige weitere Prozessgrundrechte eingegangen. Schließlich soll die Eingriffsintensität der Datenbeschlagnahme jeweils näher beleuchtet werden.

1. Die durch die Datenbeschlagnahme betroffenen Rechte des Beschuldigtengrundrechte

a) Allgemeines Persönlichkeitsrecht

aa) Grundlegender Digitalitätsbezug

Dass beim Zugriff auf persönliche Daten – bspw. auf Smartphones – zunächst ein Eingriff in das allgemeine Persönlichkeitsrecht in Betracht kommt,[58] liegt auf der Hand. In einem Zeitalter, in dem sich die Interaktion zu anderen Mitmenschen zunehmend auf die digitale Welt des Internets verlagert und der Umgang mit Freunden von

[53] Vgl. *Basar*, in: Sosnitza et al., Digitalisierung im Europäischen Recht, 2022, S. 19 (25); zur Zulässigkeit externer privater Dienstleister vgl. *OLG Rostock*, SVR 2016, 76.
[54] *Basar*, in: Sosnitza et al., S. 19 (26).
[55] *Basar*, in: Sosnitza et al., S. 19 (27).
[56] *Basar*, in: Sosnitza et al., S. 19 (30).
[57] *Jahn/Brodowski*, in: Hoven/Kudlich, S. 67 (92); im Einzelnen *Momsen*, in: FS Beulke, S. 871 (S. 881, 883 ff.).
[58] Vgl. *OLG Bremen*, NJW 2025, 847; m. krit. Anm. *El-Ghazi*, NJW 2025, 847 (850).

jungen Jahren an aktiv über das eigene Smartphone oder Soziale Netzwerke gelebt wird, kann man von einer zweiten „Online-Identität“[59] sprechen. Betrachtet man das eigene Online-Verhalten tatsächlich als „identitätsstiftend oder -prägend“,[60] erscheint es angezeigt, das allgemeine Persönlichkeitsrecht mit seinem verfassungsrechtlichen Schutzgehalt auch auf den persönlichen Online-Avatar zu übertragen. Eine Datenbeschlagnahme, z.B. durch Kopie von Bewegungsdaten auf dem Smartphone oder durch Beschlagnahme eines Social-Media-Accounts, kann einen nicht nur unerheblichen Eingriff in die freie Entfaltung der Persönlichkeit mit sich bringen. Jemand, der nicht abschätzen kann, welche Informationen der eigenen Persönlichkeit nach außen getreten sind, kann in der Zukunft wohl kaum in freier Selbstbestimmung seine Persönlichkeit entfalten.

bb) Recht auf informationelle Selbstbestimmung

Grundlegend durch die Entscheidung des *BVerfG*[61] aus dem Jahre 1983 geprägt, müsse die individuelle Selbstbestimmung den Bedingungen der modernen Informationsgesellschaft und -technologie hinreichend Rechnung tragen. Das *BVerfG* erkannte an, dass der Einzelne in seiner Freiheit, aus eigener Selbstbestimmung zu planen, wesentlich gehemmt sei, wenn er nicht hinreichend erkennen könne, welche Informationen in seiner sozialen Umgebung bereits bekannt seien. Im Ergebnis stellte das *BVerfG* in dieser Entscheidung heraus, dass Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG dem Einzelnen das Recht verleihe, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten“[62] zu entscheiden.

Gleichwohl sei dieses Recht nicht so zu verstehen, dass es sich dabei um eine „absolute, uneinschränkbare Herrschaft über [die eigenen] Daten“[63] handele, sondern – auch personenbezogene – Daten grundsätzlich als „Abbild sozialer Realität“ einer alleinigen Zuordnung zum Betroffenen entgegenstünden. Folglich könne dieses Grundrecht auch im überwiegenden Allgemeininteresse eingeschränkt werden. Einschränkend konkretisierte das *BVerfG* dieses überwiegende Allgemeininteresse dahingehend, dass dieses jedenfalls nur „an Daten mit Sozialbezug […] unter Ausschluss unzumutbarer intimer Angaben und von Selbstbezichtigungen“[64] bestehen könne.

Aus dieser Entscheidung folgt, dass jedenfalls unzumutbare intime Daten und Daten mit Selbstbezichtigungsgehalt nicht durch die Beschlagnahmeregelungen sichergestellt werden dürften. Gleichwohl wird man bei Daten, die im Zusammenhang mit einer Straftat stehen, einen Sozialbezug bejahen müssen und ein grundsätzliches Aufklärungsinteresse der Gesellschaft nicht ausschließen können. Das Aufklärungsinteresse kann jedoch nicht als Argument dazu dienen, dass grundsätzlich durch die Datenbeschlagnahme von sensiblen Daten die Möglichkeit zur Erstellung von Persönlichkeitsprofilen eröffnet werde. Auf diese Gefahr wird im Folgenden unter dem Gesichtspunkt der Eingriffsintensität näher eingegangen.

cc) Recht auf Gewährleistung informationstechnischer Systeme

Als weitere Ausprägung des allgemeinen Persönlichkeitsrechts ist durch das *BVerfG*[65] das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zuerkannt worden. Hiernach erfasst der Schutzgehalt des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das „Interesse […] dass die von einem […]

59 Hierzu *Hoffmann/Luch/Schulz/Borchers*, Digitale Dimension der Grundrechte, 2015, S. 46 f.
60 Hierzu *Hoffmann/Luch/Schulz/Borchers* (Fn. 59), S. 46 f.
61 BVerfGE 65, 1.
62 BVerfGE 65, 1 (43).
63 BVerfGE 65, 1 (43 f.).
64 BVerfGE, 65 1 (46).
65 BVerfGE 120, 274.

informationstechnischen System erzeugten, verarbeiteten, und gespeicherten Daten vertraulich bleiben."[66] Das *BVerfG* stellte in dieser Entscheidung insbesondere klar, dass die Schutzdimension des Grundrechts unabhängig vom Aufwand des Zugriffs auf die informationstechnischen Systeme bestehe. Damit dürfte das Grundrecht sowohl bei verschlüsselten als auch unverschlüsselten Daten zum Tragen kommen.[67]
Vor dem Hintergrund, dass der Zugriff auf die Datenmassen auf IT-Systemen, wie Smartphones, ohne Weiteres die Erstellung von Kommunikations-, Bewegungs- und Persönlichkeitsprofilen ermögliche, könne man zu Recht mit kritischem Auge betonen, dass solche Geräte und die Zugriffsmöglichkeit samt den hierauf befindlichen Daten eine wahre Goldgrube für die Ermittlungsbehörden darstellen.[68] Insoweit müsse ein besonderer Schutz gewährleistet werden.[69]

b) Pressefreiheit

Erfolgt die Datenbeschlagnahme gegenüber in der Presse tätigen Personen, so ist der Eingriff ferner am Maßstab der Pressefreiheit zu messen. Art. 5 Abs. 1 S. 2 GG schütze nach ständiger Rechtsprechung „vor dem Eindringen des Staates in die Vertraulichkeit der Redaktionsarbeit sowie in die Vertrauenssphäre zwischen Medien und ihren Informanten."[70] Dabei sei die konstituierende Bedeutung der freien Presse für die freiheitliche demokratische Grundordnung besonders hervorzuheben. Da die Gewährleistung privater Mitteilungen als Informationsquelle für die Presse ein unabdingbares Hilfsmittel darstelle, handele es sich bei einer Beschlagnahme von Datenträgern und der damit verbundenen Auswertung von redaktionellem Datenmaterial um einen besonders intensiven Eingriff in die Vertraulichkeit der Redaktionsarbeit und in das Vertrauensverhältnis zu Informationsgebern. Die Bedeutung des Grundrechts müsse schließlich vor dem Hintergrund gesehen werden, dass der in § 97 Abs. 5 S. 1 StPO verankerte Beschlagnahmeschutz für Pressemitarbeiter in Einzelfällen nicht greife. Damit weist die Datenbeschlagnahme eine gewichtige Grundrechtsrelevanz auf.

c) Post- und Fernmeldegeheimnis

Diskutabel erscheint auch das Brief-, Post- und Fernmeldegeheimnis aus Art. 10 GG. Art. 10 GG dient der freien Persönlichkeitsentfaltung durch die Gewährleistung privater Kommunikation und stellt damit ebenfalls ein zentrales Gut von Verfassungsrang dar.[71] Aufgrund der Entwicklungsoffenheit[72] ließe sich die Betroffenheit des Grundrechts mit Blick auf die Beschlagnahme von E-Mail-Verläufen oder Chats aus sozialen Netzwerken, wie WhatsApp oder Instagram, begründen.[73] Gleichwohl konzentriert sich Art. 10 GG nur auf den laufenden Kommunikationsprozess, sodass der Schutzbereich des Art. 10 GG jedenfalls dann endet, wenn E-Mails, Chats oder ähnliche Nachrichtenverläufe auf dem System des Endnutzers gespeichert werden.[74]

66 BVerfGE 120, 274 (314).
67 Vgl. bei dem offenen Zugriff auf komplexe IT-Systeme *OLG Bremen*, NJW 2025, 847; m. krit. Anm. *El-Ghazi*, NJW 2025, 847 (850).
68 *OLG Bremen*, NJW 2025, 847; m. krit. Anm. *El-Ghazi*, NJW 2025, 847 (850).
69 *OLG Bremen*, NJW 2025, 847; m. krit. Anm. *El-Ghazi*, NJW 2025, 847 (850).
70 *BVerfG*, BeckRS 2015, 51131 Rn. 16.
71 Vgl. *Hoffmann/Luch/Schulz/Borchers* (Fn. 59), S. 177.
72 Zum Fernmeldegeheimnis BVerfGE 46, 120 (134, 139, 141).
73 *Hoffmann/Luch/Schulz/Borchers* (Fn. 59), S. 181 f.
74 *Hoffmann/Luch/Schulz/Borchers* (Fn. 59), S. 182 f.

Chats auf sozialen Netzwerken werden jedoch üblicherweise auf dem Nutzerkonto des Sozialen Netzwerkes gespeichert und nicht unmittelbar auf dem eigenen Smartphone, Laptop oder Ähnlichem, sodass es durchaus vertretbar erscheint, wenn man in solchen Fällen noch einen laufenden Kommunikationsvorgang annehme.[75]
Folglich birgt die Datenbeschlagnahme je nach Einzelfall eine nicht unerhebliche Gefahr für den privaten Kommunikationsverkehr.[76] Auch begründet der offene Zugriff die Gefahr, dass Betroffene das Erlebnis eines nachträglichen „Überwachungsstaates" vermittelt bekommen und sich bei künftigen Kommunikationsvorgängen in ihrer freien kommunikativen Form der Persönlichkeitsentwicklung wesentlich gehemmt sehen können.[77]

d) Berufsfreiheit

Die Berufsfreiheit gewährleistet die Freiheit der beruflichen Betätigung und schützt die Berufswahl sowie die Berufsausübung.[78] Die Berufsfreiheit kann dann durch die Beschlagnahme berührt werden, wenn Daten betroffen sind, die im Zusammenhang mit der beruflichen Tätigkeit einer Person stehen.[79] Eine Arbeit ohne Internet scheint bereits jetzt in vielen Bereichen undenkbar. Werden sämtliche EDV-Geräte oder Programme beschlagnahmt, kann dies dazu führen, dass der Geschäftsbetrieb vorübergehend lahmgelegt wird.[80] Indes sprechen vielfach Gerichte den Normen der §§ 94 ff. StPO die für den Eingriff in die Berufsfreiheit notwendige berufsregelnde Tendenz ab.[81] Folgt man dem, so verbleibt für Gefahren im Zusammenhang zu Unternehmensstrukturen nur der Anwendungsbereich der allgemeinen Handlungsfreiheit gemäß Art. 2 Abs. 1 GG.[82]

e) Recht auf Unverletzlichkeit der Wohnung

Nicht betroffen wird durch die Datenbeschlagnahme das Grundrecht auf Unverletzlichkeit der Wohnung gemäß Art. 13 Abs. 1 GG. Zwar greift die vorangehende Durchsuchung in Wohn- oder Geschäftsräume regelmäßig in dieses Grundrecht ein. Die Datenbeschlagnahme als „Resultat einer Wohnungsdurchsuchung"[83] unterfällt jedoch nicht mehr dem sachlichen Schutzbereich des Art. 13 Abs. 1 GG.[84]

f) Eigentumsfreiheit

Da bei einer Beschlagnahme regelmäßig eine andauernde Besitzentziehung der zu beschlagnahmenden Gegenstände einhergeht, ist an die Betroffenheit des Art. 14 Abs. 1 GG zu denken. Hier stellen sich jedoch angesichts der Unkörperlichkeit ähnliche Probleme wie bei der Einordnung der Daten unter den Begriff des Gegenstandes. Grundsätzlich schützt Art. 14 Abs. 1 GG nur Sacheigentum. Nach aktueller Rechtslage ließe sich zivilrechtlich

75 Zutreffend *Hoffmann/Luch/Schulz/Borchers* (Fn. 59), S. 182 f.
76 Unter dem Gesichtspunkt der unbeobachteten Fernkommunikation vgl. BVerfGE 120, 274 (323).
77 Insoweit wird hier der Gedanke des „*chilling effect*" übertragen; zum „*chilling effect"* im Rahmen des „*Predictive Policing*" vgl. *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. (2021), G. Rn. 1346.
78 BVerfGE 113, 29 (45, 48).
79 So etwa bei der Beschlagnahme von Datenträgern einer Rechtsanwalts- und Steuerberaterkanzlei vgl. BVerfGE 113, 29 (48).
80 Argumentierend, dass es hierbei auf eine faktische Enteignung hinauslaufe *Gercke*, in: HK-StPO, § 94 Rn. 57.
81 BVerfGE 113, 29 (48).
82 Beispielsweise im Falle des möglichen Verlusts von Geschäftsbeziehungen bei der Gefahr der Bekanntgabe von vertraulichen Daten durch die Datenbeschlagnahme BVerfGE 113, 29 (49) m.w.N.
83 *BVerfG,* NJW 2009, 2431 (2433).
84 BVerfGE 113, 29 (45); *BVerfG*, NJW 2009, 2431 (2433).

allenfalls ein Datenbesitz analog §§ 854 ff. BGB konstruieren; ein Dateneigentum als rechtlich anerkannte Rechtsposition könne gegenwärtig mangels gesetzlicher Zuweisung von Nutzungs-, Verfügungs- oder Verwertungsbefugnissen nicht angenommen werden.[85] Bei Unternehmen wäre an das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb zu denken.[86]

2. Weitere spezielle (Verfahrens-)Grundrechte

Konstitutiv für die Beschuldigtenrechte ist auch der gesetzliche Anspruch auf rechtliches Gehör, welcher verfassungsrechtlich in Art. 103 Abs. 1 GG verankert ist. So führt das *BVerfG* in seiner Rechtsprechung[87] zutreffend aus, dass eine Beschlagnahme zur Beweissicherung die Dispositionsfreiheit des Betroffenen als Eigentümer über die Beschlagnahmegegenstände dergestalt einschränke, dass hieraus ein bleibender rechtlicher Nachteil entstünde, der nicht oder nicht vollständig behoben werden könne. Unter Heranziehung des Gedankens des Rechtsstaatsprinzips müsse – so das *BVerfG* ferner – dem betroffenen Eigentümer schon bei diesem ersten Eingriff und nicht erst bei einer späteren möglichen Einziehung im Beschwerdeverfahren ohne Einschränkung rechtliches Gehör gewährt werden.

Zwar bildet eine vorherige Anhörung den Grundsatz. Eine Einschränkung erfährt dieser Grundsatz aber dort, wo sie den Zweck der Maßnahme vereiteln würde, worunter exemplarisch auch die Beschlagnahme fällt.[88] Der Rechtsstaatsgedanke gebiete dennoch, dass dem Betroffenen nachträglich Gelegenheit zur Stellungnahme gewährt und die Maßnahme einer gerichtlichen Entscheidung zugeführt werden müsse.[89] Mögliche Spannungen können sich hierbei mit Blick auf die bestehenden Rechtsschutzmöglichkeiten im Zusammenhang mit der Datenbeschlagnahme ergeben, worauf im weiteren Verlauf der Bearbeitung noch eingegangen wird.

Es ist jedoch zu beachten, dass die nähere Ausgestaltung dieses Verfahrensgrundrechts über die einzelnen Verfahrensordnungen erfolgt.[90] Im Strafverfahren finden sich diese Anforderungen im Recht auf Akteneinsicht des Beschuldigten und seines Verteidigers gemäß § 147 Abs. 1, Abs. 4 S. 1 StPO wieder. Möchte man die beschlagnahmten Daten als Beweisstück[91] oder als Aktenbestandteil[92] klassifizieren, so müsse man konsequenterweise dem Betroffenen und seinem Verteidiger ein Akteneinsichtsrecht bzw. ein Recht auf Besichtigung dieser Daten gestatten. Solange dies – unterstellt – über die Bereitstellungsmöglichkeit nach § 32f StPO[93] hinreichend gewährleistet wird, scheidet eine Verletzung des Verfahrensgrundrechts aus.

Im Zusammenhang mit Daten beschäftigt sich die Rechtsprechung zunehmend mit dem Grundsatz des fairen Verfahrens.[94] Aus diesem Grundsatz folge grundsätzlich, dass dem Betroffenen nach der Datenbeschlagnahme ein vergleichbarer Informations- und Erkenntnisstand wie der Ermittlungsbehörde zugänglich gemacht werden müsse,

85 Zu alldem *Michl*, NVwZ 2019, 1631 (1635).
86 So *Gercke*, in: HK-StPO, § 94 Rn. 56.
87 BVerfGE 18, 399 (404).
88 Vgl. *Dahs*, Das rechtliche Gehör im Strafprozess, 1965, S. 58, 64 f.
89 *Dahs*, S. 65 m.w.N.
90 BVerfGE 18, 399 (405); BVerfGE 9, 89 (95 f).
91 Unter überzeugender Differenzierung zwischen dem Datenträger als solchem, der Mitnahme des Datenträgers und anschließender Kopie des Datensatzes und der sofortigen Mitnahme einer Datenkopie vgl. *Bell*, S. 13 ff., S. S. 66 ff., S. 146 ff.
92 So mangels Augenscheinsobjektqualität *Kämpfer/Travis*, in: MüKo-StPO, § 147 Rn. 23a; ferner *Thiele*, in: NK-StPO, § 147 Rn. 27.
93 Seit dem Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5.7.2018, BGBl. 2017 I, S. 2208.
94 Ausführlich zum Grundsatz des fairen Verfahrens BVerfGE 133, 168 (200).

um sich in angemessener Form gegen Eingriffe zur Wehr setzen zu können.[95] Folglich ließe sich hieraus ein Anspruch auf Bereitstellung sämtlich verfahrensbezogener Daten ableiten, auch wenn einzelne Daten nicht Bestandteil der Akte geworden sind.[96] Dieses Recht findet seine Grenze allerdings in einem über existente Beweismittel hinausgehenden Verlangen.[97] Der Grundsatz des fairen Verfahrens kann jedoch dann verletzt sein, wenn solche Beweismittel verwertet werden, denen eine schwerwiegende Rechtsverletzung zugrunde liegt.[98]

3. Zur Eingriffsintensität

Die Beurteilung, inwieweit ein Eingriff in die Grundrechte des Betroffenen als erheblich zu beurteilen sind, ist einzelfallabhängig. Dennoch ist bei der Beschlagnahme von Datensätzen davon auszugehen, dass diese in der Regel – unabhängig von privaten oder juristischen Personen – eine weitaus größere Dichte annehmen können als dies bei analogen Beweismitteln der Fall wäre.

Das *BVerfG* stellte bereits bei seiner Entscheidung aus dem Jahre 2005[99] wegweisend heraus, dass sich die besondere Eingriffsintensität bei Datenzugriffen daraus ergäbe, dass eine solche strafprozessuale Maßnahme wegen der Vielzahl verfahrensunerheblicher Daten eine Streubreite aufweise und daher zahlreiche Personen in den Wirkungskreis der Maßnahme mit einbezogen werden, die in keiner Beziehung zu dem Tatvorwurf stünden und den Eingriff durch ihr Verhalten nicht veranlasst hätten. Hinzu komme, dass bei Berufsgeheimnisträgern regelmäßig auch das zugrundeliegende Vertrauensverhältnis zu Kunden/Mandanten erheblich erschüttert werden könne und in die Abwägung miteingestellt werden müsse. Bei Privaten ist überdies ins Feld zu führen, dass die Gefahr der Erstellung umfassender Persönlichkeitsprofile der Bürger besteht.[100]

Auch der jüngsten Entscheidung des *BGH* zur Zulässigkeit der zwangsweisen Entsperrung eines Smartphones lässt sich entnehmen, dass der Zugriff auf Smartphone-Daten einen besonders schwerwiegenden Eingriff in das Recht des Beschuldigten auf informationelle Selbstbestimmung darstelle, der sich auch nicht zwingend durch die Tatsache, dass es sich hierbei um eine offene Ermittlungsmaßnahme handele, entkräftigt werde.[101] Vielmehr sei anzuerkennen, dass sich auf dem Speichermedium eine „Vielzahl an vertraulichen und höchstpersönlichen Daten […] die bei dem Zugriff […] potentiell der Kenntnisnahme der Ermittlungsbehörden unterliegen“[102], befinden. Dies lasse Erkenntnismöglichkeiten qhinsichtlich politischer, religiöser oder weltanschaulicher Überzeugungen und damit auf die Persönlichkeit des Betroffenen oder gar die Bildung von Verhaltens- bzw. Kommunikationsprofilen zu.[103] Folglich macht der Zugriff auf Daten oder auf sonstige Gegenstände einen weitreichenden qualitativen Unterschied.

Zusammenfassend ließe sich hier erneut das *BVerfG* anführen, dass zutreffend herausstellte, dass „die Ermittlungsmethoden der StPO […] im Hinblick auf die Datenerhebung und den Datenumfang weit gefasst“[104] seien – vielleicht zu weit?

95 Unter dem Gesichtspunkt der Parität des Wissens *OLG Koblenz*, BeckRS 2020, 42647 Rn. 23 f.
96 Vgl. *OLG Karlsruhe*, NZV 2020, 368 (369).
97 *OLG Koblenz*, BeckRS 2020, 42647 Rn. 24.
98 Etwa bei grober Verkennung der Rechtslage *Gercke*, in: HK-StPO, § 94 Rn. 70; *BGH*, NJW 2007, 2269 (2271).
99 BVerfGE 113, 29 (53).
100 *Bildner*, in: Zöller (Hrsg.), Digitalisierung im Straf- und Strafprozessrecht, KriPoZ-JuP 2021, 4 (17); *Singelnstein*, NStZ 2012, 593 (606).
101 *BGH,* BeckRS 2025, 9876 Rn. 33.
102 *BGH*, BeckRS 2025, 9876 Rn. 33.
103 *BGH*, BeckRS 2025, 9876 Rn. 33.
104 BVerfGE 113, 29 (52).

4. Mechanismen zum Schutz der Beschuldigtenrechte nach geltendem Recht

Angesichts der erheblichen Grundrechtsrelevanz und Eingriffsintensität der Datenbeschlagnahme ist zu analysieren, inwieweit die Instrumente des geltenden Rechts einen ausreichenden Schutz der Beschuldigtenrechte gewährleisten.

a) Die Begrenzungsfunktion des Legalitätsprinzips?

Freilich unterliegt § 94 StPO dem Legalitätsprinzip,[105] wonach die Strafverfolgungsbehörden bei tatsächlichen Anhaltspunkten für eine verfolgbare Straftat zum Einschreiten verpflichtet sind,[106] vgl. § 152 Abs. 2 StPO. Daraus folgt, dass auch bei der Beschlagnahme jedenfalls ein Anfangsverdacht vorliegen muss.[107] Erforderlich, aber ausreichend ist daher, dass bereits vor Beginn einer Durchsuchung[108] entsprechende tatsächliche Anhaltspunkte für den konkreten Verdacht des Vorliegens einer Straftat bestehen.[109] Zugleich sind nur solche Gegenstände zu beschlagnahmen, die als Beweismittel für die Untersuchung von Bedeutung sein können, vgl. § 94 Abs. 1 Hs. 1 StPO, mithin solchen, denen eine potenzielle Beweisbedeutung[110] zukommt. Der bereits skizzierte Anfangsverdachts-Maßstab ist auch hinsichtlich der Beweisbedeutung zugrunde zu legen, sog. Auffindeverdacht.[111] Folglich wird die Bewertung, ob eine hinreichende Beweisbedeutung vorliegt, regelmäßig positiv ausfallen, wenn aus ex-ante-Sicht[112] die Erwartung besteht, dass eben jener Gegenstand bzw. dessen Untersuchung Rückschlüsse auf verfahrensrelevante Tatsachen ermöglichen könnte.[113] Dabei ist die potentielle Beweismitteleigenschaft gerade im EDV-Bereich stets im Einzelfall zu prüfen.[114] Zu klären ist daher stets, ob auf dem Smartphone gespeicherten Daten eine potentielle Beweisbedeutung zukommt.

Da *Big Data*[115] ein vergleichsweises relativ junges Phänomen ist, liegt es auf der Hand, dass Daten kein eigenständiges Beweismittel[116] in der Strafprozessordnung darstellen. Mittels Ausdrucks von Chatnachrichten, E-Mails oder Screenshots von Profilen ließe sich jedoch über den Augenscheins- und Urkundsbeweis[117] eine entsprechende Einführung in das Hauptverfahren konstruieren. Auch erscheint ein Zeugenbeweis denkbar.[118] Wenn man über die vielfachen Datenaufzeichnungen und Speicherungsvorgänge – beispielsweise durch autonome Fahrassistenzsysteme – nachdenkt, lassen sich hiermit durchaus Rückschlüsse auf relevante Handlungszeitpunkte einer möglichen Tat ziehen, wie bereits das eingangs erwähnte Mord-Beispiel illustriert. Folglich wird man Daten wohl eine potentielle Beweisbedeutung beimessen können.

105 *Hauschild*, in: MüKo-StPO, § 94 Rn. 14; *Greven*, in: KK-StPO, § 94 Rn. 12; *Menges*, in: LR-StPO, § 94 Rn. 50.
106 *Park*, Durchsuchung und Beschlagnahme, 5. Aufl. (2022), § 3 Rn. 506; *Greven*, in: KK-StPO, § 94 Rn. 12.
107 Hierzu im Einzelnen *Greven*, in: KK-StPO, § 94 Rn. 8; *Sieber*/*Brodowski* (Fn. 8); Teil 19.3 Rn. 71; *Roxin*/*Schünemann* (Fn. 24), § 34 Rn. 5; *BVerfG*, BeckRS 2015, 52454.
108 Vgl. *BVerfG*, BeckRS 2020, 18937 Rn. 43; *LG Mainz*, BeckRS 2019, 25962 Rn. 9; *Greven*, in: KK-StPO, § 94 Rn. 8.
109 *Greven*, in: KK-StPO, § 94 Rn. 8.
110 Vgl. *Engelhart*, in: NK-StPO, § 94 Rn. 14; *Park* (Fn. 106), § 3 Rn. 496 ff.; *Greven*, in: KK-StPO, § 94 Rn. 11.
111 Zum Begriff vgl. BVerfGE 113, 29 (57); BVerfGE 124, 43 (66 f.); *Köhler*, in: Schmitt/Köhler, StPO, 68. Aufl. (2025), § 94 Rn. 19a.
112 *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 8; *Hauschild*, in: MüKo-StPO, § 94 Rn. 21; *Engelhart*, in: NK-StPO, § 94 Rn. 14; *BGH*, BeckRS 2018, 15545 Rn. 6.
113 Vgl. *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 11; *Hauschild*, in: MüKo-StPO, § 94 Rn. 21.
114 *Marbeth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl. (2010), S. 219.
115 Ausführlich zum Begriff *Braun*, in: SWK Legal Tech, 2023, Big Data, Rn. 1-15.
116 *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2. Aufl. (2023), Rn. 984.
117 *Brunst*, in: Gercke/Brunst, Rn. 985; *Marbeth-Kubicki*, S. 219.
118 Näher *Brunst*, in: Gercke/Brunst, Rn. 986.

Festzuhalten ist im Ergebnis, dass eine Datenbeschlagnahme erst dann in Betracht kommt, wenn bereits tatsächliche Anhaltspunkte auf die Begehung einer Straftat hindeuten und für die zu beschlagnahmenden Daten ebenfalls Anhaltspunkte bestehen, die für eine Verwendbarkeit im Verfahren sprechen. Eine Datenbeschlagnahme aus willkürlichen Gesichtspunkten[119] oder „ins Blaue hinein"[120] scheint damit zumindest auf den ersten Blick ausgeschlossen. Gleichwohl begründet ein Handeln allein auf der Annahme eines Anfangsverdachts einen weiten Ermessensspielraum,[121] da sich ein Anfangsverdacht auch durch legales Verhalten in Kombination mit weiteren Anhaltspunkten begründen ließe.[122]

b) Hinreichender Schutz durch die Anwendung des Verhältnismäßigkeitsgrundsatzes?

Die Ermessensentscheidung[123] im Rahmen der Beschlagnahme unterliegt jedoch nicht nur einem reinen Willkürverbot, sondern ist am Grundsatz der Verhältnismäßigkeit zu messen, welcher sich nach dem verfassungsrechtlichen Maßstab richtet.[124] Dass dem Verhältnismäßigkeitsgrundsatz im Rahmen der Beschlagnahme hinreichend Rechnung zu tragen ist,[125] ergibt sich im einfachen Recht aus § 73a S. 1 RiStB und gebietet, dass im Einzelfall zu prüfen ist, ob die Maßnahme hinsichtlich des angestrebten Ziels geeignet, erforderlich und angemessen ist,[126] sog. Übermaßverbot.[127] So wird in ständiger Rechtsprechung vertreten, dass die Beschlagnahme in angemessenem Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen sowie für die Ermittlungen notwendig sein müsse.[128]

Vor diesem Hintergrund könnte man vertreten, dass der Einzelfallgerechtigkeit über den Weg der Verhältnismäßigkeit hinreichend gedient ist, ohne dass es einer weiteren Anpassung bedürfe. Dafür könnte sprechen, dass bei korrekter Ermessensausübung unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes die Beschlagnahme bereits in ihrer Art und ihrem Umfang nach ausreichend begrenzt wird. Dies ist im Folgenden näher zu untersuchen.

aa) Begrenzung hinsichtlich der Maßnahmenform

Während die Geeignetheit der Beschlagnahme in der Regel wohl nur ausnahmsweise[129] abzulehnen sein wird, wird man im Rahmen der Erforderlichkeit stets alternative Handlungsmöglichkeiten in Erwägung ziehen können und müssen, die weniger eingriffsintensiv sind. In Betracht kommen etwa ein Auskunftsverlangen gegenüber öffentlichen Institutionen[130] oder ein Herausgabeverlangen nach § 95 StPO[131] in Verbindung mit der Androhung

119 *Hoven*, NStZ 2014, 361 (363 f.).
120 *Wohlers/Singelnstein*, in: SK-StPO, § 94 Rn. 18; vgl. auch *Hauschild*, in: MüKo-StPO, § 94 Rn. 17; *BGH,* NStZ 2001, 604 (606).
121 *Hoven*, NStZ 2014, 361.
122 Vgl. hierzu der sog. Fall Edathy *BVerfG*, NJW 2014, 3085 (3087); näher *Hoven*, NStZ 2014, 361 (365 ff.).
123 BVerfGE 20 162 (186); 27 104 (110); a.A. *Menges*, in: LR-StPO, § 94 Rn. 50.
124 *Park* (Fn. 106), § 2 Rn. 158.
125 *Hartmann*, in: HK-GS, § 94 Rn. 9; Park (Fn. 106), § 3 Rn. 571 f.; *Sieber/Brodowski* (Fn. 8), Teil 19.3 Rn. 74; *Greven*, in: KK-StPO, § 94 Rn. 6; *Roxin/Schünemann* (Fn. 24), § 34 Rn. 26; grundlegend zur Verhältnismäßigkeit *Fischer*, in: KK-StPO, Einl. Rn. 129.
126 Vgl. *Hauschild*, in: MüKo-StPO, § 94 Rn. 23; *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 18; *Engelhart*, in: NK-StPO, StPO, § 94 Rn. 21.
127 *Hauschild*, in: MüKo-StPO, § 94 Rn. 23.
128 BVerfGE, 29 162 (186); vgl. auch *Köhler*, in: Schmitt/Köhler, StPO, § 94 Rn. 18.
129 Beispielsweise bei einem umfassenden Verwendungsverbot *Engelhart*, in: NK-StPO, § 94 Rn. 21; ferner bei evident mangelnder Beweisbedeutung vgl. *Greven*, in: KK-StPO, § 94 Rn. 7.
130 *Hauschild*, in: MüKo-StPO, § 94 Rn. 26; *Engelhart*, in: NK-StPO, § 94 Rn. 22; *BVerfG*, NJW 2012, 2096.
131 So *LG Dresden*, NZI 2014, 236 (237); *LG Saarbrücken*, NStZ-RR 2013, 183; *LG Saarbrücken*, NStZ 2010, 534 (535); *LG Bielefeld*, BeckRS 1996, 11458, vgl. auch *Park* (Fn. 106), § 3 Rn. 529; *Frister*, in: Lisken/Denninger, PolR-Hdb. F. Rn. 235.

einer Beschlagnahme.[132]

Auch müssen Dokumente nicht zwingend im Original vorliegen, um als Beweismittel zu dienen,[133] sodass regelmäßig als mildere Maßnahme die Beschlagnahme von Kopien in Betracht kommt. Dies gilt auch bei Datenbeschlagnahmen. Hier genügt es regelmäßig, wenn Kopien von Datenträgern[134] beschlagnahmt oder Screenshots[135] erstellt werden.

So sollte im Ergebnis die konkrete Beschlagnahmeform bzw. die Art des zu beschlagnahmenden Gegenstandes stets das mildeste Mittel darstellen, was im Ausgangspunkt die Überlegung zuließe, dass so die Einzelperson von vornherein keine schweren Eingriffe in ihre Grundrechte befürchten müsse. Hier ist jedoch hervorzuheben, dass die Beschlagnahme ganzer Datenbestände nicht zwingend ausgeschlossen ist, beispielsweise bei tatsächlichen Anhaltspunkten für verschlüsselte oder verborgene Daten,[136] da hier gerade ein Beweismittelverlust zu befürchten ist. Eine Unterbrechung des täglichen Geschäftsablaufs und damit einhergehender möglicher Umsatzeinbußen[137] kann nicht unter allem Umständen ausgeschlossen werden und ist daher an der Verhältnismäßigkeit im engeren Sinne zu messen.

bb) Begrenzung hinsichtlich des Maßnahmenumfangs

Ferner ermöglicht der Verhältnismäßigkeitsgrundsatz eine Begrenzung des Umfangs der Beschlagnahme. So wird nur in Einzelfällen die Erforderlichkeit der Beschlagnahme ganzer Datenbestände[138] zu bejahen sein, da grundsätzlich das Erlangen „überschießende[r], für das Verfahren bedeutungslose[r] Informationen, insbesondere vertrauliche[r] Daten Unbeteiligter“[139] nicht dem Ziel der Beschlagnahme entspricht und damit bestmöglich abgewendet werden soll, sog. Grundsatz der Datensparsamkeit.[140] Wie bereits im Rahmen der Maßnahmenform gilt dieser Grundsatz jedoch nicht bedingungslos.

Schließlich spielt der Verhältnismäßigkeitsgrundsatz auch für die zeittechnische Begrenzung der Beschlagnahme eine Rolle, da *de lege lata* eine Beschlagnahmedauer gesetzlich nicht festgeschrieben ist. Damit kann eine Beschlagnahme wegen ihrer Dauer unverhältnismäßig werden,[141] was sich nach den Umständen des Einzelfalles bemisst und eine exakte zeitliche Grenze[142] unmöglich macht. Zwar könne der Ermittlungsrichter die Beschlagnahme mittels Anordnung befristen,[143] doch ist dies gesetzlich nicht zwingend festgelegt. Dies birgt Rechtsunsicherheiten und führt im Ergebnis dazu, dass Daten unter Umständen auch für mehrere Monate oder gar Jahre[144]im Verbleib der Ermittlungsbehörden stünden.

---

132 *Engelhart*, in: NK-StPO, § 94 Rn. 22.
133 Vgl. *Engelhart*, in: NK-StPO, § 94 Rn. 23; *BGH*, NJW 1977, 1545 (1546).
134 Mit Ausnahmen vgl. *Engelhart*, in: NK-StPO, § 94 Rn. 24; *LG Lübeck*, BeckRS 2022, 5388; m. zust. Anm. *Krug*, Fachdienst Strafrecht 2022, 447817; vgl. auch *Cornelius*, NJW 2024, 2725 (2716); *Park* (Fn. 106), § 3 Rn. 529; *Greven*, in: KK-StPO, § 94 Rn. 4c; BVerfGE 113, 29 (55).
135 *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 94 Rn. 18; *Engelhar*t, in: NK-StPO, § 94 Rn. 2.
136 *Hauschild*, in: MüKo-StPO, § 94 Rn. 29; *Hartmann*, in: HK-GS, § 94 StPO Rn. 10.
137 Hierzu exemplarisch Amazon und Google aufgeführt *Brunst*, in: Gercke/Brunst, Rn. 969.
138 Vgl. *Hartmann*, in: HK-GS, § 94 StPO Rn. 10; im Einzelnen vgl. BVerfGE 113, 29 (47); *BGH*, NJW 2010, 1297 (1298).
139 Unter Verweis auf BVerfGE 113, 29; 124, 43 *Köhler*, in: Schmitt/Köhler, § 94 Rn. 18a.
140 Zum Begriff der Datensparsamkeit *Engelhart*, in: NK-StPO, § 94 Rn. 24.
141 Vgl. *Gercke*, in: HK-StPO, § 94 Rn. 58.
142 Bei EDV-Anlagen bis maximal 6 Wochen und bei Privatpersonen eher großzügiger *Gercke*, in: HK-StPO, § 94 Rn. 58.
143 *Park* (Fn. 106), § 3 Rn. 654.
144 Vgl. *Park*, in: FS Ignor, S. 757 (S. 764, 768).

cc) Begrenzung hinsichtlich des Beschlagnahmegegenstandes

Neben den Beschlagnahmeverboten aus §§ 96, 97 StPO können sich aus dem Grundsatz der Verhältnismäßigkeit[145] weitere Begrenzungen hinsichtlich des zu beschlagnahmenden Datensatzes ergeben, namentlich dann, wenn der absolute Kernbereich privater Lebensgestaltung berührt wird.[146] Damit findet durch das Verhältnismäßigkeitsprinzip ferner eine Begrenzung des Beschlagnahmegegenstandes statt.

dd) Problem: Keine gesetzliche Festschreibung der Einhaltung technischer Standards und der Verfahrensdokumentation

Problematisch erscheint, dass der Verhältnismäßigkeitsgrundsatz zwar wichtige Begrenzungen zum Schutz des Beschuldigten vorsieht, in der Praxis jedoch vielfach Schwierigkeiten auftreten, da die Einhaltung elementarer Standards und die Dokumentation des Datenbeschlagnahmeprozesses in Form der Datensicherung und IT-forensischer Auswertung im Rahmen der Beschlagnahmeregelungen der §§ 94 ff. StPO nicht festgeschrieben werden.[147] Fehlende festgeschriebene Standards lassen die Befürchtung zu, dass der Verhältnismäßigkeitsgrundsatz in der Praxis nicht immer hinreichend eingehalten wird, was für ein justizförmiges Verfahren[148] aber unabdingbar ist.

c) (Begrenzte) Schutzwirkung durch Beschlagnahmeverbote

Wie bereits angedeutet, ist zu untersuchen, wie sich die Vorschriften der Beschlagnahmeverbote zu den Entwicklungen im Zeitalter von *Big Data* verhalten. Hierzu wird im Folgenden die Vorschrift des § 97 StPO näher beleuchtet.

Geschützt werden nach § 97 Abs. 1 StPO im Einzelnen schriftliche Mitteilungen (Nr. 1), Aufzeichnungen über Mitteilungen (Nr. 2) und andere Gegenstände, auf die sich ein Zeugnisverweigerungsrecht nach § 52 StPO (nur bei Nr. 1) oder § 53 Abs. 1 S. 1 Nr. 1 bis 3b StPO erstreckt. Unter Verweis auf § 11 Abs. 3 StGB sei das Medium, auf dem sich die Aufzeichnungen iSd Nr. 2 befinden, nach der Rechtsprechung des *BVerfG*[149] gleichgültig, weshalb hierunter auch elektronische Daten zu fassen seien.[150] Darüber hinaus ist ein ungeschriebenes Beweisverwertungsverbot für Fälle anerkannt, in denen der absolute Kernbereich privater Lebensgestaltung berührt wird.[151] Es scheint also, als seien zumindest solche Daten, die aufgrund eines Zeugnisverweigerungsrechts durch den Beschuldigten oder Dritten nicht preisgegeben werden müssen, ausreichend über das Instrumentarium der strafprozessualen Verwertungsverbote[152] geschützt.

Dem ist jedoch entgegenzuhalten, dass ungeschriebene Beweisverwertungsverbote nur subsidiär[153] gegenüber den ausdrücklich geregelten Beschlagnahmeverboten gelten. Auch erscheint angesichts der weitreichenden Bedeutung dieses ungeschriebenen Beschlagnahme- und einhergehenden Verwertungsverbots fraglich, warum sich hier

145 BGHSt 43, 303; *Gercke*, in: HK-StPO, § 94 Rn. 61; vgl. auch *Hauschild*, in: MüKoStPO, § 94 Rn. 36 m.w.N.
146 *Hauschild*, in: MüKoStPO, § 94 Rn. 54.
147 Bezüglich der Beweiseignung und -qualität von digitalen Daten *Momsen*, in: FS Beulke, S. 871 (879 ff.).
148 Zum justizförmigen Verfahren *Dölling*, in: FS Beulke, S. 679 (684).
149 *BVerfG*, NJW 2002, 1410.
150 *Engelhart*, in: NK-StPO, § 97 Rn. 7; *Greven*, in: KK-StPO, § 97 Rn. 13.
151 *Hauschild*, in: MüKo-StPO, StPO, § 94 Rn. 54.
152 Zu Folgen unzulässiger Beschlagnahme *Greven*, in: KK-StPO, § 97 Rn. 9.
153 *Gercke*, in: HK-StPO, § 94 Rn. 61.

keine vergleichbare Konstruktion zu § 100d StPO wiederfindet. Zudem ist nicht mit der Verwertung ein intensiver Grundrechtseingriff verbunden, sondern bereits mit dessen Erhebung. Entscheidend für ein Beschlagnahmeverbot nach § 97 StPO ist ferner, dass sich der dem Beschlagnahmeverbot unterliegende Gegenstand im Gewahrsam des Zeugnisverweigerungsberechtigten befinden muss. Schließlich handelt es sich bei der Zeugnisverweigerungsberechtigung um ein disponibles Recht, auf das grundsätzlich verzichtet werden kann.[154] Gibt der Betroffene die Daten freiwillig heraus, endet der Beschlagnahmeschutz des § 97 StPO.[155] Damit gilt der Schutz (höchstsensibler) Daten nach § 97 StPO nicht grenzenlos. Folglich leisten die Beschlagnahmeverbote nur einen begrenzten Beschuldigtenschutz.

d) Rechtsschutzmöglichkeiten

Daher ist weiter zu klären, inwieweit die bestehenden Rechtsbehelfe dem Betroffenen ausreichenden Schutz vor Rechtsgutsverletzungen bieten. Kennzeichnend ist, dass in der deutschen Strafprozessordnung jedenfalls kein präventiver Rechtsbehelf bei drohenden Maßnahmen der §§ 94 ff. StPO vorgesehen ist.[156] Es verbleiben folglich nur Rechtsbehelfe, die nachträglichen Rechtsschutz bieten.

aa) Revision

Zunächst wäre an eine Revision iSd §§ 333 ff. StPO zu denken. Da ein „Urteil [in der Regel jedoch] nicht auf der Rechtswidrigkeit der Beschlagnahme beruh[t]“[157], hat dieses Rechtsmittel nur einen begrenzten Anwendungsbereich.

bb) Beschwerde nach § 304 Abs. 1 StPO

Möchte der Betroffene den richterlichen Beschlagnahmebeschluss überprüfen lassen, ist vielmehr die Beschwerde nach § 304 Abs. 1 StPO statthaft. Hierbei kann der Betroffene seine Beschwerde auf Aufhebung des Beschlusses richten, um der Ingewahrsamnahme die Rechtsgrundlage zu entziehen und so seine beschlagnahmten Gegenstände zurückzuerhalten.[158] Damit kann wohl zumindest nachträglich dem Bedürfnis der Zurückgewinnung seiner Daten gedient werden.

Eine Beschwerde gemäß § 304 Abs. 1 StPO zielt jedoch nur auf die Überprüfung des „Ob“ des richterlichen Beschlagnahmebeschlusses ab, für die Überprüfung der Rechtswidrigkeit der Beschlagnahme in ihrer konkreten Art und Weise der Durchführung ist indes auf einen Antrag auf gerichtliche Entscheidung unter entsprechender Anwendung des § 98 Abs. 2 S. 2 StPO abzustellen.[159]

Zwar entfaltet die Beschwerde nach § 304 StPO grundsätzlich keine aufschiebende Wirkung, vgl. § 307 Abs. 1 StPO. Das Gericht hat jedoch von Amts wegen zu prüfen, ob die Aussetzung der Vollziehung geboten ist,[160] vgl. auch § 307 Abs. 2 StPO.

Umstritten ist in diesem Zusammenhang jedoch, ob dem Beschuldigten ein Anhörungsrecht eingeräumt werden

154 *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 97 Rn. 58.
155 *Gerhold*, in: BeckOK-StPO, 55. Ed. (1.4.2025), § 97 Rn. 59.
156 *Gercke*, in: HK-StPO, Vorb. §§ 94 ff. Rn. 21.
157 *Engelhart*, in: NK-StPO, § 97 Rn. 40.
158 *Park* (Fn. 106), § 3 Rn. 675.
159 *Park* (Fn. 106), § 3 Rn. 330, 333, 676.
160 *Zabeck*, in: KK-StPO, § 307 Rn. 5.

sollte, da § 308 Abs. 1 StPO jedenfalls nicht unmittelbar anwendbar sei.[161] Dies vermag jedoch mit Blick auf den Anspruch auf rechtliches Gehör iSd Art. 103 Abs. 1 GG[162] nicht zu überzeugen. Folglich wäre ein klarstellender Hinweis zur Klärung dieses Streits wünschenswert.

cc) Antrag nach § 98 Abs. 2 StPO

Möchte sich der Betroffene hingegen gegen eine Beschlagnahmeanordnung der Staatsanwaltschaft oder ihrer Ermittlungspersonen zu Wehr setzen, kommt grundsätzlich nur ein Antrag auf gerichtliche Entscheidung gemäß § 98 Abs. 2 S. 2 StPO (analog) in Betracht. Dies gilt für die Fälle, in denen die Beschlagnahme bereits beendet ist und nicht nur das „Ob" der Beschlagnahmeanordnung, sondern auch das „Wie" der konkreten Ausführung überprüft werden soll.[163]

Überraschend ist, dass in der Rechtsprechung inzwischen anerkannt ist, dass ein ähnliches Überprüfungsinteresse bei der Löschung sichergestellter elektronischer Daten bestehe[164] und insoweit auch sämtlichen Personen, deren personenbezogene Daten durch die Beschlagnahme berührt sind, eine Antragsbefugnis iSd § 98 Abs. 2 S. 2 StPO zugebilligt werde.[165] Diese Tendenz ist zu begrüßen.

Dennoch ist hier einzuwenden, dass ein solcher Antrag keine aufschiebende Wirkung entfaltet. Damit wäre im Falle einer rechtswidrigen Durchführung der Beschlagnahme eine Rechtverletzung sehenden Auges hinzunehmen. Dies erscheint vor dem Hintergrund, den Beschuldigten grundsätzlich als Subjekt des deutschen Strafverfahrens zu erachten, nur schwer hinnehmbar. Zu Recht plädiert *El-Ghazi*,[166] dass ein entsprechender Verweis im Rahmen des § 98 StPO auf die Vorschrift des § 307 Abs. 2 StPO notwendig sei.

e) Zwischenfazit: Unzureichender Schutz der Beschuldigtenrechte im Rahmen der Datenbeschlagnahme de lege lata

Im Ergebnis bietet das geltende Regelungskonzept mit einer Verbindung aus einer gebundenen Entscheidung hinsichtlich der Entschließung des „Ob" der Beschlagnahmemaßnahme und einer Ermessensentscheidung hinsichtlich des „Wie" der Beschlagnahmemaßnahme eine gewisse Flexibilität und ein auf den ersten Blick durchdachtes Rahmenkonzept. Gleichwohl gehen Unsicherheiten in der Judikatur über die konkrete Ausgestaltung der Beschlagnahme bei Daten(-sätzen) zulasten des Beschuldigten. Dies erscheint angesichts der Bandbreite der betroffenen Grundrechte nicht akzeptabel und bedarf eines Umdenkens. So erscheint vor allem bedenklich, dass es keine hinreichenden Kriterien für die Verhältnismäßigkeitsprüfung im Rahmen der Ermessensausübung durch die Ermittlungsbehörden gibt und dieses im Übrigen durch die Gerichte gerade nicht überprüfbar ist. Darüber hinaus findet das bestehende Regelungskonzept seine Grenzen, wenn es um die Aussetzung des Vollzugs der Beschlagnahmemaßnahme geht.

---

161 Ablehnend *Schmitt*, in: Schmitt/Köhler, StPO, § 307 Rn. 3; *Merz*, in: Radtke/Hohmann, StPO, 2. Aufl. (2025), § 307 Rn. 7; *Halbritter*, in: HK-GS, § 307 StPO Rn. 3; befürwortend *Rotsch/Wagner*, in: NK-StPO, § 307 Rn. 9; *Pfeiffer*, StPO, § 307 Rn. 2; *Zabeck*, in: KK-StPO, § 307 Rn. 6; *Fritsch*, in: SK-StPO, Bd. 6, 6. Aufl. (2021), § 307 Rn. 10.

162 *Rotsch/Wagner*, in: NK-StPO, § 307 Rn. 9; *Pfeiffer*, StPO, § 307 Rn. 2; *Zabeck*, in: KK-StPO, § 307 Rn. 6; *Fritsch*, in: SK-StPO, § 307 Rn. 10.

163 *Hartmann*, in: HK-GS, § 97 StPO Rn. 9 m.w.N.

164 Andeutend *BVerfG*, BeckRS 2006, 22591 Rn. 10.

165 *Hartmann*, in: HK-GS, § 97 StPO Rn. 9; unter dem Begriff des „mittelbar Betroffenen" vgl. *Hauschild*, in: MüKo-StPO, § 97 Rn. 39 m.w.N.

166 *El-Ghazi*, NJW-Beil 2024, 46 (49).

V. Anregungen für eine Regelung der Datenbeschlagnahme *de lege ferenda*

Im Folgenden möchte die Bearbeitung einige ergänzende Anregungen zur Verbesserung der Beschlagnahmeregelungen im Kontext der Digitalisierung und der Beschuldigtenrechte aufzeigen, ohne bestehende Regelungen zu ersetzen.

1. Klarstellung des Datenbegriffs bei § 94 StPO

Wie bereits eingangs aufgezeigt, bestanden in der Vergangenheit erhebliche Unklarheiten, wie mit beweisrelevanten Daten im Rahmen der Beschlagnahme zu verfahren ist. Zwar hat sich die Frage, ob Daten unter den Begriff des „Gegenstandes" iSd § 94 Abs. 1 StPO fallen, inzwischen in der Judikatur[167] – jedenfalls dahingehend, dass der Wortsinn des § 94 StPO eine entsprechende Subsumtion der Daten unter den Begriff des Gegenstandes zuließe – geklärt. Eine Klarstellung im Normtext erscheint gleichwohl sinnvoll.
Da den Normen der StPO ferner kein einheitlicher Datenbegriff zugrunde liegt, sondern vielfach Beschränkungen auf personenbezogene Daten oder Verkehrsdaten bestehen, sollte aus Klarstellungsgründen eine Legaldefinition des Datenbegriffes in einen neuen § 94 Abs. 3 StPO aufgenommen werden.
Exemplarisch wird folgender Absatz vorgeschlagen:

> „(3) [1]*Die Absätze 1 und 2 gelten auch für Daten.* [2]*Daten sind alle digital gespeicherte Informationen, die auf einem Datenträger mittels Nullen und Einsen als Zahlenfolgen dargestellt werden, deren Bedeutung aber ohne entsprechende Abstraktion nicht ohne Weiteres menschlich wahrnehmbar sind und die sich durch eine nichtkörperliche Form kennzeichnen."*

2. Klarstellungen im Rahmen der Rechtsschutzmöglichkeiten

Die aufgezeigten Rechtsbehelfe tragen nicht dem Bedürfnis Rechnung, dass bei so empfindlichen Grundrechten wie dem allgemeinen Persönlichkeitsrecht eine Verteidigungsmöglichkeit im Zeitpunkt der Vornahme besteht. So sollte zumindest bei § 98 Abs. 2 S. 2 StPO ein Verweis auf die Vorschrift des § 307 Abs. 2 StPO enthalten sein, der das Gericht von Amts wegen dazu verpflichtet zu überprüfen, ob die Vollziehung der angefochtenen Entscheidung nicht auszusetzen ist.
So bietet sich beispielsweise ein neuer § 98 Abs. 2 S. 3 StPO an:

> „(2) [1]Der Beamte, der einen Gegenstand ohne gerichtliche Anordnung beschlagnahmt hat, soll binnen drei Tagen die gerichtliche Bestätigung beantragen, wenn bei der Beschlagnahme weder der davon Betroffene noch ein erwachsener Angehöriger anwesend war oder wenn der Betroffene und im Falle seiner Abwesenheit ein erwachsener Angehöriger des Betroffenen gegen die Beschlagnahme ausdrücklichen Widerspruch erhoben hat. [2]Der Betroffene kann jederzeit die gerichtliche Entscheidung beantragen. [3][*Die Vorschrift des § 307 Abs. 2 StPO findet entsprechende Anwendung.*]"

[167] BVerfGE 113, 29 (50).

Zusätzlich bedarf es zwingend zur Wahrung des Grundsatzes des rechtlichen Gehörs gemäß Art. 103 Abs. 1 GG einer vorherigen Anhörung durch den Betroffenen, was nach jetziger Rechtslage umstritten ist. Angesichts dieser Rechtsunsicherheit und zur Stärkung der Beschuldigtenrechte im Zeitalter der Digitalisierung sollte hier im Rahmen des § 307 Abs. 2 StPO ein ergänzender Hinweis eingefügt werden, der ein solches Anhörungsrecht im Rahmen der Entscheidung des § 307 Abs. 2 StPO gesetzlich verankert.
Dieser könnte wie folgt formuliert werden:

> „(2) Jedoch kann das Gericht, der Vorsitzende oder der Richter, dessen Entscheidung angefochten wird, sowie auch das Beschwerdegericht [*nach vorheriger Anhörung des Beschuldigten*] anordnen, [*dass*] die Vollziehung der angefochtenen Entscheidung auszusetzen ist."

3. Inhaltliche Beschränkungen

a) Konkretisierung des Verhältnismäßigkeitsprinzips

Indes bietet sich gleichfalls eine nähere Regelung hinsichtlich der Durchführung des Beschlagnahmeverfahrens zur Vermeidung von Rechtsunsicherheiten im Umgang mit Daten an. Da § 98 StPO bereits das Verfahren der Beschlagnahme regelt, könnte hieran angesetzt werden und ein neuer Absatz 3 geschaffen werden, in welchem die bisherigen Grundsätze der Verhältnismäßigkeit aus der Rechtsprechung gesetzlich niedergelegt werden.[168] Auch könne hierzu erwogen werden, als Vorbild die gesetzliche Ausgestaltung des § 100d StPO heranzuziehen.[169] Hierzu schlägt die Bearbeitung folgenden Absatz vor:

> *„(3) [1]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach § 94 StPO Kenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. [2]Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. [3]Das Verfahren über die Sicherstellung der betroffenen Daten ist zu dokumentieren. [4]Es ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden und überschießende, für das Verfahren bedeutungslose Informationen und vertrauliche Daten Dritter bestmöglich ausgesondert werden."*

Zusätzlich erscheint im Rahmen des § 94 Abs. 1 StPO sodann ein entsprechender Verweis auf die Durchführungsregelungen der Beschlagnahme durch Hinzufügen eines weiteren Satzes sinnvoll, wie beispielsweise:

> „(1) [1]Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. [2]*Bei der Durchführung der Inverwahrungnahme und Sicherstellung gelten die Grundsätze des § 98 Abs. 3* (n.F.)."

[168] Unter Verortung bei § 94 StPO vgl. *Bildner*, in: Zöller (Hrsg.), Digitalisierung im Straf- und Strafprozessrecht, KriPoZ-JuP 2021, 4 (19 f.).
[169] So *Bildner*, a.a.O., S. 4 (20).

b) Gesetzliche Verankerung des zeitlichen Umfangs der Beschlagnahmemaßnahme und -auswertung

Bislang bestehen keine zeitlichen Grenzen für die Ermittlungsbeamten zur Auswertung des beschlagnahmten Gegenstandes. Hierbei ist zwar dahingehend anzuerkennen, dass eine Auswertung eines Datenbestandes von mehreren Gigabytes und ggf. bestehenden Verschlüsselungen ein ausreichender Raum zur Bearbeitung zugrunde gelegt werden muss,[170] doch bedeutet dies im Umkehrschluss auch für den Betroffenen eine gewisse Unsicherheit, wann dieser wieder seine Daten zurückerhält. Zwar kann durch den Ermittlungsrichter im Beschlagnahmebeschluss eine Frist bestimmt werden, die jedoch nicht zwingend ist.
Vielmehr bietet es sich an, bereits in der Normierung des § 94 Abs. 1 StPO eine gesetzliche Frist zu verankern,[171] wie beispielsweise:

> „(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind [*unter Berücksichtigung einer angemessenen Frist*] in Verwahrung zu nehmen oder in anderer Weise sicherzustellen."

VI. Fazit

1. Schlussbetrachtung

Das Strafverfahren dient dem Ziel einer „materiell richtigen, justizförmig zustande gekommenen und rechtsbeständigen Entscheidung."[172] Diesem Ziel ist auch im Rahmen der Datenbeschlagnahme hinreichend Rechnung zu tragen. Damit dient die Beschlagnahme – auch vor dem Hintergrund der vielfachen Erkenntnisquellen im digitalen Zeitalter – nicht nur einseitig der materiellen Wahrheitsfindung, sondern muss gewährleisten, dass „Eingriffe in Grundrechte des Beschuldigten […] nach Maßgabe des Verhältnismäßigkeitsgrundsatzes"[173] erfolgen.
Zu Beginn wurde die Frage aufgeworfen, ob die Beschuldigtenrechte im Zeitalter von *Big Data* im Rahmen der Datenbeschlagnahme *de lege lata* untergehen. Anders als vermutet, handelt es sich bei der Datenbeschlagnahme um kein modernes Problem des Zeitalters von *Big Data*. Dennoch birgt dieses Problem in der weiter zunehmenden Digitalisierung und Anhäufung von Datenmaterial Schwierigkeiten. Vielfach sind Fragen in der Praxis gesetzlich nicht klargestellt und führen im Ergebnis zu Rechtsunsicherheiten und vereinfachten Praktiken, wie etwa die vollständige Auswertung aller Daten. Viele Problemfelder wurden auch nach jahrelangem Streit in der Literatur schlicht durch die Judikatur und nicht durch die Gesetzgebung geklärt. Hierbei ist der Rechtsprechung zuletzt eine eher bedenkliche Tendenz zu entnehmen, die alles andere als die Stärkung der Beschuldigtenrechte befürchten lässt.
Angesichts dessen erscheint gesetzgeberischer Handlungsbedarf zwingend notwendig. Dies gilt sowohl vor dem Hintergrund, dass es einiger Klarstellungen im Zusammenhang der Datenbeschlagnahme bedarf, als auch, dass

[170] *Momsen*, in: FS Beulke, S. 871 (887).
[171] Eine gesetzliche Frist fordernd im Rahmen des § 110 StPO vgl. *Park*, in: FS Ignor, S. 757 (770 f.).
[172] *Dölling*, in: FS Beulke, S. 679 (687).
[173] Unter Verweis auf BVerfGE 19, 342 (348 f.); *Dölling*, in: FS Beulke, S. 679 (684).

ein hinreichendes Regelungssystem zum Vorgehen der Beschlagnahme aus Verhältnismäßigkeits- und Rechtssicherheitsgesichtspunkten erforderlich wird.

Zwar ist der Datenbeschlagnahme *de lege lata* zuzugeben, dass diese bereits einige Schutzvorkehrungen zugunsten des Betroffenen – wie beispielsweise eine Beschränkung durch das Legalitätsprinzip und der Verhältnismäßigkeit – vorsieht, doch es genügt an dieser Stelle nicht, dass sich konkrete Handhabung nur anhand einiger Rechtsprechungsleitlinien konkretisiert und sich gesetzgeberische Lücken im Ergebnis zulasten des Beschuldigten auswirken können. So weist insbesondere der Rechtsschutz des Betroffenen nach geltendem Recht mit Blick auf sensible Daten Lücken auf, die die Stellung des Betroffenen im Rahmen der Beschlagnahme erheblich schwächen.

Vor dieser äußersten Praxisrelevanz sollte für die künftige Behandlung der Datenbeschlagnahme *de lege ferenda* bedacht werden, dass sich die

„neuen" Erkenntnismöglichkeiten der Ermittlungsbehörden durch die Digitalisierung nicht nur einseitig fortentwickeln dürfen, sondern stets der Betroffene auf der anderen Seite als hinreichendes Subjekt gewürdigt und in den gesetzgeberischen Handlungsprozess einbezogen werden sollte.

2. Zusammenfassung in Thesen

1. Die Digitalisierung der Lebenswirklichkeit führt dazu, dass sich digitale Daten anhäufen, die auch für den Strafprozess zunehmend an Bedeutung gewinnen. In der Vergangenheit war lange umstritten, ob unter den Begriff des „Gegenstandes" i.S.d. § 94 StPO auch unkörperliche Datenbestände fallen können. In der Rechtsprechung scheint dieser Streit inzwischen entschieden. Gesetzlich niedergeschlagen hat sich dies jedoch nicht.
2. Die Ermittlungsbehörden verfügen nach der derzeitigen Gesetzeslage über einen weiten Handlungsspielraum hinsichtlich des „Wie" der Beschlagnahmemaßnahme. Die konkreten Anforderungen des Verhältnismäßigkeitsgrundsatz, der auch bei der Datenbeschlagnahme zu beachten ist, ergeben sich nur aus der Judikatur, was zwar eine notwendige Einzelfallflexibilität vermitteln mag, aber auch eine erhebliche Missbrauchsgefahr birgt. So führt die Nichtverankerung der Dauer der Datenbeschlagnahme in der Praxis regelmäßig dazu, dass Datenbestände über Monate oder Jahre hinweg in den Händen der Ermittlungsbehörden verbleiben.
3. Die Datenbeschlagnahme berührt diverse Grundrechte, allen voran das Recht auf informationelle Selbstbestimmung, in besonders schwerwiegendem Maße. Angesichts des Datenspektrums und der weitreichenden Ermittlungsmöglichkeiten bietet diese ein Einfallstor für die Erstellung umfassender Persönlichkeitsprofile. Die Datenbeschlagnahme weist damit im Vergleich zur „normalen" Beschlagnahme einen qualitativen Unterschied auf.
4. Zugleich sind die Beschuldigten nicht hinreichend über die bestehenden Rechtsschutzmöglichkeiten geschützt. Eine Verhinderung des Zugriffs im Zeitpunkt der Beschlagnahme kann nicht herbeigeführt werden, sodass im Zweifel sehenden Auges die Verletzung von Grundrechten hinzunehmen ist.
5. Die Datenbeschlagnahme *de lege lata* stellt zwar ein durchdachtes Grundgerüst dar, das jedoch mit Blick auf die fortschreitende Digitalisierung Anpassungsbedarf hat. Hierbei darf nicht verkannt werden, dass

sich die Möglichkeiten der Digitalisierung strafprozessual nicht nur einseitig auswirken dürfen. Die Bearbeitung zeigt daher entsprechende Ansatzpunkte für einen möglichen Reformbedarf zum verbesserten Schutz der Beschuldigtenrechte auf.