TWP STRAF RECHTS KANZLEI
BÜROGEMEINSCHAFT

TWP STRAFRECHTSKANZLEI
Thiel | Weller | Pinar | Kistner | Scherbarth | Großneumarkt 50 | 20459 Hamburg

per beA

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

ANDREAS THIEL
Rechtsanwalt | Strafverteidiger

ARNE WELLER
Rechtsanwalt | Fachanwalt für Strafrecht

GÜL PINAR
Rechtsanwältin | Fachanwältin für Strafrecht
Zertifizierte Beraterin Steuerstrafrecht (DAA)

NOAH KISTNER
Rechtsanwalt | Strafverteidiger

SANDRA SCHERBARTH
Rechtsanwältin | Strafverteidigerin

Großneumarkt 50
20459 Hamburg

kanzlei@twp-strafrecht.de
www.twp-strafrecht.de

Telefon 040 432744-34
Fax 040 432744-35

Sekretariat Thiel direkt
040 432744-341

Datum: 29.07.2025 Unser Zeichen: [redacted]

[redacted]

Verfassungsbeschwerde

des [redacted]

- Beschwerdeführer -

Bevollmächtigte: Rechtsanwältin Gül Pinar, Großneumarkt 50, 20459 Hamburg

wegen Beschlagnahme und Datenzugriff auf Mobiltelefon.

Namens und in Vollmacht des Beschwerdeführers erhebe ich

Verfassungsbeschwerde

gegen

den Beschluss des Landgerichts Bamberg vom 27. Juni 2025 - [redacted] -.

Die vorbezeichnete Entscheidung verletzt den Beschwerdeführer in seinem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, jedenfalls in Form des Grundrechts auf informationelle Selbstbestimmung, in seinem Grundrecht auf Eigentumsfreiheit (Art. 14 Abs. 1 Satz 1 GG), in seinem Grundrecht auf Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG), in seinem Grundrecht auf Meinungsfreiheit (Art. 5 Abs. 1 Satz 1 GG), jedenfalls in seinem Grundrecht auf allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) sowie in seinem Recht auf rechtliches Gehör (Art. 103 Abs. 1 GG) und seinem Recht auf den*die gesetzliche*n Richter*in (Art. 101 Abs. 1 Satz 2 GG).

Es wird beantragt,

> den Beschluss des Landgerichts Bamberg vom 27. Juni 2025 - ... - aufzuheben und die Sache zur erneuten Entscheidung an das Landgericht Bamberg zurückzuverweisen.

Es wird gebeten, die Verfassungsbeschwerde im Hinblick auf die laufende Anhörungsrüge und den Antrag auf gerichtliche Entscheidung zunächst im Allgemeinen Register zu erfassen. Die Beschlüsse werden, sobald diese vorliegen, dem Bundesverfassungsgericht übersandt und sodann im Falle der Erfolglosigkeit um Umschreibung zur BvR-Sache gebeten.

Der Beschwerdeführer hat mir für das Verfahren vor dem Bundesverfassungsgericht Vollmacht gem. § 22 BVerfGG erteilt. Die Vollmacht liegt als **Anlage 1** bei. Der Beschluss des LG Bamberg vom 27. Juni 2025 - ... - (**Anlage 2**) ist mir als seine Verteidigerin am 30. Juni 2025 zugegangen. Dem Beschwerdeführer wurde der Beschluss nicht zugestellt.

Gliederung

A. Vorbemerkung

In dieser Verfassungsbeschwerde geht es um den umfassenden Datenzugang auf ein beschlagnahmtes Mobiltelefon nach §§ 94 ff. StPO. Die Strafverfolgungsbehörden haben das Mobiltelefon des Beschwerdeführers entsperrt und Zugriff auf den gesamten Datenbestand erlangt. Anschließend haben sie alle Daten zum Zwecke einer inhaltlichen Auswertung gesichert.

Der Beschwerdeführer rügt eine Verletzung seines allgemeinen Persönlichkeitsrechts in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, hilfsweise seines Rechts auf informationelle Selbstbestimmung. Außerdem rügt er die Verletzung seines Grundrechts auf Eigentumsfreiheit aus Art. 14 Abs. 1 Satz 1 GG, auf Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG, auf Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG, auf allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG, seines Rechts auf rechtliches Gehör aus Art. 103 Abs. 1 GG und seines Rechts auf den*die gesetzliche*n Richter*in aus Art. 101 Abs. 1 Satz 2 GG.

Handybeschlagnahme als Standardmaßnahme der Strafverfolgungsbehörden

Die Verfassungsbeschwerde betrifft keinen Einzelfall. Täglich beschlagnahmen Strafverfolgungsbehörden Mobiltelefone und werten sie anschließend aus. Die konkrete Anzahl solcher Maßnahmen wird statistisch regelmäßig nicht erfasst. Recherchen zufolge wurden jedoch allein in Bayern innerhalb eines Zeitraums von fünf Jahren 175.000 Mobiltelefone bei knapp 80.000 Straftaten sichergestellt,

> vgl. *Pitz*, Beschlagnahmte Smartphones, Ein Grundrechtseingriff unbekannten Ausmaßes vom 30. Oktober 2023, netzpolitik.org, abrufbar unter: https://netzpolitik.org/2023/beschlagnahmte-smartphones-ein-grundrechtseingriff-unbekannten-ausmasses/ (Letzter Abruf: 18 Juli 2025).

Häufig geschieht dies bereits bei geringfügigen Straftaten oder Ordnungswidrigkeiten. So reichte etwa dem Amtsgericht Pirna bereits der Verdacht der Begehung einer

Verkehrsordnungswidrigkeit nach §§ 49 Abs. 1 Nr. 22, 23 Abs. 1a StVO aus, um eine Beschlagnahme des Mobiltelefons des Beschuldigten anzuordnen,

> AG Pirna, Beschluss vom 05. Februar 2020 - 23 Gs 66/20 -, BeckRS 2020, 5134.

Die Strafverfolgungsbehörden bedienen sich dafür – wie auch im vorliegenden Fall – regelmäßig forensischer Extraktions- und Auswertungssoftware des Herstellers Cellebrite und können sich damit einen Vollzugriff auf den gesamten Datenbestand verschaffen und auch gelöschte Daten rekonstruieren,

> *Meister*, Mit diesen sieben Programmen liest die Polizei Smartphone-Daten aus vom 15. August 2018, netzpolitik.org, abrufbar unter: https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/; zum Funktionsumfang der Software vgl. Produktinformation zu Cellebrite Universal Forensic Extraction Device, abrufbar unter https://cellebrite.com/en/ufed/ (Letzter Abruf der Online-Quellen: 22. Juli 2025)

Aufgrund des aufwendigen technischen Vorgangs der forensischen Entsperrung und der anschließenden Durchsicht und inhaltlichen Auswertung der großen Datenmengen, verbleibt das Gerät in der Regel Monate oder Jahre bei den Strafverfolgungsbehörden,

> für die Dauer der Datendurchsicht in der Praxis nach § 110 Abs. 1, 3 StPO vgl. *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 106 m.w.N.

Angesichts des langen Eigentumsentzugs sowie der zentralen Bedeutung von Mobiltelefonen für die private Lebensgestaltung sowie geschäftliche Tätigkeiten haben solche Ermittlungsmaßnahmen erhebliche Auswirkungen auf das Leben der Betroffenen. Hinzu kommt, dass Mobiltelefone eine enorme Menge und Vielfalt an höchst sensiblen Daten aus fast allen Lebensbereichen enthalten, die in der berechtigten Erwartung auf Vertraulichkeit gespeichert sind. Der Zugriff auf diese Daten birgt ein hohes Missbrauchspotential sowie das Risiko der Erstellung umfassender Kommunikations-, Verhaltens- und Persönlichkeitsprofile – Risiken, die sich beim Beschwerdeführer verwirklicht haben:

Obwohl die Ermittlungsmaßnahme mangels Strafantrags nach Ablauf des … Dezember 2023 unverzüglich hätte eingestellt und das Mobiltelefon zurückgegeben werden müssen, haben die Strafverfolgungsbehörden den Datenzugriff fortgesetzt. Dabei haben sie eine Vielzahl an Daten durchsucht, ausgewertet und gespeichert, die keinen Bezug zum Strafvorwurf aufwiesen. Aus diesen Daten haben die Strafverfolgungsbehörden ein politisches Profil des Betroffenen erstellt, in dem u.a. seine Zugehörigkeiten zu politischen Organisationen sowie seine politischen Einstellungen und Aktivitäten ausführlich dokumentiert wurden. Auch eine Vielzahl an persönlichen Fotos und Kommunikationsinhalten – unter anderem mit journalistischen Quellen – wurden ausgewertet und auf eigenen Datenträgern der Polizei gespeichert. Bis zum heutigen Zeitpunkt sind diese höchstsensiblen und besonders geschützten Daten (vgl. Art. 10 JI-Richtlinie) immer noch im Besitz der Polizei.

Defizitärer Grundrechtsschutz durch die geltende Rechtslage

Die Strafverfolgungsbehörden und Fachgerichte stützen sich für einen solchen Datenzugriff und die anschließende Auswertung auf eine Annexkompetenz der Beschlagnahmevorschriften aus §§ 94 ff. StPO. Diese Vorschriften regeln einen Datenzugriff sowie die Datenauswertung in ihrem Wortlaut jedoch überhaupt nicht. Die Vorschriften enthalten weder Regelungen zum Umfang, zu den Grenzen noch zur Art der technischen Durchführung eines Datenzugriffs. Darüber hinaus fehlen ausreichende Dokumentationspflichten, die den Betroffenen ermöglichen, den konkreten Vorgang in transparenter Weise nachzuvollziehen und gerichtlich überprüfen zu lassen.

Auch der in § 98 Abs. 1 StPO vorgesehene Gerichtsvorbehalt bezieht sich ausschließlich auf die Anordnung der Beschlagnahme an sich. Es ist weder gesetzlich vorgesehen, dass Gerichte in ihren Anordnungsbeschlüssen über die Zulässigkeit und Modalitäten eines nachfolgenden Datenzugriffs entscheiden, noch erfolgt dies in der gerichtlichen Praxis.

Das Landgericht Bamberg hat auf die am 19. Juni 2025 eingereichte Beschwerde hin keine eigenständige Prüfung der Verfassungs- und Unionsrechtswidrigkeit vorgenommen und den diesbezüglichen umfassenden Vortrag des Beschwerdeführers vollständig unberücksichtigt gelassen,

siehe LG Bamberg, Beschluss vom 27. Juni 2025 - ... -, S. 4 (**Anlage 2**).

Keinesfalls ausreichend ist dessen bloße Feststellung der Vereinbarkeit mit Verfassungsrecht und Unionsrecht in einem einzigen Satz unter Verweis auf die jüngste, verfassungsrechtlich höchst problematische Entscheidung des Bundesgerichtshofs vom 13. März 2025 - 2 StR 232/24 -.

Dieser Beschluss des Bundesgerichtshofs hat für starke Verunsicherung gesorgt und ist sowohl in der Öffentlichkeit als auch in der Rechtswissenschaft auf breite und vehemente Kritik gestoßen,

> *Raillon*, Die Polizei darf den Finger heben vom 2. Juni 2025, Tagesschau, abrufbar unter: https://www.tagesschau.de/inland/gesellschaft/smartphone-sperre-fingerabdruck-100.html; *Breithut/Hipp*, Darf die Polizei mich zwingen, mein Handy per Fingerabdruck zu entsperren vom 24. Mai 2025, Spiegel Online, abrufbar unter: https://www.spiegel.de/netzwelt/gadgets/bgh-urteil-darf-die-polizei-mich-zwingen-mein-handy-per-fingerabdruck-zu-entsperren-a-13a456a0-cf7a-4c11-a51d-729654108f7f; *Ferner*, Zwangsweise Entsperrung von Smartphones: Die Büchse der Pandora ist offen vom 23. Mai 2025, abrufbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-2str232-24-zwangsweise-entsperrung-smartphone-fingerabdruck; *Mansouri/Rückert*, Touch me if you can – Die Zulässigkeit der zwangsweisen Entsperrung eines Mobiltelefons mittels Fingerabrdrucks, JR 2025, 2064 m.w.N., abrufbar unter: https://doi.org/10.1515/juru-2025-2064; Jahn, † Strafprozessrecht: Zwangsweise Entsperrung von Smartphones, JuS 2025, 791 (Letzter Abruf der Online-Quellen: 17. Juli 2025).

In dieser Entscheidung hat der Bundesgerichtshof die Rechtmäßigkeit einer zwangsweisen Entsperrung eines Mobiltelefons durch Fingerabdruck bestätigt und die Vereinbarkeit eines auf die §§ 94 ff. StPO gestützten Datenzugriffs mit Verfassungs- und Unionsrecht bejaht. Dabei hat das Gericht aber die besonders hohe Eingriffsintensität in die Grundrechte der Betroffenen und die damit einhergehenden strengen verfassungs- und unionsrechtlichen Vorgaben für eine hinreichend bestimmte und verhältnismäßige Ermächtigungsgrundlage eklatant verkannt.

In seinem Beschluss hat sich der Bundesgerichtshof für die Begründung der Verfassungsmäßigkeit auf eine Entscheidung des angerufenen Gerichts berufen, die fast 20 Jahre zurückliegt (BVerfG, Beschluss vom 12. April 2006 - 2 BvR 1027/02 -, BVerfGE 113, 29, 50 ff.). Angesichts des technischen Fortschritts, der damit einhergehenden Veränderung des Nutzungsverhaltens sowie des Umfangs, der Vielfalt sowie der Vernetzung der auf modernen Smartphones gespeicherten Daten – die zu der damaligen Zeit noch nicht berücksichtigt werden konnten – ist davon auszugehen, dass die damals aufgestellten verfassungsrechtlichen Maßstäbe nicht auf die heutige Situation übertragbar sind.

Auch lässt der Bundesgerichtshof die unionsrechtlichen Anforderungen an eine gesetzliche Ermächtigungsgrundlage für den Datenzugriff auf beschlagnahmte Mobiltelefone unzureichend berücksichtigt. Die durch den Europäischen Gerichtshof in seinem Urteil vom 4. Oktober 2024 - C 548/21 - aufgestellten Maßstäbe hat der Bundesgerichtshof lücken- und fehlerhaft ausgelegt.

In dieser Entscheidung hat der Europäische Gerichtshof für eine unionsrechtskonforme gesetzliche Grundlage die Anforderung aufgestellt, dass sie zumindest die Art oder Kategorien der Straftaten festlegen müsse, bei denen ein Datenzugriff ermöglicht werden könne. Dies sei für die Wahrung der Verhältnismäßigkeit und der hinreichenden Bestimmtheit einer Ermächtigungsgrundlage unabdingbar,

> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 99 ff.

Darüber hinaus brauche es einen Gerichtsvorbehalt, der spezifisch die Zulässigkeit und Grenzen des Datenzugriffs regelt – dieser fehlt auch in den derzeit bestehenden deutschen Beschlagnahmevorschriften.

Die jüngste Entscheidung des Bundesgerichtshofs verstärkt die Angst vor staatlicher Ausforschung und entfaltet eine große Abschreckungswirkung – insbesondere im Kontext von zivilgesellschaftlichem und politischem Engagement sowie von journalistischer Arbeit.

Notwendigkeit eines ausdifferenzierten Regelungskonzepts

In der strafrechtlichen Literatur gibt es zahlreiche Stimmen, die die geltenden Beschlagnahmevorschriften in Bezug auf die Ermächtigung zu einem umfassenden Datenzugang und anschließender Datenauswertung als verfassungsrechtlich unzureichend ansehen. Für den 74. Deutschen Juristentag 2024 wurde ein umfassendes Gutachten zur verfassungsrechtlich defizitären Ermächtigungsgrundlage für den Datenzugriff und die Auswertung beschlagnahmter komplexer IT-Geräte angefertigt und als zentrales Thema im Strafrechtsreferat zur Diskussion gestellt,

> vgl. Deutscher Juristentag e.V., 74. Deutscher Juristentag 2024, Strafrecht, abrufbar unter: https://djt.de/74-djt/fachprogramm/strafrecht/ (Letzter Abruf: 18. Juli 2025); *El-Ghazi*, Beschlagnahme und Auswertung von Handys, Laptops & Co. – Sind beim offenen Zugriff auf Datenträger die Persönlichkeitsrechte angemessen geschützt?, Gutachten C zum 74. Deutschen Juristentag, 2024.

Auch ein Blick auf unser Nachbarland Österreich verdeutlicht die Tragweite des Problems. Es wird deutlich, dass veraltete strafprozessuale Normen zwingend an die technologische Entwicklung und die damit einhergehenden Gefahren angepasst werden müssen. Der österreichische Verfassungsgerichtshof hat am 14. Dezember 2023 entschieden, dass die damals geltenden Beschlagnahmevorschriften hinsichtlich des Zugriffs und der Auswertung von Datenträgern nicht mehr zeitgemäß sind und den verfassungsrechtlichen Anforderungen nicht genügen,

> VfGH Österreich, Erkenntnis vom 14. Dezember 2023 - G 352/2021-46-, BeckRS 2023, 36793.

Daraufhin hat der Nationalrat am 27. Dezember 2024 umfassende Neuregelungen in Bezug auf die Beschlagnahme von Datenträgern und der anschließenden Datenauswertung verabschiedet, die – im Gegensatz zu den deutschen Vorschriften in §§ 94 ff. StPO – deren Anlass, Zweck und Umfang sowie notwendige Verfahrensvorschriften hinreichend klar und detailliert festlegen,

> BGBl. Nr. 631/1975, zuletzt geändert durch BGBl. I Nr. 157/2024, abrufbar unter: https://ris.bka.gv.at/eli/bgbl/1975/631/P115f/NOR40267211?Sort=1%7cDesc&Abfrage=Bundesnormen&FassungVom=05.02.2025 (Letzter Abruf: 18. Juli 2025).

Das Bedürfnis, auch Mobiltelefone zur effektiven Verfolgung von Straftaten entsperren und auswerten zu können, darf zwar nicht außer Acht gelassen werden. Ein solch schwerwiegender Eingriff – wie auch im vorliegenden Fall – kann und darf aber nur auf Grundlage eines ausdifferenzierten Regelungskonzepts erfolgen, das der spezifischen Gefahrenlage und der besonders hohen Eingriffsintensität ausreichend Rechnung trägt und die Zulässigkeit, den Anlass und die Grenzen des Datenzugriffs klar und rechtssicher normiert.

B. Sachverhalt

I. Einfachrechtlicher Hintergrund

Die gesetzlichen Grundlagen für Ermittlungsmaßnahmen nach den §§ 94 ff. StPO wurden bereits mit dem Einführungsgesetz zur Strafprozessordnung im Jahre 1877 verabschiedet und sind seit ihrem Inkrafttreten am 1. Oktober 1879 ihrem ermächtigenden Wortlaut nach nahezu unverändert Teil unserer heutigen Strafprozessordnung,

> siehe Wortlaut des § 94 StPO aus dem Jahr 1877, abrufbar unter: https://lexetius.com/StPO/94/sicherstellung-und-beschlagnahme-von-gegenstanden-zu-beweiszwecken (Letzter Abruf: 23. Juli 2025).

1. Beschlagnahme nach § 94 StPO

Nach § 94 Abs. 1 StPO können Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, in Verwahrung genommen oder in anderer Weise sichergestellt werden. Sofern sich die Gegenstände im Gewahrsam einer Person befinden und sie nicht freiwillig herausgegeben werden, können sie nach § 94 Abs. 2 StPO beschlagnahmt werden.

Seit jeher und bis heute ermächtigt § 94 StPO seinem Wortlaut nach lediglich zur Beschlagnahme oder Sicherstellung von „Gegenständen“ zu Beweiszwecken. Der Gesetzeswortlaut wurde dahingehend bis heute jedoch nicht geändert; die Beschlagnahme von Daten ist nicht ausdrücklich vom Tatbestand der Norm gedeckt. In der Rechtspraxis wird der Datenträger, auf

dem sich die relevanten Dateien befinden, als tauglicher Gegenstand im Sinne der strafprozessualen Eingriffsermächtigungen nach § 94 StPO behandelt,

> BVerfGE 113, 29 (32).

Die bisherige Rechtspraxis legt den Anwendungsbereich der Norm weit aus und erstreckt ihn dabei auch auf die in Datenträgern gespeicherten Informationen. Aufgrund ihrer Bedeutung im alltäglichen Leben und damit auch im Rahmen etwaiger Ermittlungsmaßnahmen nimmt die bisherige Rechtsprechung das Bedürfnis an, diese in den Anwendungsbereich des § 94 StPO (und im Rahmen einer Durchsuchung des § 110 StPO, dazu sogleich unter **3.**) zu ziehen, der eine solche Anwendung von seinem Wortsinn her ebenfalls auch gestatte,

> BVerfGE 113, 29 (50 f.); BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 44 m.w.N.; dazu eingehend: *Bäumerich*, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung, NJW 2017, 2718 (2719 f.).

Für die Durchführung einer Beschlagnahme ist in jedem Fall das Vorliegen eines Anfangsverdachts hinsichtlich einer Straftat gem. § 152 Abs. 2 StPO erforderlich. Dieser Anfangsverdacht muss eine Tatsachengrundlage haben, aus der sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt, ohne dass es auf eine erhöhte Wahrscheinlichkeit ankommt; nur eine bloße Vermutung würde nicht ausreichen,

> BVerfG, Beschluss vom 23. Januar 2004 - 2 BvR 766/03 -, NStZ-RR 2004, 143.

Gem. § 46 Abs. 1 OWiG kommen die §§ 94 ff. StPO auch im Bußgeldverfahren zur Anwendung. Trotz der niedrigschwelligen Eingriffsvoraussetzungen der OWiG-Bestimmungen sieht das Gesetz für hiernach ergriffene Ermittlungsmaßnahmen – neben den gem. § 46 Abs. 3 OWiG unzulässigen Handlungsformen – keine weiteren ausdrücklichen Einschränkungen vor,

> *Hauschild*, in: Münchener Kommentar zur StPO, 2. Auflage 2023, § 94 Rn. 6; *Bücherl*, in: BeckOK OWiG, 46. Edition, Stand: 1. April 2025, § 46 Rn. 4 f.

Der Tatbestand des § 94 Abs. 1, Abs. 2 StPO erfordert weiterhin, dass die sicherzustellenden oder zu beschlagnehmenden Gegenstände für die Untersuchung von Beweisbedeutung sein können, wobei eine potentielle Beweisbedeutung erforderlich und ausreichend ist. Dies erfordert eine mögliche Relevanz des Gegenstandes für den Fortgang des weiteren Verfahrens,

> BVerfG, Beschluss vom 13. Dezember 1994 - 2 BvR 894/94 -, wistra 1995, 139 (140); BVerfGE 113, 29; BGH, Urteil vom 24. November 1995 - StB 84/95 -, NJW 1996, 532.

Sofern der Datenträger durch eine PIN, ein Passwort oder ein Entsperrmuster geschützt ist, kann der Beschuldigte wegen des gem. § 136a Abs. 1 StPO bzw. der Selbstbelastungsfreiheit geltenden Verbots des zwangsweisen Hinwirkens auf die Preisgabe der Daten nicht zur Freigabe des Geräts gezwungen werden,

> *Bäumerich*, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung, NJW 2017, 2718 (2720 f. m.w.N.).

In diesen Fällen kann nur der Datenträger als Ganzes beschlagnahmt werden, damit es durch die Strafverfolgungsbehörden mithilfe forensischer Software entsperrt werden kann, um anschließend die Daten auszulesen und inhaltlich auszuwerten. Für den Datenzugriff und die Datenauswertung stützen sich die Fachgerichte sowie frühere Entscheidungen des angerufenen Gerichts ebenfalls auf die §§ 94 ff. StPO,

> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 46 m.w.N.; vgl. BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917; BVerfG, Urteil vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, 976.

Soweit ein Datenträger durch biometrische Merkmale vor dem Zugriff Dritter geschützt ist, wird die zwangsweisen Durchsetzung der zur Entsperrung erforderlichen Mitwirkungshandlung der beschuldigten Person – wie etwa der unter Zwang verwendete Daumenabdruck – auf § 81b Abs. 1 StPO gestützt. Der Bundesgerichtshof hat die Rechtmäßigkeit einer solchen auf § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO gestützten Maßnahme in seinem Beschluss vom 13. März 2025 (Az. 2 StR 232/24) erstmalig höchstgerichtlich bestätigt,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 28 ff.

Diese Entscheidung sieht sich erheblicher Kritik aus der Rechtswissenschaft ausgesetzt (siehe dazu **C.II.c.cc.(1)(dd)**).

Wie alle strafprozessualen Ermittlungsmaßnahmen unterliegt die Beschlagnahme und der anschließende Datenzugriff der Beschränkung auf den Ermittlungszweck. Dies ergibt sich der bundesverfassungsgerichtlichen Rechtsprechung nach aus dem Normzusammenhang – insbesondere aus den § 152 Abs. 2, § 155 Abs. 1, §§ 160, 170, 244 Abs. 2, § 264 StPO – in welchen die §§ 94 ff. StPO eingebettet seien,

BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1920).

Diese Rechtsprechung hat der Bundesgerichtshof übernommen. Mit dieser strengen Begrenzung sämtlicher Ermittlungen und damit auch der Datenerhebung auf den Zweck der Aufklärung der begangenen Tat begrenze die StPO die Eingriffe in das Recht an den eigenen Daten grundsätzlich auf diejenigen, die für die Strafverfolgung im konkreten Anlassfall von Bedeutung sind. Auf die Ermittlung anderer Lebenssachverhalte und Verhältnisse dürften sich diese konkreten Eingriffsermächtigungen nicht erstrecken,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 47.

Darüber hinaus ist wie bei jeder Ermittlungsmaßnahme der Grundsatz der Verhältnismäßigkeit im Einzelfall zu beachten.

2. Gerichtsvorbehalt nach § 98 StPO

Beschlagnahmen nach § 94 Abs. 2 StPO bedürfen gem. § 98 Abs. 1 StPO der Anordnung durch das Gericht, wobei bei Gefahr im Verzug auch die Anordnung durch die Staatsanwaltschaft oder ihrer Ermittlungspersonen möglich ist. Die Beschlagnahmeanordnung muss dabei den Tatvorwurf, insbesondere das Delikt, den Tatort sowie die Tatzeit so weit wie möglich konkretisieren und dabei notwendigerweise Angaben zum Tatverdacht, zur potentiellen Beweisfunktion und

zum Umfang der Beschlagnahme, d.h. die konkrete Benennung der beschlagzunehmenden Gegenstände, enthalten,

Hauschild, in: Münchener Kommentar zur StPO, 2. Auflage 2023, § 94 Rn. 46 m.w.N.

Damit werden insbesondere Anforderungen an die Dokumentation des Beschlagnahmegrundes gestellt. So ist etwa der Beweisgegenstand so genau zu bezeichnen, dass keine Zweifel über den Umfang der Maßnahme bestehen, wobei Mängel in dieser Beschreibung durch Bezeichnung der gesuchten Beweismittel, diese Rückschlüsse auf den Vorwurf zulassen, ausgeglichen werden können,

Hauschild, in: Münchener Kommentar zur StPO, 2. Auflage 2023, § 98 Rn. 18 ff.

Auch sind Ausführungen zur Verhältnismäßigkeit für die Anordnung der Beschlagnahme geboten, insbesondere sind dabei die Schwere der Tat und die Stärke des Tatverdachts zu berücksichtigen,

Gerhold, in: BeckOK StPO, 56. Edition, Stand: 1. April 2025, § 98 Rn. 10.

Spezifische Vorgaben für die Modalitäten eines Datenzugriffs auf einen beschlagnahmten Datenträger und der anschließenden Auswertung sowie diesbezügliche Verhältnismäßigkeitserwägungen sind weder gesetzlich vorgesehen noch wurden solche bisher durch Gerichte etabliert.

3. Besonderheiten bei Durchsuchungen

Wenn der Beschlagnahme eine Durchsuchung nach § 102 StPO vorgelagert ist, ermöglicht § 110 Abs. 1, Abs. 3 StPO den Strafverfolgungsbehörden die Durchsicht der auf einem Datenträger gespeicherten Daten und die vorläufige Sicherung von Daten, die für die Untersuchung von Bedeutung sein können. Im Rahmen der Durchsicht können der Datenträger durchsucht und die beweisrelevanten Daten aussortiert werden, bevor diese durch eine Beschlagnahme einem dauerhaften und damit vertiefenden Eingriff zugeführt werden,

BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1921).

Damit bezweckt die Durchsicht die Vermeidung einer übermäßigen und auf Dauer angelegten Datenerhebung und damit eine Verminderung der Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung,

> BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1922).

Eine Durchsicht nach § 110 Abs. 3 StPO ist jedoch nur möglich, wenn zuvor eine Durchsuchung nach § 105 Abs. 1 StPO gerichtlich angeordnet wurde oder die Staatsanwaltschaft eine Durchsuchung aufgrund Gefahr in Verzug selbständig durchführt; die Durchsicht ist dem Stadium der Durchsuchung zugeordnet,

> BVerfG, Beschluss vom 30. November 2021 - 2 BvR 2038/18 -, DStRE 2022, 1020 (1022 Rn. 44 m.w.N.).

Die Möglichkeit einer Datendurchsicht nach § 110 Abs. 3 StPO scheidet in solchen Fällen aus, in denen keine Durchsuchung angeordnet bzw. durchgeführt wurde, sondern der Datenträger unmittelbar beschlagnahmt wurde.

4. Lösch- und Dokumentationspflichten

Gem. § 483 Abs. 1 Satz 1 StPO dürfen personenbezogene Dateien in Dateisystemen verarbeitet werden, soweit dies für Zwecke des Strafverfahrens erforderlich ist. Diese Vorschrift und die dazugehörige Löschpflicht nach § 489 Abs. 1 StPO sind aber nicht auf beschlagnahmte Daten anwendbar, die als Beweismittel erhoben und sichergestellt wurden,

> OLG Rostock, Beschluss vom 29. Juni 2017 - 20 VAs 5/16 -, BeckRS 2017, 119395 Rn. 12; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 10 m.w.N.

Sobald die Erforderlichkeit entfällt – insbesondere bei einem rechtskräftigen Freispruch, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder einer nicht nur vorläufigen Einstellung – greifen Löschpflichten nach § 489 Abs. 1 StPO für auf sonstige Weise gespeicherte Daten und nach § 500 StPO i.V.m. §§ 75 Abs. 2, 58 Abs. 2 BDSG. Diese gelten aber nur

beschränkt und sehen zahlreiche Ausnahmen vor, vgl. u.a. § 489 Abs. 1 Nr. 1 i.V.m. §§ 484, 485 StPO und § 75 Abs. 3 BDSG i.V.m. § 58 Abs. 3 BDSG.

Eine Protokollierungspflicht sieht § 500 StPO i.V.m. § 76 BDSG vor, beschränkt sich dabei aber auf wenige, sehr allgemeine Umstände der Datenverarbeitung, vgl. § 76 Abs. 1 BDSG.

II. Individueller Sachverhalt

1. Person des Beschwerdeführers

Der Beschwerdeführer engagiert sich als Mitglied bei der Gewerkschaft …. Im Rahmen dieser Tätigkeit veröffentlicht der Beschwerdeführer regelmäßig journalistische Beiträge, in denen er von Veranstaltungen und Demonstrationen berichtet. Aufgenommen hat er diese Tätigkeit ...

So berichtete der Beschwerdeführer beispielsweise von …,

vgl. ….

Die Beiträge des Beschwerdeführers erscheinen jeweils sowohl in der Print- als auch in der digitalen Ausgabe ….

2. Geschehnisse und polizeiliche Maßnahmen am … September 2023

Am … September 2023 begleitete der Beschwerdeführer mit zwei weiteren Mitgliedern der … eine Versammlung der Organisation „Letzte Generation“ in Bamberg. Ziel des Beschwerdeführers war dabei, mit den Teilnehmenden der Demonstration ins Gespräch zu kommen und anschließend über die Versammlung in der Zeitschrift … zu berichten, so wie er es bereits zuvor mit anderen Aufzügen gemacht hatte. Einer seiner Begleiter trug eine Kamera bei sich, um für den Artikel Fotos zu schießen. Zwei der Polizeibeamten, die später die Beschlagnahme des Mobiltelefons des Beschwerdeführers durchführten, kannten den Beschwerdeführer und seine beiden Begleitpersonen von vorherigen Demonstrationen und wurden schon zu dieser Zeit darauf aufmerksam, dass der Beschwerdeführer die Demonstration berichterstattend begleitete.

So führte einer der Polizeibeamten in seinem zeugenschaftlichen Bericht vom … September 2023 aus:

„…“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 18 (**Anlage 3**).

Ein anderer der anwesenden Polizeibeamten gab in seinem zeugenschaftlichen Bericht vom … September 2023 an:

„…“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 36 (**Anlage 3**).

Schließlich wurde im Schlussvermerk vom … Oktober 2023 nach weiteren Ermittlungen festgestellt:

„*Das politische Engagement des Herrn … umfasst demnach auch diverse Demonstrationen, denen er in der Vergangenheit in verschiedenen Funktionen beiwohnte*“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 50 (**Anlage 3**).

Nach Ende der Versammlung beobachtete der Beschwerdeführer wie zwei Polizisten in Zivil drei Teilnehmende der Versammlung auf der Kapuzinerstraße in der Bamberger Innenstadt anhielten und gegen diese polizeiliche Maßnahmen durchführten.

Der Beschwerdeführer näherte sich der Gruppe und unterhielt sich kurz mit den Teilnehmenden der Versammlung. Er nahm sodann sein Mobiltelefon zur Hand und zeichnete die Ansprache der Polizeibeamten an die Betroffenen mit der Sprachnotiz-Funktion der Messaging-App … auf. Ihm wurde von einem der Polizisten mitgeteilt, dass das Aufzeichnen der Ansprache eine Straftat darstelle. Der Beschwerdeführer erwiderte hierauf, dass dem nicht so sei, da es sich um ein öffentlich gesprochenes Wort handele,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 17 (**Anlage 3**).

Einer der anwesenden Polizeibeamten schildert die Situation in seinem zeugenschaftlichen Bericht wie folgt:

> *„Als POK … nun von dem Erstellen der Lichtbilder zurückkam, erklärte er den weiteren Werdegang und beendete die polizeiliche Maßnahme. Hierbei sah ich, wie der spätere Beschuldigte sein Handy weiterhin in unsere Richtung hielt. Ich lief um POK … herum und begab mich auf Höhe des späteren Beschuldigten. Hierbei sah ich, wie er einen mir unbekannten „Messenger" geöffnet hatte und unter mehreren Textnachrichten eine Sprachnachricht aufgenommen hat. Als ich den Beschuldigten auf die Aufnahme ansprach, sperrte er sein Handy und steckte dieses in seine Hosentasche. Kurz vor dem versperren* [sic] *sah ich, wie er seinen Finger losließ und die eben aufgenommene Sprachnachricht versendete. ich teilte ihm mit, dass die Aufnahme unseres gesprochenen Wortes eine Straftat darstelle. Daraufhin erwiderte die Person … dass dies ein öffentlich gesprochenes Wort sei und somit nicht strafbar sei. Ich teilte den Personen mit, dass die polizeiliche Maßnahme … betrifft und somit nicht öffentlich sei*",
>
> siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 17 (**Anlage 3**).

Die Polizeibeamten forderten den Beschwerdeführer daraufhin dazu auf, sich zu identifizieren. Der Beschwerdeführer lehnte dies zunächst mit Hinweis darauf ab, dass er keine Straftat begangen habe, händigte seinen Ausweis dann aber einem der Beamten aus. Der Beschwerdeführer wurde dann darüber informiert, dass gegen ihn wegen Aufzeichnung des nicht-öffentlich gesprochenen Wortes ermittelt werden müsste und wurde als Beschuldigter über seine Rechte und Pflichten belehrt,

> siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 18 (**Anlage 3**).

Der Beschwerdeführer wurde sodann über die freiwillige Herausgabe seines Mobiltelefons belehrt und händigte sein Mobiltelefon sodann in gesperrtem Zustand an einen der Polizeibeamten aus. Der darauffolgenden Sicherstellung stimmte der Beschwerdeführer nicht zu, sodass die Polizei das Mobiltelefon beschlagnahmte. Einen PIN zur Entsperrung des Handys gab der

Beschwerdeführer nicht an. Nach Abschluss dieser polizeilichen Maßnahmen wurde der Beschwerdeführer entlassen,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 18 (**Anlage 3**).

Während der Maßnahmen erklärte einer der Polizisten dem Beschwerdeführer gegenüber, dass er ihn schon von anderen Versammlungen kenne und dass eine Aufzeichnung „nichts mehr mit Berichterstattung zu tun“ habe und „feige“ wäre.

Am ... September 2023 beantragte die Kriminalpolizeiinspektion Bamberg die Bestätigung der Beschlagnahme des Mobiltelefons. Die Ermittlungssache wurde hier wie folgt bezeichnet:

„*Verletzung der Vertraulichkeit des Wortes am … 09.2023, … in Bamberg, …*“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 22 (**Anlage 3**).

In der Begründung wurde folgende Passage festgehalten:

„…“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 22 (**Anlage 3**).

Noch am selben Tag wurde die Beschlagnahme durch Beschluss des Amtsgerichts Bamberg - … - bestätigt,

siehe Beschluss des Amtsgerichts Bamberg vom 8. September 2023 - … - (**Anlage 4**).

Das Amtsgericht stützte seine Entscheidung auf §§ 94, 98 Abs. 2 StPO i.V.m. §§ 111b, 111c, 111j Abs. 2 StPO,

siehe Beschluss des Amtsgerichts Bamberg vom 8. September 2023 - … -, S. 1 (**Anlage 4**).

In der Begründung der Entscheidung führte das Gericht unter anderem wie folgt aus:

> *„Die auf Anordnung d. POK …, PI Bamberg-Stadt bewirkte Beschlagnahme d. folgenden Gegenstände: „Mobiltelefon …“ wird gemäß §§ 94, 98 Abs. 2 StPO i.V.m. §§ 111b, 111c, 111j Abs. 2 StPO bestätigt. Gründe: Aufgrund der bisherigen Ermittlungen, insbesondere den Angaben d. PHM … besteht folgender Tatverdacht:* [Ausführungen zum Tatgeschehen]
>
> *Dies ist strafbar als Verletzung der Vertraulichkeit des Wortes gem. §§ 201a Abs. 1 Nr. 2, 205 StGB. Die oben genannten Gegenstände können als Beweismittel von Bedeutung sein. Die Aufnahme und der Versendungsnachweis befinden sich auf dem Mobiltelefon. Nach dem Ergebnis der bisherigen Ermittlungen sind Gründe für die Annahme vorhanden, dass die Voraussetzungen für die Einziehung vorliegen, § 201 Abs. 5 StGB.*
>
> *Die angeordnete/n Maßnahme/n steht/stehen im angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts und ist/sind für die Ermittlungen notwendig***“,**
>
> siehe Beschluss des Amtsgerichts Bamberg vom 8. September 2023 - … - (**Anlage 4**).

3. Zugriff auf und Auswertung des Mobiltelefons

Zur Entsperrung und Auslesung der Daten wurde das Mobiltelefon, das die Kriminalpolizeiinspektion Bamberg zuvor an die Staatsanwaltschaft Bamberg übermittelt hatte, zunächst an den Technischen Ergänzungsdienst Bamberg übermittelt:

> *„Das am ...09.2023 beschlagnahmte Handy des Beschuldigten … wurde nach Beauftragung über den Sachbearbeiter durch den Technischen Ergänzungsdienst Bamberg softwaretechnisch gesichert*“,

siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Wie sich aus den insgesamt sieben der Akte beigefügten Extraktionsberichten entnehmen lässt, wurde für diese Extraktion sowie die anschließende inhaltliche Auswertung forensische Extraktions- und Auswertungssoftware des Herstellers Cellebrite verwendet,

siehe Extraktionsbericht 1, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 57 ff. (**Anlage 3**).

Die Extraktionssoftware von Cellebrite ist weit verbreitet und wird von vielen deutschen Polizeibehörden zur digitalen Forensik eingesetzt. Die Extraktionssoftware von Cellebrite, insbesondere das sog. UFED (Universal Forensic Extraction Device), wird von Strafverfolgungsbehörden genutzt, um beschlagnahmte Mobiltelefone zu entsperren und die sich darauf befindlichen Daten auszulesen und zu analysieren. Dazu wird das Telefon an ein spezielles UFED-Gerät angeschlossen. Abhängig vom gewählten Verfahren können dann verschiedene Datenebenen abgerufen werden. Während die logische Extraktion nur aktiv gespeicherte Daten wie SMS, Anruflisten, Mediendateien oder App-Informationen erfasst, erlaubt die physikalische Extraktion eine bitweise Auslesung des Gerätespeichers, bei der auch bereits gelöschte Inhalte wie SMS oder Chatverläufe rekonstruiert und ein vollständiger sog. Speicherdump, d.h. eine vollständige Kopie des Inhalts des Hauptspeichers des Mobiltelefons (Flash-Speicher), erstellt werden können. Die ausgelesenen Informationen werden anschließend in einem strukturierten Bericht zusammengeführt. Dieser enthält neben allgemeinen Geräteinformationen (z.B. IMEI, Apple-ID, Telefonnummer) auch Metadaten zu Medieninhalten, eine vollständige Kontaktliste, Anrufprotokolle, WLAN-Verbindungen, Sprachmitteilungen und App-Daten. Darüber hinaus visualisiert die Software Geodaten von Fotos auf Karten, stellt Nachrichten in chronologischer Gesprächsansicht dar und analysiert Aktivitäten einzelner Telefonnummern. In speziellen Fällen lassen sich sogar gelöschte Notizen, Konfigurationen oder Login-Daten rekonstruieren,

Produktinformation zu Cellebrite Universal Forensic Extraction Device, abrufbar unter: https://cellebrite.com/en/ufed/ (Letzter Abruf: 22. Juli 2025).

Wie sich aus dem Inhalt der Ermittlungsakte und insbesondere dem darin enthaltenen Bericht „Sonstige Erkenntnisse Handyauswertung“ (dazu sogleich) ergibt, wurde bei der technischen Sicherung der gesamte Datenbestand des Mobiltelefons ausgelesen und zur inhaltlichen Auswertung zur Verfügung gestellt. In diesem Ermittlungsbericht wurde festgehalten, dass die „*Mobiltelefonauswertung des Gerätes*“, d.h. die inhaltliche Analyse der vorfindlichen Informationen, nur „*stichprobenartig*“ hätte erfolgen können, da eine umfassende Auswertung aufgrund der Menge der ausgelesenen Daten „*mindestens mehrere Wochen Zeit in Anspruch genommen hätte*“. Der Wortlaut des Berichts verdeutlicht das Ausmaß der Datenauslesung und der auf diese Daten gestützte Auswertung:

> „*Abschließend bleibt festzuhalten, dass die Mobiltelefonauswertung des Gerätes des Herrn … nur stichprobenartig durchgeführt werden konnte. Es waren beispielhaft … Kontakte in allen erdenklichen Social-Media-Netzwerken hinterlegt. Hinzu kamen … Nachrichten, die über diese Plattformen versandt wurden. Die gleichen Größenordnungen lagen auch bei Bildern und Videos vor, sodass eine detaillierte Auswertung demnach mindestens mehrere Wochen Zeit in Anspruch genommen hätte*“,
>
> siehe „Sonstige Erkenntnisse Handyauswertung“, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 76 ff. (**Anlage 3**).

Am 6. Dezember 2023 wurde der zuvor ausgelesene komplette Datenbestand des Mobiltelefons zur inhaltlichen Auswertung an die Kriminalpolizeiinspektion übermittelt:

> „*Das am ...09.2023 beschlagnahmte Handy des Beschuldigten Herrn … wurde nach Beauftragung über den Sachbearbeiter durch den Technischen Ergänzungsdienst Bamberg softwaretechnisch gesichert und schließlich zur Auswertung dessen am ….12.2023 an den Unterzeichner ermittelt*“,
>
> siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Nach dem Ermittlungsbericht vom 18. Dezember 2023 des zuständigen Bearbeiters lag bei der Datenauswertung das

„*Hauptaugenmerk zunächst darauf, den Nachweis für die möglicherweise begangene Verwirklichung des Tatbestandes der Verletzung der Vertraulichkeit des Wortes nach § 201 StGB durch den Beschuldigten zu finden*“,

siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Die Beamt*innen werteten hierfür einen Chat des Anbieters …, der bis auf den Beschwerdeführer keine weiteren Teilnehmer*innen enthielt, sondern vielmehr als digitales Notizbuch bzw. digitaler Merkzettel diente, vollständig aus:

„…“,

siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Wie auch diesem Vermerk zu entnehmen ist, wurden in den ersten, der Akte beigefügten Extraktionsberichten aber nicht nur Notizen vom … September 2023 aufgenommen, sondern vielmehr der gesamte Nachrichtenverlauf des Chats. Insbesondere wurden alle neun Sprachnachrichten auf einem weiteren Datenträger gesichert sowie unter der Überschrift „*Verschriftung Inhalt tatrelevanter Daten*“ durch die Polizei transkribiert und an die Staatsanwaltschaft übersendet,

siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Acht der neun Aufnahmen enthalten ausschließlich die Stimme des Beschwerdeführers und beziehen sich auf seine Kommentare zum allgemeinen Geschehen nach der Demonstration. Diese wurden allesamt auf einem Datenträger gesichert,

siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**).

Wie sich aus dem weiteren Bericht „*Sonstige Erkenntnisse Handydatenauswertung*“ ebenfalls vom 18. Dezember 2023 ergibt, beließen es die Beamt*innen aber nicht dabei, für den Tatvorwurf relevante Daten auszuwerten,

> siehe „Sonstige Erkenntnisse Handyauswertung“, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 76 f. (**Anlage 3**).

Vielmehr kam es neben der Auswertung des …-Chats auch zu einer Auswertung sonstiger auf dem Mobiltelefon gespeicherter Daten, die der Erstellung eines politischen Profils des Beschwerdeführers diente. Ausgewertet wurden dabei unter anderem Chats des Beschwerdeführers mit privaten und professionellen Kontakten (auf …), auf dem Mobiltelefon gespeicherte Bilder, sowie Mitgliedschaften in Chatgruppen und Newslettern. Der zuständige Beamte analysierte etwa Text- und Sprachnachrichten, die der Beschwerdeführer mit anderen politisch engagierten Personen austauschte, versuchte durch die Mitgliedschaft in Chat-Gruppen Verbindungen des Beschwerdeführers zu bestehenden politischen Gruppierungen nachzuzeichnen und las Sprachdateien aus, um mehr über die politische Gesinnung des Beschwerdeführers zu erfahren.

Unter den Dutzenden der Akte beigefügten Textnachrichten und anderen Dateien finden sich beispielsweise Nachrichten mit den folgenden Inhalten:

> *„…“*,
>
> siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 78 (**Anlage 3**).
>
> *„Teilnehmer:*
> *…*
> *… (Eigentümer)*
> *…*
> *Hallo, ich würde gerne mit einem Kollegen mit nach …, um die Demo journalistisch zu begleiten. Sind … noch zwei Plätze frei? Liebe Grüße!“*,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 79 (**Anlage 3**).

„…“,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 79 (**Anlage 3**).

Im Wortlaut liest sich der Bericht „*Sonstige Erkenntnisse Handydatenauswertung*“ wie folgt (Auszüge):

„…“,

siehe „Sonstige Erkenntnisse Handyauswertung“, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 76 f. (**Anlage 3**).

Die dem Ermittlungsbericht beigefügten Extraktionsberichte umfassen die genannten und eine Vielzahl an weiteren Nachrichten und zahlreiche Kontakte Dritter,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 78-110 (**Anlage 3**).

Im Einzelnen enthalten diese Extraktionsberichte jeweils Kopien versandter Nachrichten inklusive der beteiligten Kommunikationspartner*innen unter Angabe entweder der Telefonnummer und des Namenseintrags im Kontaktverzeichnis des Mobiltelefons oder anderer identifizierender Bezeichnungen (etwa des …-Benutzernamens),

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 78-110 (**Anlage 3**).

Teile der Auswertung wurden auf einer Daten-DVD gespeichert oder sind als Extraktionsberichte der Akte beigefügt,

siehe „Sonstige Erkenntnisse Handyauswertung“, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 76 (**Anlage 3**).

Am … August 2024 wurde das Verfahren dann gem. § 170 Abs. 2 StPO eingestellt, da der gem. § 205 Abs. 1 StGB zwingend erforderliche Strafantrag nicht rechtzeitig gestellt worden war,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 136 (**Anlage 3**).

Am … September 2024 wurde dem Beschwerdeführer sein Mobiltelefon zurückgegeben,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 162 (**Anlage 3**).

Am … Dezember 2024 überließ der Beschwerdeführer sein Mobiltelefon der Organisation Reporter ohne Grenzen (Reporters sans frontières – RSF), um untersuchen zu lassen, wie sein Handy ausgewertet wurde, ob durch den Einsatz der Forensik-Software auf Daten unter Überwindung der Verschlüsselung zugegriffen und Veränderungen an Programmdateien oder Konfigurationen des Betriebssystems oder Applikationen des Smartphones vorgenommen und dabei Sicherheitslücken ausgenutzt wurden. Dazu hat RSF einen Auswertungsbericht erstellt,

Schlüter/Besendorf, RSF Digital Security Lab, Forensische Analyse … (**Anlage 5**).

Eine Löschung der nach dem Datenzugriff gespeicherten Daten wird der Beschwerdeführer zeitnah bei der Staatsanwaltschaft beantragen.

4. Verfahrensverlauf

Der Beschwerdeführer legte am 17. April 2025 Beschwerde gegen den Beschluss des Amtsgerichts Bamberg vom … September 2023 - … - ein, mit welchem die Beschlagnahme seines Mobiltelefons bestätigt wurde,

siehe Beschwerde vom 17. April 2025 (**Anlage 6**).

Mit Schriftsatz vom 19. Juni 2025 begründete der Beschwerdeführer diese Beschwerde,

siehe Beschwerdebegründung vom 19. Juni 2025 (**Anlage 7**).

Der Beschwerdeführer beantragte, den Beschluss des Amtsgericht Bamberg vom 8. September 2023 aufzuheben, die Rechtswidrigkeit der Sicherstellung und Auswertung festzustellen und die Löschung aller gesicherten Daten anzuordnen.

Zur Begründung führte der Beschwerdeführer aus, dass die Beschlagnahme und der Datenzugriff auf sein Mobiltelefon sowie die Auswertung der Daten schwerwiegende Eingriffe in seine Grundrechte darstellen würden, die nicht gerechtfertigt seien.

Betroffen seien die Grundrechte auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), auf Eigentumsgarantie (Art. 14 Abs. 1 Satz 1 GG) sowie die Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG),

siehe Beschwerdebegründung vom 19. Juni 2025, S. 2, 11-15 (**Anlage 7**).

Es mangele schon an einer spezifischen Gesetzesgrundlage, die verfassungs- und unionsrechtlichen Vorgaben genüge. Es handele sich um Eingriffe mit besonders hoher Intensität. Polizeibehörden erhielten durch die Nutzung der hier gegenständlichen Forensik- und Analyse-Tools Zugriff auf den gesamten Datenbestand eines beschlagnahmten Mobiltelefons und erhielten dadurch gewissermaßen Zugang zum gesamten digitalen Hausstand des Betroffenen. Dies umfasse auch besonders private und sensible Daten wie etwa Nachrichten an Familienmitglieder und Partner*innen, Informationen über Gesundheitszustand, sexuelle Orientierung und politische Überzeugung, Zugang zu Email-Accounts und vielem mehr. Das Eingriffsgewicht würde durch die enorme Streubreite und dadurch, dass der Betroffene keine Kenntnis davon erhalten könne, in welcher Form auf sein Gerät zugegriffen, wie dieses anschließend ausgewertet würde und der Eingriff deswegen im Wesentlichen intransparent erfolge, noch erheblich erhöht,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 15-21 (**Anlage 7**).

Aufgrund dieser Umstände bedürfe es vergleichbar zu den in ihrer Intensität ähnlichen Eingriffen nach § 100b Abs. 1 StPO oder § 100a StPO einer spezifischen, hinreichend bestimmten Ermächtigungsgrundlage, die Schutzvorkehrungen für den Kernbereichsschutz sowie strenge Vorgaben für die Wahrung der Verhältnismäßigkeit vorsehen müsse. Diesen Anforderungen

würden die §§ 94 ff. StPO nicht gerecht. Die Normen verstießen gegen die verfassungsrechtlichen Gebote der Bestimmtheit und Normenklarheit, weiter auch gegen den Grundsatz, dass der Gesetzgeber in allen grundlegenden normativen Bereichen die wesentlichen Entscheidungen selbst treffen muss. Die §§ 94 ff. StPO regelten den Zugriff und die Auswertung von Datenträgern schon gar nicht. Dementsprechend sähen sie auch keine – verfassungsrechtlich erforderlichen – bestimmten Grenzen für derartige Eingriffe vor. Weiter fehle es auch an gesetzlichen Sicherungen, die einen hinreichenden Schutz des Kernbereichs privater Lebensgestaltung gewährleisten könnten, wie dies vom Bundesverfassungsgericht gefordert werde,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 21-29 (**Anlage 7**).

Weiter seien die §§ 94 ff. StPO, insofern sie einen vollständigen Datenzugriff und eine umfassende Datenauswertung ermöglichten, auch unverhältnismäßig, da die Vorschriften keine hinreichenden tatbestandlichen Begrenzungen auf angemessene Fälle vorsähen. Die hohe Eingriffstiefe und -intensität begründeten hohe gesetzliche Anforderungen an die Wahrung der Verhältnismäßigkeit. Diesen genügten die §§ 94 ff. StPO nicht, da sie weder Beschränkungen hinsichtlich der Anlasstat vorsähen noch hinreichende Vorgaben zur erforderlichen Erfolgstauglichkeit enthielten,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 30-32 (**Anlage 7**).

Schließlich seien die §§ 94 ff. StPO auch deswegen nicht verfassungsgemäß, weil sie nicht die notwendigen verfahrensrechtlichen Sicherungen in Gestalt von Auskunfts-, Lösch-, Dokumentations- und Beteiligungspflichten vorsähen. In den §§ 94 ff. StPO fehlten solche Transparenz- und Auskunftspflichten sowie Protokollierungspflichten und Vorgaben zur Ermöglichung effektiver Beteiligung von Verteidiger*innen, die zur Wahrung der Verhältnismäßigkeit notwendig seien,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 32-34 (**Anlage 7**).

Weiter verstieße die Anwendung der §§ 94 ff. StPO auf den Zugriff und die Auswertung der sich auf beschlagnahmten Mobiltelefonen befindlichen Daten auch gegen Unionsrecht, konkret gegen Art. 4 Abs. 1 lit. c der Richtlinie (EU) 2016/680 (nachfolgend JI-Richtlinie). In der

Entscheidung „Bezirkshauptmannschaft Landeck“ vom 4. Oktober 2024 habe der Europäische Gerichtshof unionsrechtliche Anforderungen an die Vereinbarkeit des Datenzugriffs auf Mobiltelefone aus den Vorgaben der JI-Richtlinie hinsichtlich der Ausgestaltung der Rechtsgrundlage abgeleitet, denen die §§ 94 ff. StPO im vorliegenden Fall nicht genügten. Konkret hätte der Europäische Gerichtshof hier klargestellt, dass eine gesetzliche Grundlage, die den Datenzugriff auf Mobiltelefone ermöglicht, dem in Art. 4 Abs. 1 lit. c JI-Richtlinie angelegten Grundsatz der Datenminimierung entsprechen müsse, und der Grundsatz der Verhältnismäßigkeit nationale Gesetzgeber dazu verpflichte, insbesondere die Art oder die Kategorien der betroffenen Straftaten hinreichend präzise zu definieren. Weiter bedürfe es bei jedem Datenzugriff grundsätzlich einer vorgelagerten unabhängigen Kontrolle, die sich nicht nur auf die Beschlagnahme beziehen dürfe, sondern eigenständig (auch) den Datenzugriff und dessen Reichweite selbst umfassen müsse. Sämtlichen Anforderungen würden die §§ 94 ff. StPO nicht gerecht,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 35-41 (**Anlage 7**).

Weiter seien die Maßnahmen auch im Einzelfall rechtswidrig gewesen. Es habe schon am erforderlichen Anfangsverdacht gefehlt, denn der Beschwerdeführer hätte das Gesagte offensichtlich aufnehmen dürfen. Es hätte sich bei der Ansprache um eine für jedermann sichtbare und hörbare polizeiliche Maßnahme auf offener Straße gehandelt. Der Beschwerdeführer sei eindeutig als unbeteiligter Passant erkennbar gewesen; es habe sich insofern um eine faktische Öffentlichkeit gehandelt,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 41 f. (**Anlage 7**).

Außerdem sei die Maßnahme auch im konkreten Einzelfall unverhältnismäßig gewesen. Es hätte sich um einen gravierenden Eingriff in die Pressefreiheit und die übrigen einschlägigen Grundrechte gehandelt. Der Zugriff sei in großen Teilen schon nicht erforderlich gewesen, da umfangreich auf Daten zugegriffen wurde, die in gar keinem Zusammenhang mit dem Strafvorwurf stünden. Zu beachten sei außerdem, dass es sich um einen äußerst geringfügigen Tatvorwurf gehandelt habe, der in keinem Verhältnis zu einem derart schwerwiegenden Grundrechtseingriff stünde,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 42-47 (**Anlage 7**).

Schließlich seien auch die Rechte auf effektive Verteidigung und ein faires Verfahren nach den Art. 6 EMRK und Art. 103 Abs. 1 GG und das Recht auf Privatleben aus Art. 8 EMRK verletzt,

siehe Beschwerdebegründung vom 19. Juni 2025, S. 47 f. (**Anlage 7**).

Das Landgericht Bamberg entschied über diese Beschwerde mit Beschluss vom 27. Juni 2025 - ... - und half der Beschwerde im Wesentlichen nicht ab,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 1 (**Anlage 2**).

Der Beschwerdeführer obsiegte hier nur soweit die Ermittlungsmaßnahmen, konkret die Beschlagnahme und Auswertung des Mobiltelefons, nach Ablauf des … Dezember 2023, an dem die Frist für die Stellung des zwingend notwendigen Strafantrags ablief, nicht eingestellt wurden. Insofern stellte das Gericht fest,

„*dass die Fortdauer der Beschlagnahme und Auswertung des am … 09.2023 sichergestellten Mobiltelefons …, nach Ablauf des … 12.2023 bis zur Herausgabe des Mobiltelefons am ...09.2024 rechtswidrig gewesen ist*“,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 1 (**Anlage 2**).

Im Übrigen wies das Landgericht die Beschwerde im hier gegenständlichen Bereich als unbegründet zurück,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 1 (**Anlage 2**).

Das Landgericht ging dabei davon aus, dass die Beschlagnahmeanordnung vom … September 2023 ursprünglich rechtmäßig ergangen ist und bis zum Ablauf des ... Dezember 2023 rechtmäßig war.

Zur Begründung führte das Landgericht zunächst aus:

„*Nach der obergerichtlichen Rechtsprechung entsprechen die §§ 94 ff. StPO den verfassungsrechtlichen und den sich aus der Richtlinie 2016/680/EU, auch unter Berücksichtigung des Urteils des EuGH vom 4. Oktober 2024, Az. C-548/21, ergebenden Anforderungen hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern - inklusive Mobiltelefonen - und den hierauf gespeicherten Daten (vgl. BGH Beschl. v. 13.3.2025 - 2 StR 232/24, BeckRS 2025, 9876 m.w.N.)*“,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 5 (**Anlage 2**).

Weiter sei die Beschlagnahmeanordnung vom … September 2023 ursprünglich rechtmäßig ergangen, da die Voraussetzungen der §§ 94 ff. StPO zum Zeitpunkt des Erlasses und bis zum Ablauf des … Dezember 2023 vorgelegen hätten.

Ein ausreichender Anfangsverdacht hätte vorgelegen. Insbesondere hätte es sich bei den aufgezeichneten Äußerungen um „*nichtöffentlich gesprochenes Wort*“ im Sinne des § 201 Abs. 1 Nr. 1 StGB gehandelt. Entscheidend hierfür wäre nämlich zunächst die Bestimmung durch den Sprecher. Grundsätzlich unterfielen daher auch polizeiliche Kontrollen dem Schutzbereich des § 201 StGB. Äußerungen einer Demonstrantin und eine hierauf erfolgende Gegenäußerung gegenüber einem Polizeibeamten seien nicht deswegen öffentlich, weil dieses Gespräch am Rande einer Demonstration erfolgte. Auch Medienvertreter hätten insoweit keinen Sonderstatus und bedürften zur Aufzeichnung der Einwilligung des Betroffenen. Mit weiteren Zuhörern außerhalb des abgegrenzten Personenkreises hätten die Polizeibeamten nicht rechnen müssen,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 5 (**Anlage 2**).

Auch der Umstand, dass zum Zeitpunkt des Beschlusserlasses am 8. September 2023 ein Strafantrag noch nicht gestellt worden war, hätte der Rechtmäßigkeit nicht entgegengestanden, da nur die begründete Annahme, dass ein Strafantrag auch bis zum Ende der Antragsfrist nicht mehr gestellt würde, der Rechtmäßigkeit hätte entgegenstehen können,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 5 f.
(**Anlage 2**).

Weiter hätte die auf dem beschlagnahmten Mobiltelefon gespeicherte relevante Sprachnachricht auch Beweisbedeutung für die Untersuchung des vorliegenden Tatverdachts im Sinne des § 94 StPO gehabt. Es wäre in Betracht gekommen, dass das Mobiltelefon und das etwaige Vorhandensein einer entsprechenden Sprachnachricht als Beweismittel für die Tatbestandsverwirklichung des § 201 Abs. 1 Nr. 1 StGB dienen könnten,

siehe Beschluss des LG Bamberg vom 27. Juni 2025 - ... -, S. 6 (**Anlage 2**).

Schließlich wäre auch der Verhältnismäßigkeitsgrundsatz in dem Zeitraum zwischen Beschlagnahme und Ablauf der Strafantragsfrist gewahrt gewesen. Hierzu führte das Gericht wie folgt aus:

> „*Der besonderen Eingriffsintensität in die Grundrechte des Beschuldigten beim Zugriff auf ein Mobiltelefon ist im Rahmen der Verhältnismäßigkeitsprüfung Rechnung zu tragen (BGH Beschl. v. 13.3.2025 - 2 StR 232/24, BeckRS 2025, 9876 m.w.N.). Abzuwägen sind einerseits das staatliche Interesse an einer wirksamen Strafverfolgung (die Sicherung des Rechtsfriedens durch Strafrecht, die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind seit jeher staatliche Kernaufgaben), andererseits die geschützten Rechtsgüter der von der Maßnahme Betroffenen. Die Schwere der Straftat, die Gegenstand der Ermittlungen ist, stellt dabei einen zentralen Parameter dar. Maßgebend ist, wie sich das Gewicht der Straftat im Einzelfall darstellt. Bestimmende Gesichtspunkte sind daneben der Grad des Tatverdachtes und die potentielle Beweisbedeutung der auf dem Mobiltelefon vermuteten Daten. In Betracht zu ziehen ist auch, ob die in Rede stehenden Straftaten mittels eines Mobiltelefons begangen oder angebahnt wurden. Denn wenn der Beschuldigte bewusst ein Medium als Tatmittel seiner strafbaren Handlung einsetzt, muss er es eher hinnehmen, dass sich die Strafverfolgungsbehörden des darauf befindlichen Datenbestandes bedienen (BGH Beschl..v. 13.3.2025 - 2 StR 232/24, BeckRS 2025, 9876 Rn. 48 m.w.N.). Der Zugriff auf überschießende, für das Verfahren bedeutungslose Informationen, insbesondere vertrauliche Daten Unbeteiligter, muss jedoch im Rahmen des Vertretbaren vermieden werden. Es ist stets zu prüfen, ob z.B. die Anfertigung einer Kopie der verfahrensrelevanten Daten genügt (Meyer-Goßner/Schmitt,*

StPO, 67. Auflage 2024, § 94 Rn. 18a). Auch kann die weitere Beschlagnahme wegen Zeitablaufs unverhältnismäßig sein, wobei sich aus dem Grundsatz der Verhältnismäßigkeit keine allgemeingültigen Zeitgrenzen für die Auswertung von Beweismitteln ableiten lassen. Welcher Zeitraum für die Durchsicht angemessen erscheint, beurteilt sich im Wege einer Abwägung nach den Umständen des Einzelfalls (Hauschild in Münchener Kommentar zur StPO, § 94 Rn. 33 m.w.N.).

Vorliegend lag dem damaligen Beschuldigten einerseits lediglich ein Vergehen nach § 201 Abs. 1 Nr. 1 StGB zur Last. Andererseits bestand der Tatverdacht, dieses gerade durch Aufnahme einer Sprachnachricht mittels Mobiltelefon begangen zu haben, sodass der beschlagnahmte Gegenstand entscheidende Beweisbedeutung für die Frage der Tatbestandsverwirklichung hatte. Mildere Mittel, wie eine Datenspiegelung, kamen zwischen der Sicherstellung und dem Ablauf der Strafantragsfrist noch nicht in Betracht, da die PIN zur Entsperrung des Handys nicht benannt wurde (Bl. 8 d. A.) und die Datensicherung erst am 6.12.2023 vorlag (Bl. 40 d. A.). Angaben dahingehend, dass der Beschwerdeführer journalistisch tätig sei, das Mobiltelefon im Rahmen von Pressearbeit benötigen würde und entsprechende vertrauliche Kontakte und Informationen über Dritte eingespeichert seien, hatte jener weder im Rahmen der Sicherstellung am … 09.2023 noch danach - auch nicht, nachdem sich ein Rechtsanwalt als Verteidiger angezeigt hatte (Bl. 28 d. A.) - gemacht. Diese Umstände waren vor Ablauf der Strafantragsfrist weder aktenkundig noch sonst bekannt. Die inhaltliche Auswertung des Mobiltelefons fand ausweislich der Datierung der entsprechenden Vermerke (vgl. B.l 41, 62 d. A.) erst danach statt. Auch war die bis zum Ablauf der Strafantragsfrist dreimonatige Dauer der Beschlagnahme zum Zwecke der Auswertung des Mobiltelefons noch nicht unverhältnismäßig, insbesondere weil die PIN zur Entsperrung des Mobiltelefons nicht bekannt gewesen war. Insgesamt stellte sich die Beschlagnahme damit als ursprünglich und bis zum Ablauf der Strafantragsfrist verhältnismäßig dar“,

siehe Beschluss des LG Bamberg vom 27. Juni 2025, S. 6 ff. (**Anlage 2**).

Gegen den Beschluss legte der Beschwerdeführer am 10. Juli 2025 beim LG Bamberg Anhörungsrüge gem. § 33a StPO ein,

siehe Anhörungsrüge vom 10. Juli 2025 (**Anlage 8**).

Der Beschwerdeführer rügte damit, dass das Gericht seinen tatsächlichen und rechtlichen Vortrag in mehreren wesentlichen Punkten nicht bzw. nicht hinreichend zur Kenntnis genommen und in Erwägung gezogen habe. Konkret rügte der Beschwerdeführer zunächst, dass das Gericht ersichtlich keinen der in der Beschwerdebegründung ausgeführten rechtlichen Gesichtspunkte berücksichtigt hätte, aus denen sich die Verfassungs- und Unionsrechtswidrigkeit eines auf §§ 94 ff. StPO gestützten Datenzugangs ergebe,

siehe Anhörungsrüge vom 10. Juli 2025, S. 5 (**Anlage 8**).

Das Beschwerdegericht hätte die Verfassungs- und Unionsrechtsmäßigkeit in nur einem einzigen Satz angenommen. Das Gericht hätte die in der Beschwerdebegründung erfolgten Ausführungen zur Verfassungswidrigkeit des Datenzugangs vollständig unberücksichtigt gelassen. Es hätte sich weder mit dem Fehlen einer hinreichend bestimmten Gesetzesgrundlage noch mit dem Erfordernis gesetzlicher Schutzvorkehrungen für den Kernbereich oder mit der Unverhältnismäßigkeit des Eingriffs auseinandergesetzt. Auch die Ausführungen zum Verstoß gegen die Gebote der Normenklarheit und Bestimmtheit, zum Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, zur Unanwendbarkeit der bisherigen verfassungsgerichtlichen Rechtsprechung und zum Fehlen des Kernbereichsschutzes hätte das Gericht in Gänze ignoriert. Auch Gesichtspunkte zur Unverhältnismäßigkeit des Datenzugriffs wären unberücksichtigt geblieben,

siehe Anhörungsrüge vom 10. Juli 2025, S. 6 ff. (**Anlage 8**).

Den Vortrag zur Unionsrechtswidrigkeit des Datenzugriffs hätte das Gericht vollständig übergangen und nur pauschal auf die lückenhafte Auseinandersetzung mit den unionsrechtlichen Vorgaben in dem benannten BGH-Beschluss verwiesen,

siehe Anhörungsrüge vom 10. Juli 2025, S. 8 ff. (**Anlage 8**).

Auch den Vortrag zum Nichtbestehen eines Anfangsverdachts hätte das Gericht in zentralen Punkten missachtet. Insofern hätte das Gericht insbesondere nicht zu erkennen gegeben,

warum die gegenständlichen Äußerungen der Polizeibeamten als „nicht-öffentlich gesprochenes Wort“ gelten konnten, obwohl sie in einer allgemein zugänglichen und wahrnehmbaren Situation erfolgten,

siehe Anhörungsrüge vom 10. Juli 2025, S. 10 f. (**Anlage 8**).

Schließlich hätte das Gericht auch wesentliche Gesichtspunkte des Vortrags zur Unverhältnismäßigkeit der Maßnahme im Einzelfall nicht beachtet. Insofern hätte das Gericht im Rahmen seiner Verhältnismäßigkeitsprüfung insbesondere keine hinreichende Differenzierung der erfolgten Maßnahmen vorgenommen und den diesbezüglichen Vortrag des Beschwerdeführers nicht beachtet. Das Gericht hätte in seinem Beschwerdebeschluss maßgeblich nur zwischen der Beschlagnahme des Mobiltelefons (nach Meinung des Gerichts verhältnismäßig) und der inhaltlichen Auswertung des Mobiltelefons zur Erstellung eines politischen Profils des Beschwerdeführers (wegen Ablaufs der Antragsfrist rechtswidrig) unterschieden, nicht aber – wie von der Beschwerdebegründung mehrfach unterstrichen – auch die anderen erfolgten Eingriffsschritte (eigenständig) bewertet, d.h. insbesondere den Zugriff unter Überwindung der PIN-Sperre des Mobiltelefons, jede nachfolgende Durchsicht, die Speicherung und die Übermittlung der auf dem Mobiltelefon vorgefundenen Daten. Aufgrund der fehlenden Differenzierung hätte sich das Gericht auch nicht hinreichend mit der Notwendigkeit einer Beschränkung der Eingriffsmaßnahmen auseinandersetzen können. Das Gericht hätte demnach auch nicht erkannt, dass schon die Bestätigung der Beschlagnahme und die übrigen der inhaltlichen Auswertung vorgehenden Eingriffsmaßnahmen von vornherein auf die Sicherstellung der betroffenen Sprachnachricht beschränkt werden hätten müssen bzw. eine Eingrenzung der Maßnahmen nach Dateiname, -typ oder -datum erfolgen hätte müssen,

siehe Anhörungsrüge vom 10. Juli 2025, S. 11 ff. (**Anlage 8**).

Zuletzt hätte sich das Gericht auch mit weiteren zentralen Teilen des Vorbringens des Beschwerdeführers zur Unverhältnismäßigkeit der Maßnahmen nicht befasst. So hätte es nicht zu erkennen gegeben, ob es seinen Einschätzungen zur Betroffenheit der Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 14 Abs. 1 GG folge,

siehe Anhörungsrüge vom 10. Juli 2025, S. 11 ff. (**Anlage 8**).

Die Entscheidung über die Anhörungsrüge steht noch aus.

C. Verfassungsbeschwerde

Die Verfassungsbeschwerde ist zulässig und begründet.

I. Zulässigkeit und Annahmevoraussetzungen

Die Verfassungsbeschwerde ist zulässig.

1. Beschwerdeberechtigung

Der Beschwerdeführer ist als natürliche Person Träger von Grundrechten und damit beschwerdeberechtigt.

2. Beschwerdegegenstand

Die Verfassungsbeschwerde richtet sich gegen den Beschluss des Landgerichts Bamberg vom 27. Juni 2025 - ... -. Bei diesem handelt es sich um einen Akt der öffentlichen Gewalt, der dem Beschwerdeführer gegenüber auch Außenwirkung entfaltet, und dementsprechend gem. § 90 Abs. 1 BVerfGG einen tauglichen Beschwerdegegenstand der Verfassungsbeschwerde darstellt.

3. Beschwerdebefugnis

Der Beschwerdeführer ist beschwerdebefugt. Er ist durch den angegriffenen Beschluss selbst, gegenwärtig und unmittelbar in nach Art. 93 Abs. 1 Nr. 4a GG und § 90 Abs. 1 BVerfGG beschwerdefähigen Grundrechten verletzt.

a. Gerügte Grundrechtsverletzung

Der Beschwerdeführer rügt eine Verletzung seines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), hilfsweise seines Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Darüber hinaus rügt er eine Verletzung seines Grundrechts auf Eigentum (Art. 14 Abs. 1 S. 1 GG), auf Pressefreiheit (Art. 5 Abs. 1 S. 2 GG), auf Meinungsfreiheit (Art. 5 Abs. 1 Satz 1 GG), auf allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) sowie seines Rechts auf rechtliches Gehör (Art. 103 Abs. 1 GG) und seines Rechts auf den*die gesetzliche*n Richter*in (Art. 101 Abs. 1 S. 2 GG). Dabei handelt es sich um beschwerdefähige Grundrechte und grundrechtsgleiche Rechte, deren Verletzung mit der Verfassungsbeschwerde gerügt werden kann.

Die Geltung der Grundrechte ist vorliegend auch nicht durch den Anwendungsvorrang des Unionsrechts verdrängt, denn es handelt sich nicht um einen Fall der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen,

> BVerfG, Beschluss vom 6. November 2019 - 1 BvR 16/13 -, NJW 2020, 300 (301 Rn. 42).

Diese Grundrechte sind verletzt: Die Entsperrung eines Mobiltelefons, der technische Zugriff darauf und die Auslesung sowie Übermittlung der auf diesem befindlichen Daten stellt eine besonders schwerwiegende Beeinträchtigung sowohl der Integrität als auch der Vertraulichkeit eines komplexen IT-Systems gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar (siehe dazu **II.1.a.** und **II.1.b.**), jedenfalls einen Eingriff in das Recht auf informationelle Selbstbestimmung mit besonders hoher Intensität (siehe dazu **II.2.a.**), der verfassungsrechtlich nicht gerechtfertigt werden kann (siehe dazu **II.1.c.** und **II.2.b.**). Die §§ 94 ff. StPO bieten für derartige Eingriffe schon keine verfassungs- oder unionsrechtskonforme Grundlage. Die Normen regeln den Zugriff auf informationstechnische Systeme selbst nicht explizit und stellen deshalb – insbesondere unter Anbetracht der Schwere des Eingriffs – keine hinreichend klare und bestimmte Eingriffsgrundlage dar. Die Gesetzesgrundlage sieht überhaupt keine Grenzen oder Regeln für den Zugriff auf derartige Systeme vor und eröffnet deshalb regelmäßig den Zugriff auf den gesamten Datenbestand eines Mobiltelefons. Aus diesem Grund verstößt die Regelung auch gegen die Wesentlichkeitslehre. Weiter gewährleisten die rechtlichen Ermächtigungsgrundlagen nicht den erforderlichen Kernbereichsschutz. Weder auf der Ebene der Datenerhebung noch auf der

Ebene der Datenauswertung sehen die §§ 94 ff. StPO Vorkehrungen vor, die einer Ausspähung des Kernbereichs privater Lebensgestaltung hinreichend vorbeugen können. Außerdem erlauben die §§ 94 ff. StPO, gemessen an den Maßstäben des angerufenen Gerichts, unverhältnismäßige Eingriffe, denn sie lassen besonders eingriffsintensive Maßnahmen auch beim Verdacht von ganz geringfügigen Delikten zu, die nicht dem Schutz hinreichend gewichtiger Rechtsgüter dienen. Darüber hinaus setzen die Normen auch nicht die erforderliche qualifizierte Beweisrelevanz einer Maßnahme voraus. Weiter gewährleisten die Vorschriften auch nicht die verfahrensrechtlichen Sicherungen, insbesondere keine ausreichenden Dokumentationspflichten, die für die Wahrung eines effektiven Rechtsschutzes und damit der Verhältnismäßigkeit der gesetzlichen Ermächtigungen erforderlich sind.

Außerdem verstößt die Anwendung der §§ 94 ff. StPO auf den Zugriff und die Auswertung der sich auf beschlagnahmten Mobiltelefonen befindlichen Daten auch gegen die in dem Europäischen Gerichtshof in seiner Entscheidung „Bezirkshauptmannschaft Landeck“ vom 4. Oktober 2024 aufgestellten Anforderungen an eine hinreichend bestimmte und verhältnismäßige Ermächtigungsgrundlage.

Schließlich waren die Ermittlungsmaßnahmen auch im Einzelfall verfassungswidrig. Der Zugriff, die Sicherung und Übermittlung aller auf dem Mobiltelefon gespeicherten Daten war nicht erforderlich, da für den vermeintlichen Nachweis des Strafvorwurfs ausgereicht hätte, auf eine einzelne Sprachnotiz zuzugreifen. Auch waren die Ermittlungsmaßnahmen aufgrund des massiven Ungleichgewichts zwischen Eingriffsschwere und verfolgtem Zweck unangemessen.

Aus denselben Umständen ist der Beschwerdeführer durch die Beschlagnahme des Mobiltelefons mitsamt aller darauf gespeicherten Daten in seiner Eigentumsfreiheit aus Art. 14 Abs. 1 GG verletzt (siehe dazu **II.3.**). Zudem ist der Beschwerdeführer in seinem Grundrecht auf Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG (siehe dazu **II.4.**) sowie in seinem Grundrecht auf Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG (siehe dazu **II.5.**), jedenfalls in seinem Grundrecht auf allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG (siehe dazu **II.6.**) verletzt, da deren Bedeutung und Tragweite sowohl bei der Durchführung der Ermittlungsmaßnahmen als auch im Beschluss des Landgerichts Bamberg grundlegend verkannt wurde, insbesondere mit Blick auf das gewichtige Interesse des Beschwerdeführers, die polizeiliche Maßnahme zu dokumentieren. Schließlich stellen die gerichtliche Missachtung des zentralen Vortrags des

Beschwerdeführers und der Verzicht auch eine Vorlage an den Gerichtshof der Europäischen Union eine Verletzung der Art. 103 Abs. 1 GG bzw. Art. 101 Abs. 1 Satz 2 GG dar (siehe dazu **II.7.** und **II.8.**).

b. Eigene, gegenwärtige und unmittelbare Beschwer

Die Voraussetzung der eigenen, gegenwärtigen und unmittelbaren Beschwer sind bei Verfassungsbeschwerden gegen gerichtliche Entscheidungen in der Regel,

> BVerfGE 53, 30 (48); BVerfG Beschluss vom 15. Juli 2015 - 2 BvR 2292/13 -, BeckRS 2015, 51305 Rn. 56,

und so auch hier gegeben.

Insbesondere ergibt sich die Beschwer hier, wie erforderlich,

> BVerfGE 28, 151 (160); BVerfGE 74, 358 (374); BVerfGE 82, 106 (116),

aus dem beschwerenden Tenor der angegriffenen Entscheidung.

Zum Bestehen des Rechtsschutzbedürfnisses trotz Wegfall der ursprünglichen Beschwer wird sogleich ausgeführt (dazu unter **6.**).

4. Rechtswegerschöpfung

Dem Gebot der Rechtswegerschöpfung gem. § 90 Abs. 2 BVerfGG ist Genüge getan, denn gegen den Beschluss des Landgerichts ist ein weiterer Rechtsbehelf nicht gegeben. Insbesondere ist gem. § 310 Abs. 2 StPO keine weitere Beschwerde zulässig.

Eine Anhörungsrüge wurde am 10. Juli 2025 erhoben, diese ist aber noch nicht beschieden. Für den Fall, dass die Anhörungsrüge als offensichtlich unzulässig angesehen wird, wird hiermit vorsorglich zur Fristwahrung Verfassungsbeschwerde erhoben.

5. Subsidiarität

Auch dem Grundsatz der Subsidiarität ist entsprochen. Dieser erfordert, dass der Beschwerdeführer

> „*über die bloße formelle Erschöpfung des Rechtswegs hinaus vor Erhebung der Verfassungsbeschwerde grundsätzlich alle nach Lage der Dinge zur Verfügung stehenden prozessualen Möglichkeiten ergreifen, um die geltend gemachte Grundrechtsverletzung in dem unmittelbar mit ihr zusammenhängenden sachnächsten Verfahren zu verhindern oder zu beseitigen*“,
>
> BVerfGE 134, 242 (285); BVerfGE 129, 78 (92).

Nach der Rechtsprechung des Bundesverfassungsgerichts kann das auch bedeuten, dass

> „*Beschwerdeführer zur Wahrung des Subsidiaritätsgebots gehalten sind, im fachgerichtlichen Verfahren eine Gehörsverletzung mit den gegebenen Rechtsbehelfen, insbesondere mit einer Anhörungsrüge, selbst dann anzugreifen, wenn sie im Rahmen der ihnen insoweit zustehenden Dispositionsfreiheit mit der Verfassungsbeschwerde zwar keinen Verstoß gegen Art. 103 Abs. 1 GG rügen wollen* […]*, durch den fachgerichtlichen Rechtsbehelf aber die Möglichkeit wahren, dass bei Erfolg der Gehörsverletzungsrüge in den vor den Fachgerichten gegebenenfalls erneut durchzuführenden Verfahrensschritten auch andere Grundrechtsverletzungen, durch die sie sich beschwert fühlen, beseitigt werden*“,
>
> BVerfG, Beschluss vom 16. Juli 2013 - 1 BvR 3057/11 -, NJW 2013, 3506 Rn. 27; vgl. auch BVerfGE 126, 1, 17.

Allerdings müssen Beschwerdeführer

„*aus Gründen der Subsidiarität eine Anhörungsrüge oder den sonst gegen eine Gehörsverletzung gegebenen Rechtsbehelf nur dann ergreifen, wenn den Umständen nach ein Gehörsverstoß durch die Fachgerichte naheliegt und zu erwarten wäre, dass vernünftige Verfahrensbeteiligte mit Rücksicht auf die geltend gemachte Beschwer bereits im gerichtlichen Verfahren einen entsprechenden Rechtsbehelf ergreifen würden*“,

BVerfG, Beschluss vom 16. Juli 2013 - 1 BvR 3057/11 -, NJW 2013, 3506 (3508 Rn. 28).

Auch unter Zugrundelegung dieser Maßstäbe ist dem Grundsatz der Subsidiarität entsprochen, denn der Beschwerdeführer hat gegen den angegriffenen Beschluss am 10. Juli 2025 Anhörungsrüge gem. § 33a StGB eingelegt.

Andere Rechtsbehelfe oder sonstige Mittel, mit denen der Beschwerdeführer Abhilfe gegenüber der durch den Beschluss erfolgten Beschwer erreichen hätte können, stehen nicht zur Verfügung.

6. Rechtsschutzbedürfnis

Der Beschwerdeführer hat auch ein fortbestehendes Rechtsschutzbedürfnis. Dies gilt selbst dann, wenn sich die angegriffene strafprozessuale Maßnahme hier vollständig erledigt hätte und die Beschwer des Beschwerdeführers deswegen weggefallen wäre. Nach der Rechtsprechung des angerufenen Gerichts besteht nämlich auch im Falle der Erledigung des ursprünglichen klägerischen Begehrs ein Rechtsschutzinteresse an der verfassungsgerichtlichen Klärung,

„*wenn der Beschwerdeführer unter dem Gesichtspunkt der Wiederholungsgefahr ein anerkennenswertes Interesse an der Feststellung hat, dass die angegriffene Maßnahme nicht verfassungsgemäß war, wenn ein tiefgreifender und besonders schwerwiegender Grundrechtseingriff vorlag oder wenn anderenfalls die Klärung einer verfassungsrechtlichen Frage von grundsätzlicher Bedeutung unterbliebe und ein schwerwiegender Grundrechtseingriff gerügt wird*“,

Bundesverfassungsgericht, Nichtannahmebeschluss vom 3. November 2015 - 2 BvR 2019/09 -, Rn. 23.

Dieser Maßstab gilt nach der Rechtsprechung des angerufenen Gerichts auch für den Bereich erledigter strafprozessualer Zwangsmaßnahmen:

„*Lediglich in besonderen Fällen kann das Rechtsschutzbedürfnis trotz einer solchen Erledigung fortbestehen. Hierunter fallen neben einer weiterhin von der aufgehobenen oder gegenstandslos gewordenen Maßnahme ausgehenden Beeinträchtigung Fälle der Wiederholungsgefahr und von tiefgreifenden und folgenschweren, sich typischerweise schnell erledigenden Grundrechtseingriffen*“,

BVerfG, Nichtannahmebeschluss vom 12. Juli 2023 - 1 BvR 58/23 -, juris, Rn. 8.

Gemessen an diesem Maßstab liegt ein Rechtsschutzbedürfnis hier vor.

a. Tiefgreifender, sich typischerweise schnell erledigender Grundrechtseingriff

Bei der Entsperrung und vollständigen Auslesung eines Mobiltelefons handelt es sich zum einen um einen tiefgreifenden und folgenschweren, sich typischerweise schnell erledigenden Grundrechtseingriff.

Tiefgreifende und besonders schwerwiegende Grundrechtseingriffe sind insbesondere solche, die nach dem Grundgesetz unter Gerichtsvorbehalt stehen, wie etwa Art. 13 Abs. 2 GG oder nach Art. 104 Abs. 2, Abs. 3 GG,

BVerfG, Beschluss vom 03.11.2015 - 2 BvR 2019/09 -, BeckRS 2016, 40538 Rn. 31 m.w.N.

Bei dermaßen schwerwiegenden Grundrechtseingriffen bejaht das angerufene Gericht ein fortbestehendes Rechtsschutzbedürfnis insbesondere in Fällen, in denen sich die direkte Belastung durch den angegriffenen Hoheitsakt üblicherweise auf eine Zeitspanne beschränkt, in der regelmäßig keine Entscheidung des Bundesverfassungsgerichts erwirkt werden kann,

BVerfGE 81, 138 (140 f.); BVerfGE 110, 77 (86); BVerfGE 117, 71 (122 f.); BVerfGE 117, 244 (268).

Spezifisch bezogen auf die Beschlagnahme eines Mobiltelefons hat das angerufene Gericht bereits entschieden, dass es sich um einen tiefgreifenden Grundrechtseingriff handelt,

BVerfG, Beschluss vom 4. Februar 2005 - 2 BvR 308/04 -, juris, Rn. 18 ff.

Es hat dies insbesondere damit begründet, dass das Ausgangsgericht hätte erwägen müssen, ob die Beschlagnahme eines Mobiltelefons den Schutzbereich des Fernmeldegeheimnisses berühre, und damit, dass

„*der hohe Rang der Grundrechte aus Art. 10 Abs. 1 GG, die mit der Gewährleistung eines privaten, vor der Öffentlichkeit und der öffentlichen Gewalt verborgenen Austauschs von Nachrichten, Gedanken und Meinungen die Würde des denkenden und freiheitlich handelnden Menschen wahren (vgl. BVerfGE 67, 157 <171>; 100, 313 <358 f.>; Beschluss des Ersten Senats des Bundesverfassungsgerichts vom 3. März 2004 - 1 BvF 3/92 -, NJW 2004, S. 2213 <2215>), und der einfachgesetzliche Richtervorbehalt (§§ 100b Abs. 1, 100h Abs. 1 Satz 3, 100i Abs. 4 Satz 1 StPO) auf einen schwerwiegenden Eingriff hin*[deuten]*, so dass auch hier die Möglichkeit der nachträglichen Kontrolle offen stehen muss*“,

BVerfG Beschluss vom 4. Februar 2005 - 2 BvR 308/04 -, juris, Rn. 19.

Auch in Bezug auf im Rahmen von Durchsuchungen von Wohn- und Geschäftsräumen erfolgende Beschlagnahmeanordnungen hat das angerufene Gericht ein Rechtsschutzinteresse festgestellt. Zur Begründung führt das angerufene Gericht aus, dass

„*ein Rechtsschutzinteresse aber auch in Fällen tiefgreifender Grundrechtseingriffe gegeben* [ist]*, in denen die direkte Belastung durch den angegriffenen Hoheitsakt sich nach dem typischen Verfahrensablauf auf eine Zeitspanne beschränkt, in welcher der*

Betroffene die gerichtliche Entscheidung in der von der Prozeßordnung gegebenen Instanz kaum erlangen kann“,

BVerfG, Beschluss vom 15. Juli 1998 - 2 BvR 446–98 -, NJW 1999, 273.

Diese Einschätzungen gelten uneingeschränkt auch für den vorliegenden Fall, in dem mit § 98 Abs. 1 StPO ebenso ein Gerichtsvorbehalt besteht und die Eingriffstiefe – nicht zuletzt wegen des in der Zwischenzeit aufgetretenen technischen Fortschritts – freilich als noch um einiges größer zu bewerten ist.

Im vorliegenden Fall fällt erschwerend auch der Eingriff in die Pressefreiheit ins Gewicht,

so auch BVerfGE 117, 244 (269).

Außerdem handelt es sich auch bei Beschlagnahmeanordnungen um Maßnahmen, die ihrer Natur nach häufig vor möglicher gerichtlicher Überprüfung schon wieder beendet sind,

BVerfGE 117, 244 (269),

sodass auch in Bezug auf die Rechtsschutzmöglichkeiten die Anforderungen des angerufenen Gerichts erfüllt sind.

Schließlich ist der Umfang des Datenzugriffs in entsprechenden Fällen regelmäßig erst im Nachhinein erkennbar. Dies veranschaulicht auch der vorliegende Fall, in dem der Beschwerdeführer erstmalig mit Akteneinsicht am 19. April 2024 – und damit mehr als ein halbes Jahr nach der Beschlagnahme – Kenntnis von der Art und dem Umfang des Datenzugriffs und der Auswertung erlangt hat. Insofern ist das Vorgehen gegen die Auswertung von Mobiltelefonen auch typischerweise erst nach Ausführung der Maßnahme möglich.

Würde dies anders bewertet, wären Maßnahmen der Beschlagnahme, Auslesung und Auswertung von Mobiltelefonen im Übrigen regelmäßig der verfassungsgerichtlichen Überprüfung entzogen. Weiterhin handelt es sich bei den hier aufgeworfenen Problemen auch um

verfassungsrechtliche Fragen von grundsätzlicher Bedeutung (dazu unter **8.**), sodass auch diesem Erfordernis genügt ist.

b. Wiederholungsgefahr

Zum anderen besteht auch eine das Rechtsschutzinteresse begründende Wiederholungsgefahr. Es ist mit hinreichender Wahrscheinlichkeit davon auszugehen, dass der Beschwerdeführer auch in Zukunft ähnliche Maßnahmen gegen sein Mobiltelefon oder andere Speichermedien erleiden wird,

> für vergleichbare Fälle, in denen eine Wiederholungsgefahr angenommen wurde, siehe BVerfGE 103, 44 (59); 119, 309 (317 f.); 116, 69 (79).

Es handelt sich bei der auf §§ 94 ff. StPO gestützten Beschlagnahme, Auslesung und Auswertung von Mobiltelefonen um Standardmaßnahmen, denen sich insbesondere Bürger*innen, die häufig an Demonstrationen teilnehmen und deswegen regelmäßig in engen, teils auch konfrontativen, Kontakt mit der Polizei kommen, regelmäßig aussetzen. Für Personen wie den Beschwerdeführer, die politische Demonstrationen auch journalistisch begleiten, ist diese Gefahr sogar noch gesteigert, da sie im Zweifel darauf angewiesen sind, polizeiliches Verhalten mit einem Mobiltelefon oder anderen Geräten zu dokumentieren und sich dadurch (unberechtigterweise) dem Vorwurf deliktischen Verhaltens beispielsweise nach § 201 StGB oder § 201a StGB aussetzen können. Da der Beschwerdeführer auch in Zukunft politische Aufzüge begleiten will, und auch vorhat, polizeiliche Aktivitäten hier mit entsprechenden Aufnahmegeräten zu dokumentieren, besteht für ihn die konkrete Gefahr, dass gegen ihn in Zukunft ähnliche Maßnahmen getroffen werden.

c. Ungeklärte verfassungsrechtliche Frage von grundsätzlicher Bedeutung

Weiterhin handelt es sich um die hier aufgeworfenen Probleme auch um verfassungsrechtliche Fragen von grundsätzlicher Bedeutung, sodass auch diesem Erfordernis genügt ist,

> zur grundsätzlichen verfassungsrechtlichen Bedeutung siehe BVerfGE 69, 315 (341); 103, 44.

Insbesondere ist umstritten und verfassungsgerichtlich ungeklärt, in welche Grundrechte die Beschlagnahme eines Mobiltelefons eingreift und welche verfassungsrechtlichen Anforderungen an eine solche Maßnahme zu stellen sind. Seit der Entscheidung des Bundesgerichtshofs,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876,

besteht zwar höchstgerichtliche Rechtsprechung, die aber sowohl die Anforderungen des angerufenen Gerichts als auch die des Europäischen Gerichtshofs außer Acht lässt und leistet damit den verfassungsrechtlich zu fordernden Anforderungen nicht hinreichend Gewähr (siehe dazu auch **C.II.1.c.cc.(e)**). Zudem ist nach wie vor verfassungsgerichtlich ungeklärt, ob § 201 Abs. 1 StGB aufgrund verfassungsrechtlicher Vorgaben einschränkend auszulegen ist. Beide Fragen sind von grundsätzlicher Bedeutung, da es in der Praxis häufig zu Maßnahmen wie der gegenüber dem Beschwerdeführer kommt.

7. Frist

Die Erhebung der Verfassungsbeschwerde erfolgt fristgerecht. Gem. § 93 Abs. 1 Satz 1 BVerfGG ist die Verfassungsbeschwerde binnen eines Monats zu erheben und zu begründen. Gem. § 93 Abs. 1 Satz 2 BVerfGG beginnt die Frist mit der Zustellung oder formlosen Mitteilung der in vollständiger Form abgefassten Entscheidung, wenn diese nach den maßgebenden verfahrensrechtlichen Vorschriften von Amts wegen vorzunehmen ist.

Der ohne mündliche Verhandlung ergangene Beschluss des Landgerichts Bamberg vom 27. Juni 2025 - ... - ist der Bevollmächtigten am ... Juni 2025 zugegangen,

Eingangsstempel über beA vom ... Juni 2025 (**Anlage 9**).

Dem Beschwerdeführer selbst wurde der Beschluss nicht zugestellt.

Gegen diesen Beschluss hat der Beschwerdeführer am 10. Juli 2025 Anhörungsrüge eingelegt. Für den Fall, dass die Anhörungsrüge für unzulässig erachtet wird und die Monatsfrist des § 93 Abs. 1 BVerfGG, die mit der Zustellung an die Bevollmächtigte am ... Juni 2025 gem.

§ 93 Abs. 1 BVerfGG i.V.m. § 222 ZPO i.V.m. § 187 Abs. 1 BGB am 1. Juli 2025 beginnt und gem. § 93 Abs. 1 BVerfGG i.V.m. § 222 ZPO i.V.m. § 188 Abs. 2 Fall 2 BGB mit Ablauf des ... Juli 2025 endet, wird diese Frist mit der heutigen, am 29. Juli 2025 erhobenen Beschwerde gewahrt.

8. Annahmevoraussetzungen

Die Verfassungsbeschwerde ist gem. § 93a BVerfGG zur Entscheidung anzunehmen.
Der Verfassungsbeschwerde kommt zum einen grundsätzliche verfassungsrechtliche Bedeutung zu, § 93a Abs. 2 lit. a BVerfGG. Grundsätzliche verfassungsrechtliche Bedeutung hat eine Verfassungsbeschwerde, wenn sie

> „*eine verfassungsrechtliche Frage aufwirft, die sich nicht ohne weiteres aus dem Grundgesetz beantworten läßt und noch nicht durch die verfassungsgerichtliche Rechtsprechung geklärt oder die durch veränderte Verhältnisse erneut klärungsbedürftig geworden ist*“,
>
> BVerfGE 96, 245 (248).

Diesem Maßstab ist hier entsprochen: Bei der auf die §§ 94 ff. StPO gestützten Beschlagnahme, dem technischen Zugriff auf und der informationstechnischen Auswertung von Mobiltelefonen und anderen Datenträgern handelt es sich um äußerst grundrechtsintensive Ermittlungsmaßnahmen, die heute zum Standardrepertoire polizeilicher Ermittlungsaktivitäten zählen. Es handelt sich mithin um Maßnahmen, die jedes Jahr in tausenden von Fällen zu Eingriffen in die Grundrechte betroffener Bürger*innen führen,

> vgl. *Pitz*, Beschlagnahmte Smartphones, Ein Grundrechtseingriff unbekannten Ausmaßes vom 30. Oktober 2023, netzpolitik.org, abrufbar unter: https://netzpolitik.org/2023/beschlagnahmte-smartphones-ein-grundrechtseingriff-unbekannten-ausmasses/ (Letzter Abruf: 18 Juli 2025).

Die Entscheidung hat danach also schon erhebliche quantitative Bedeutung. Es handelt sich aber auch um einen qualitativ besonders intensiven, und deshalb bedeutsamen Eingriff. Die

Schwere des Eingriffs wird dabei nicht zuletzt dadurch bestimmt, dass der Zugang zu einem Mobiltelefon heutzutage nahezu unbeschränkte Einblicke in alle Lebensbereiche des Betroffenen ermöglicht und damit den Behörden auch besonders sensible Informationen preisgibt. Aufgrund der niedrigen Eingriffsschwelle und fehlenden bzw. unzureichenden gesetzlichen Schutzvorkehrungen und Verfahrensvorschriften besteht auch ein hohes Missbrauchsrisiko. Beispielhaft sei nur auf den hier vorliegenden Fall verwiesen, in dem die Beschlagnahme und der Zugriff auf ein Mobiltelefon zum Zwecke der Kenntnisnahme einer einzigen Sprachnachricht letztlich zur Erstellung eines umfangreichen politischen Profils des Betroffenen anhand unterschiedlichster auf dem Mobiltelefon vorfindlicher Datenbestände führte.

Die Verfassungsbeschwerde ist außerdem zur Durchsetzung der in § 90 Abs. 1 BVerfGG genannten Rechte des Beschwerdeführers angezeigt, § 93a Abs. 2 lit. b BVerfGG. Nach diesem Maßstab ist eine Beschwerde zur Entscheidung anzunehmen, wenn die geltend gemachte Verletzung von Grundrechten oder grundrechtsgleichen Rechten entweder besonderes Gewicht hat oder aber den Beschwerdeführer in existenzieller Weise betrifft,

> BVerfGE 107, 395 (415).

Jedenfalls ersteres ist hier gegeben. Besonders gewichtig ist eine Grundrechtsverletzung nach der Rechtsprechung des angerufenen Gerichts insbesondere dann, wenn sie

> „*auf eine generelle Vernachlässigung von Grundrechten hindeutet oder wegen ihrer Wirkung geeignet ist, von der Ausübung von Grundrechten abzuhalten. Eine geltend gemachte Verletzung hat ferner dann besonderes Gewicht, wenn sie auf einer groben Verkennung des durch ein Grundrecht gewährten Schutzes oder einem geradezu leichtfertigen Umgang mit grundrechtlich geschützten Positionen beruht oder rechtsstaatliche Grundsätze kraß verletzt*“,
>
> BVerfGE 90, 22 (25).

Diesen Maßstäben ist hier entsprochen. Dafür ist zunächst darauf hinzuweisen, dass es sich, wie bereits dargelegt, um eine besonders gewichtige Grundrechtsverletzung handelt. Dafür spricht zum einen, dass es sich um besonders schwerwiegende Eingriffe handelt, die in der

polizeilichen Praxis auch keine „Ausreißer“ darstellen, sondern vielmehr eine generelle Vernachlässigung der Grundrechte erkennen lassen. Im Rahmen von auf §§ 94 ff. StPO gestützten Mobiltelefon-Zugriffen wird regelmäßig auf privateste und sensibelste Datenbestände zugegriffen, ohne dass die daran beteiligten staatlichen Akteure eine geordnete Berücksichtigung und Abwägung verfassungsrechtlicher Belange im Allgemeinen und grundrechtlicher Belange im Spezifischen vornehmen würden. Es handelt sich mithin um eine ständige Praxis, durch die in ähnlichen anderen Bereichen geltende verfassungsrechtliche Maßstäbe systematisch unbeachtet bleiben. Außerdem handelt es sich um eine Grundrechtsverletzung, die geeignet ist, von der Ausübung von Grundrechten abzuhalten. Tatsächlich wird Teilnehmenden insbesondere von politischen Demonstrationen heutzutage regelmäßig geraten, Mobiltelefone überhaupt nicht auf Veranstaltungen mitzunehmen, um keine Beschlagnahme und Auswertung durch die Polizei zu riskieren. Es handelt sich dabei auch nicht um unbegründete Warnungen oder Alarmismus. Dadurch kommt es aber zu einem sog. „chilling effect“ und Bürger*innen werden davon abgehalten, von ihren Grundrechten legitimen Gebrauch zu machen, etwa auf politischen Aufzügen miteinander zu kommunizieren oder diese – auch aus journalistischen Motiven heraus – zu dokumentieren.

II. Begründetheit

Die Verfassungsbeschwerde ist begründet, weil der Beschluss des Landgerichts Bamberg vom 27. Juni 2025 - ... - den Beschwerdeführer in seinem allgemeinen Persönlichkeitsrecht in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (dazu unter **1.**), jedenfalls in seinem Recht auf informationelle Selbstbestimmung (dazu unter **2.**) sowie in seinem Recht auf Eigentumsfreiheit aus Art. 14 Abs. 1 Satz 1 GG (dazu unter **3.**), seinem Recht auf Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG (dazu unter **4.**), seinem Recht auf Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG (dazu unter **5.**), jedenfalls in seinem Recht auf allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG (dazu unter **6.**), seinem Recht rechtliches Gehör aus Art. 103 Abs. 1 GG (dazu unter **7.**) und seinem Recht auf den*die gesetzliche*n Richter*in aus Art. 101 Abs. 1 Satz 2 GG verletzt (dazu unter **8.**).

1. Verletzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Der Beschluss des Landgerichts Bamberg greift in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme des Beschwerdeführers aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein, ohne dass dies verfassungsrechtlich gerechtfertigt werden könnte.

a. Eröffnung des Schutzbereiches

Der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist eröffnet. Es ist seit der Leitentscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts anerkannt. Es ist als Maßstab anzuwenden, wenn

> „*die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können*“,
>
> BVerfGE 120, 274 (314).

Die Teilgewährleistung der Vertraulichkeit schützt

„*das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben*“,

BVerfGE 120, 274 (314).

Die Integrität eines informationstechnischen Systems wird angetastet,

„*indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen*“,

BVerfGE 120, 274 (314).

Damit wird es der lückenfüllenden Funktion des allgemeinen Persönlichkeitsrechts gerecht, denn das Recht auf informationelle Selbstbestimmung trägt

„*den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht* ***in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen****, vor denen das Recht auf informationelle Selbstbestimmung schützt,* ***weit hinaus***“ [Hervorhebungen durch Unterzeichnerin],

BVerfGE 120, 274 (312 f.).

Auch tritt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

> „*zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren*“,
>
> BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, - 1 BvR 595/07 -, NJW 2008, 822 (824 Rn. 168).

Aus der Rechtsprechung des angerufenen Gerichts ergibt sich, dass sich der Schutzbereich auch auf Maßnahmen erstreckt, die einen offenen Datenzugriff vorsehen, soweit sie im selben Umfang Einblicke in die Persönlichkeit ermöglichen. Eine Begrenzung auf heimliche Zugriffe besteht nicht. Diese sind zwar „*insbesondere*“, aber nicht ausschließlich erfasst,

> BVerfGE 120, 274 (314).

Vielmehr liegt der Anknüpfungspunkt für die besondere Schutzbedürftigkeit in der fehlenden Abwehrmöglichkeit durch die betroffene Person:

> „*Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe* ***zum Teil*** *gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann*“ [Hervorhebung durch Unterzeichnerin],
>
> BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 180.

Der Datenzugriff auf Mobiltelefone betrifft die Integrität informationstechnischer Systeme, insbesondere wenn für die Entsperrung und Auswertung eine forensische Auswertungssoftware, z.B. wie vorliegend von Cellebrite, auf das Gerät gespielt wird und dadurch u.a.

Sicherheitslücken ausgenutzt, Systemeinstellungen verändert und das Risiko einer Manipulation des Datenbestandes begründet werden,

> siehe zu den technischen Details *Schlüter/Besendorf*, RSF Digital Security Lab, Forensische Analyse … (**Anlage 5**).

Gerade solche Gefahren werden vom grundrechtlichen Schutz der Integrität informationstechnischer Systeme abgedeckt,

> vgl. BVerfGE 120, 274 (314); *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2009, 1009 (1012); *Böckenförde*, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, 925 (928); *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 141 f.; ausführlich *Kubicek*, in: Klumpp/Kubicek/Roßnagel/Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, 2009, S. 17 (23 ff.); zur Entsperrung eines Smartphones nach § 81b Abs. 1 StPO auch *Mansouri/Rückert*, Touch me if you can – Die Zulässigkeit der zwangsweisen Entsperrung eines Mobiltelefons mittels Fingerabdrucks, JR 2025; aop, S. 4, abrufbar unter: https://doi.org/10.1515/juru-2025-2064 (Letzter Abruf: 18. Juli 2025) sowie *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 489.

Gleichzeitig ist die Vertraulichkeit berührt, da durch einen offenen Datenzugriff gegen den Willen des Betroffenen in sein Interesse eingegriffen wird, dass die auf seinem Datenträger erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.

Insofern macht es keinen Unterschied, ob der Staat durch eine Online-Durchsuchung oder durch die physische Beschlagnahme eines komplexen IT-Geräts Einblicke in wesentliche Teile der Lebensgestaltung einer Person gewinnt und damit erheblich tiefer in die Persönlichkeitsrechte der Betroffenen eingreift als durch einen Zugriff auf Einzeldaten,

> für die Erstreckung des Schutzbereichs auf Datenzugriffe bei beschlagnahmten Datenträgern auch OLG Bremen, Beschluss vom 8. Januar 2025 - 1 ORs 26/24 -, juris, Rn. 13; LG Ravensburg, Beschluss vom 14. Februar 2023 - 2 Qs 9/23 -, NStZ 2023, 446 (447 Rn. 17); *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme,

2015, S. 167; *Hornung*, Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, CR 2008, 299 (303); *Michalke*, Strafrechtlicher Zugriff auf elektronische Medien, StraFo 2008, 287 (291); *Polenz*, in: Kilian/Heussen, Computerrechts-Handbuch, EL 29, Februar 2011, Teil 13 Rn. 32; *Bäumerich*, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung, NJW 2017, 2718 (2722).

Sofern frühere Entscheidungen des angerufenen Gerichts den Datenzugriff auf beschlagnahmten Datenträgern allein am Grundrecht auf informationelle Selbstbestimmung gemessen haben,

vgl. BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1918 ff.); BVerfG, Urteil vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, 976 (979, Rn. 82 ff.); BVerfG, Beschluss vom 25. Juli 2007 - 2 BvR 2282/06 -, NJW 2007, 3343 (3334),

ist dem seit der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung im Jahr 2008 nicht mehr zu folgen.

Der vom Bundesverfassungsgericht in dieser Entscheidung identifizierte besondere verfassungsrechtliche Schutzbedarf hat sich seither nur noch intensiviert. Technische Geräte wie Mobiltelefone verfügten damals über einen im Vergleich zu heute stark eingeschränkten Funktionsumfang. Insbesondere haben sich mit der technischen Weiterentwicklung und der breiten Verfügbarkeit von Smartphones auch Nutzungsverhalten und -gewohnheiten stark verändert. Hinzu kommen die weitreichende Vernetzungsmöglichkeiten von Daten über eine Vielzahl von digitalen Endgeräten hinweg sowie die Auslagerung der Datenspeicherung in externen Clouds. Auch Art und Umfang der in vor fast 20 Jahren hergestellten Mobiltelefonen gespeicherten Daten unterscheiden sich erheblich von den vielfältigen und sensiblen Informationen, die moderne Smartphones enthalten. Von den oben zitierten Entscheidungen des angerufenen Gerichts betraf lediglich die Entscheidung des Bundesverfassungsgerichts vom 2. März 2006,

BVerfG, Urteil vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, 976 (979 Rn. 82 ff.),

die Beschlagnahme eines Mobiltelefons. Die den damaligen Entscheidungen zugrunde liegende Gefahrenlage für das allgemeine Persönlichkeitsrecht ist jedoch nicht mit der heutigen Situation vergleichbar, in der ein Zugriff auf den gesamten Datenbestand eines Smartphones weit tiefergehende Einblicke ermöglicht.

Die zwei späteren Entscheidungen, in denen sich das Bundesverfassungsgericht mit dem Datenzugriff und der Auswertung im Rahmen des §§ 94 ff. StPO beschäftigt hat, betrafen keine komplexen IT-Geräte, sondern lediglich beschlagnahmte (geschäftliche) E-Mails der Betroffenen. Konkret für diese Fallkonstellation hat das Gericht entschieden, dass der Eingriff allein am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art 10 Abs. 1 GG und nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen sei, da Ersteres einen ausreichenden Schutz gewährleiste,

> BVerfG, Urteil vom 16. Juni 2009 - 2 BvR 902/06 -, NJW 2009, 2431 (2432 Rn. 51); bestätigt in BVerfG Beschluss vom 15. August 2014 - 2 BvR 969/14 -, NJW 2014, 3085.

Soweit sein Schutzbereich eröffnet ist, verdrängt in diesen Fällen das Grundrecht auf Gewährleistung des Fernmeldegeheimnisses damit als spezielleres Grundrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Diese Bewertung lässt sich nicht auf den Zugriff und die Auswertung komplexer IT-Systeme – insbesondere von Smartphones – übertragen, da in diesen Fällen bereits abgespeicherte Daten betroffen sind, die nicht mehr der laufenden Kommunikation zuzuordnen sind und damit aus dem Schutzbereich des Fernmeldegeheimnisses herausfallen. Auch geht deren Informationsgehalt sowie die Vielfalt und Tiefe der gespeicherten Daten – etwa Fotos, Bewegungsprofile, Gesundheitsdaten, private Kommunikation und Apps mit sensiblen Inhalten – weit über den Umfang und die Sensibilität von E-Mails hinaus, insbesondere wenn es sich dabei lediglich um geschäftliche Kommunikation handelt. Insofern unterscheidet sich der hier vorliegende Fall sowohl hinsichtlich seiner Eingriffsrichtung und -intensität als auch im Hinblick auf das damit verbundene Gefahrenpotenzial grundlegend von den damals entschiedenen Konstellationen.

b. Eingriff

Bereits die Entsperrung eines beschlagnahmten Mobiltelefons stellt einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar, da dadurch die Integrität des Datenträgers beeinträchtigt und der Zugriff auf den gesamten Datenbestand ermöglicht und mithin die Gefahr unbefugter oder missbräuchlicher Verwendung der Daten begründet wird,

> so auch OLG Bremen, Beschluss vom 8. Januar 2025 - 1 ORs 26/24 -, juris, Rn. 13; vgl. auch die Rspr. im Verwaltungsrecht: für den Datenzugriff auf nach § 48 Abs. 3 AufenthG sichergestellte Datenträger so auch VGH Mannheim, Beschluss vom 23. November 2022 - 12 S 3213/21 -, BeckRS 2022, 36497 Rn. 20; VG Karlsruhe, Beschluss vom 9. August 2023 - A 19 K 1797/23 -, BeckRS 2023, 20923 Rn. 22; VG Karlsruhe, Urteil vom 11. Dezember 2024 - 10 K 4631/23 -, BeckRS 2024, 44454 Rn. 52 f., 82; VG Berlin, Urteil vom 1. Juni 2021 - VG 9 K 135/20 A -, ZD 2021, 718 (719 Rn. 24).

Dem anschließenden Datenzugriff, der Extraktion des gesamten Rohdatenbestandes, dessen (Zwischen-)Speicherung sowie dessen Übermittlung an eine andere behördliche Stelle zwecks inhaltlicher Auswertung kommt jeweils eigenständige Eingriffsqualität zu.

Ausweislich der Akte hat ein Sachbearbeiter des technischen Ergänzungsdiensts Bamberg in einem Zeitraum vor dem ... Dezember 2023 die Entsperrung des Mobiltelefons sowie eine Extraktion und Sicherung des gesamten Datenbestandes auf behördeneigenen Datenträgern mit einer forensischen Software des Herstellers Cellebrite durchgeführt,

> siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 ff. (**Anlage 3**).

Die gesicherten Daten wurden anschließend am … Dezember 2025 vollständig einem Kriminalhauptmeister der Kriminalpolizeiinspektion Bamberg zur inhaltlichen Auswertung der Daten übermittelt,

> siehe Ermittlungsbericht vom 18. Dezember 2023, Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 55 (**Anlage 3**),

und dürften dort am selben Tag auch nochmal auf einem eigenen Datenträger gespeichert worden sein. Damit wurde sowohl durch den Datenzugang auf das Mobiltelefon als auch durch die Datenauslesung und -sicherung sowie durch die Übermittlung der Daten an die Kriminalpolizeiinspektion Bamberg und der anschließenden Speicherung jeweils eigenständig in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme des Beschwerdeführers eingegriffen.

c. Verfassungsrechtliche Rechtfertigung

Die mit dem Datenzugang und dem anschließenden Zugriff, der Speicherung und Übermittlung der Daten einhergehenden Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind verfassungsrechtlich nicht zu rechtfertigen. Zwar kann das Grundrecht zur Strafverfolgung eingeschränkt werden (dazu unter **aa.**), doch handelt es sich um Eingriffe mit einer besonders hohen Intensität (dazu unter **bb.**), für deren Rechtfertigung es an einer spezifischen, hinreichend bestimmten Ermächtigungsgrundlage fehlt (dazu unter **cc.(1)**), die auch unionsrechtlichen Maßstäben genügen (dazu unter **cc.(2)**) und Vorkehrungen für den Kernbereichsschutz (dazu unter **cc.(3)**) sowie ausreichende Vorgaben für die Wahrung der Verhältnismäßigkeit vorsehen muss (dazu unter **cc.(4)**). Diesen Anforderungen genügen die §§ 94 ff. StPO nicht.

aa. Schranke

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird entsprechend seiner Herleitung aus dem allgemeinen Persönlichkeitsrecht nicht schrankenlos gewährleistet, sondern kann u.a. zur Strafverfolgung eingeschränkt werden, soweit die Beschränkung auf einer verfassungsmäßigen gesetzlichen Grundlage beruht,

> BVerfGE 120, 274 (315).

bb. Besonders hohe Eingriffsintensität

Der auf die §§ 94 ff. StPO gestützte Zugriff auf den gesamten Datenbestand beschlagnahmter komplexer IT-Geräte – insbesondere eines Smartphones – und die anschließende

Datenauswertung und -speicherung stellen Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme mit einer besonders hohen Intensität dar.

(1) Gefahren der technischen Ausführung

Durch spezielle Software, z.B. von Cellebrite, lassen die Strafermittlungsbehörden Mobiltelefone entsperren und haben dadurch Zugriff auf den gesamten Datenbestand, den sie anschließend auslesen und auswerten können. Darüber hinaus können durch Ausnutzung von Sicherheitslücken Verschlüsselungen umgangen und der Zugriff auf den Root-Benutzer des Android-Systems erlangt werden. Das führt dazu, dass die Behörden durch das Erlangen von Administrator*innenrechten einen umfassenden Zugriff auf die Daten bekommen und erweiterte Download-Befugnisse erwerben, z.B. um ein Backup von verschlüsselten Messenger-Diensten wie Signal anfertigen zu können. Auch können dauerhafte Spuren auf einem Mobiltelefon hinterlassen werden wie Tombstone-Dateien, d.h. Dateien, die Betriebssysteme von Android anlegen, wenn Prozesse abstürzen, und geänderte Einstellungen im Betriebssystem und das Gerät in einen deutlich anderen Zustand versetzen als vor der Auswertung. Dies erhöht die Manipulationsgefahr und eröffnet die technische Möglichkeit, Hintertüren zu eröffnen. Sollte beispielsweise eine Schadsoftware das Telefon angreifen, wäre es schwierig bis unmöglich zu erkennen, ob bestimmte Spuren durch die Auswertung mit Cellebrite entstanden sind oder von der Schadsoftware stammen,

> siehe hierzu sowie zu weiteren technischen Gefahren *Schlüter/Besendorf*, RSF Digital Security Lab, Forensische Analyse … (**Anlage 5**); vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 201.

Der Datenzugriff beeinträchtigt damit die Manipulationssicherheit und die Integrität des Systems, auf das zugegriffen wird, erheblich. Durch die Erlangung von Root-Rechten, die zur Erstellung eines Dateisystem-Abbilds durch die Forensiksoftware zwingend notwendig sind, verlieren gleichzeitig alle Sicherheitsmechanismen ihre Wirksamkeit, die den Datenspeicher des Smartphones vor Veränderung und Manipulation schützen. Dies hat zur Folge, dass alle Dateien auf dem System gelesen und verändert sowie Veränderungen von Dateien auch verschleiert werden können, was eine hohe Manipulationsgefahr begründet. Darüber hinaus sind aufwändig

durchgeführt und technisch gut kaschierte Veränderungen für die betroffen Person kaum oder gar nicht erkennbar und eine eindeutige Aufklärung durch eine unabhängige Untersuchung im Nachhinein praktisch nicht möglich. Schließlich kann es dazu kommen, dass mit der Nutzung der Forensiksoftware frühere Angriffe auf das Gerät verschleiert werden, da dabei ähnliche Spuren wie bei Spähsoftware hinterlassen werden. Dies erschwert es, bei einer späteren Analyse des Mobiltelefons frühere Eingriffe eindeutig nachzuvollziehen oder voneinander zu unterscheiden,

> für weitere Ausführungen siehe *Schlüter/Besendorf*, RSF Digital Security Lab, Technische Einschätzungen zu verschlüsselungsbrechender Mobilforensik-Software (**Anlage 10**).

Daher lässt sich in vielen Fällen eine Manipulation – sei es bewusst oder unbeabsichtigt – nicht ausschließen. Es kann selten mit Sicherheit nachgewiesen werden, dass die erhobenen Daten nicht von einer dritten Person erzeugt wurden,

> *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 200 f., 665 m.w.N.

(2) Umfang und Vielfalt der Daten

Wenn ein Datenträger durch eine Zugangssperre geschützt ist, kann nur das Gerät als Ganzes beschlagnahmt werden – und damit auch der gesamte Datenbestand. Nach der Entsperrung von Mobiltelefonen werden in der Praxis alle auf dem Gerät befindlichen Daten ausgelesen und gesichert. Das erstellte forensische Duplikat stellt ein genaues Abbild des Originals dar, das alle Datenspuren mitumfasst. Darüber hinaus erstellen die Strafverfolgungsbehörden meistens eine „Arbeitsversion“ der Daten für den jederzeitigen Zugriff durch den zuständigen Ermittler sowie eine „Sicherungskopie“ beim IT-Referenten,

> *Basar/Hiéramente*, Datenbeschlagnahme in Wirtschaftsstrafverfahren und die Frage der Datenlöschung, NStZ 2018, 681 (682 m.w.N.).

Aufgrund der Vielzahl und Art der auf komplexen IT-Systemen wie Smartphones gespeicherten Daten, die erhebliche Rückschlüsse auf das Leben der Betroffenen zulassen und die Erstellung von einem umfassenden Verhaltens- und Persönlichkeitsprofil ermöglichen, liegt ein Eingriff mit einer besonders hohen Intensität vor, dessen Eingriffscharakter mit der von verdeckten Überwachungsmaßnahmen wie die Telekommunikationsüberwachung nach § 100a StPO und der Online-Durchsuchung nach § 100b StPO vergleichbar ist,

> so auch *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 57, 64 ff.; *Greco*, Ermittlungsziel: Smartphone, StV 2024, 276 (280); *Mansouri/Rückert*, Touch me if you can – Die Zulässigkeit der, zwangsweisen Entsperrung eines Mobiltelefons mittels Fingerabdrucks, JR 2025, aop, S. 4, abrufbar unter: https://doi.org/10.1515/juru-2025-2064 (Letzter Abruf: 18. Juli 2025).

Die Strafverfolgungsbehörden erhalten Zugriff auf einen immensen Datenbestand, welchen sie sowohl automatisiert als auch durch Lesen der einzelnen auf dem Datenträger gespeicherten Informationen auswerten können. Insbesondere Smartphones verbinden große Mengen persönlicher Daten aus fast allen Lebensbereichen und enthalten gewissermaßen den gesamten digitalen Hausstand: Nachrichten an Familienmitglieder und Partner*innen, Kontaktdaten, inklusive Informationen über Anwält*innenkontakte, Konto- und Zahlungsdaten, Zugang zu Email-Accounts, die Suchmaschinen-Historie, der Browserverlauf, Kalender mit Terminen, Aufenthaltsdaten, intime und persönliche Fotos aus allen Lebensbereichen, Informationen zu Tagesabläufen und Gewohnheiten, Gesundheitszustand, sexueller Orientierung und politischer Überzeugung. Fotos, Videos, Textnachrichten und sonstige gespeicherte Aufzeichnungen geben im Zusammenspiel dem Smartphone regelmäßig die Funktion eines Tagebuchs. Aus Smartphone-Daten lassen sich Kommunikations-, Verhaltens- und Bewegungsprofile sowie soziale Netzwerke ableiten; sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen,

> *Boonstra/Larsen/Christensen*, Mapping dynamic social networks in real life using participants' own smartphones, 2015, abrufbar unter: https://www.cell.com/action/showPdf?pii=S2405-8440%2815%2930056-6; *Stachl/Hilbert/Au/Buschek/De Luca/Bischl/Hussmann/Bühner*, Personality Traits Predict Smartphone Usage. Eur. J. Pers., 31: 701 – 722, 2017, abrufbar unter:

https://www.researchgate.net/publication/318879569_Personality_Traits_Predict_Smartphone_Usage (Letzter Abruf: 18. Juli 2025).

Weiter ist zu berücksichtigen, dass die Informationen weit in die Vergangenheit reichen und neben persönlichen auch berufliche Informationen enthalten können. Letztere können sensible und geheimhaltungsbedürftige Daten umfassen, wie etwa Kommunikationsinhalte mit journalistischen Quellen, Mandant*innen, Patient*innen, vertrauliche Forschungsdaten oder sensible Gesundheitsinformationen. Auch ermöglicht es moderne KI-Analysesoftware, bestehende Datenbestände mit neu erlangten Daten automatisiert zu verknüpfen und abzugleichen, was wiederum umfassende und detaillierte Einblicke erlaubt, die ansonsten so nicht zugänglich wären und zur weiteren Vervollständigung des Persönlichkeitsbildes einer Person beitragen,

Cornelius, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 Rn. 1 m.w.N; *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 2023, 1070 (1074); zu den Gefahren einer automatisierten Datenanalyse und -verknüpfung in Bezug auf Palantir vgl. BVerfG, Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, NJW 2023, 1196 (1201).

Auch die Aussagekraft von Telekommunikationsverbindungsdaten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten gewinnen. Dabei können sich auch Rückschlüsse über politische Aktivitäten oder das individuelle Dating-Verhalten ergeben.

Der Eingriff wird dadurch vertieft, dass auf jegliche Art von Datenträgern und Daten zugegriffen und die darauf befindlichen Daten anschließend ausgewertet werden können. Neben Smartphones kann sich auch Zugriff auf Laptops und Tablets verschafft werden sowie auf extern abgelegte Daten, die vom beschlagnahmten Gerät aus erreichbar sind – zum Beispiel der Zugriff auf Cloud-Speicher oder Social Media-Accounts,

Hartmann, in: HK-GS, 5. Auflage 2022, StPO § 110 Rn. 5; *Gerhold*, in: BeckOK StPO mit RiStBV und MiStra, Graf, 54. Edition, Stand: 1. Januar 2025, § 94 Rn. 3 f. m.w.N.

In Anbetracht der immer weiter zunehmenden cloudbasierten Nutzung von Diensten und der automatisierten Synchronisation verschiedener Endgeräte finden sich auch auf anderen Datenträgern wie Laptops oder Tablets eine immense Menge und Vielfalt an höchstsensiblen Daten,

> *Hiéramente*, Umgang mit Smartphones im Strafprozess: Überlegungen zu den Reformideen des 74. Deutschen Juristentags 2024, StV 2024, 611 (614).

(3) Erhebliche Streubreite und weitreichende Zugriffsmöglichkeit

Der Eingriff hat zudem eine erhebliche Streubreite. Es können zunächst alle Personen als direktes Ziel der Maßnahme betroffen sein, gegen die ein einfacher Anfangsverdacht gem. § 152 Abs. 2 StPO vorliegt, unabhängig von der Schwere der jeweiligen Straftat – selbst Ordnungswidrigkeiten sind betroffen, vgl. § 46 OWiG – und sofern eine Beweisbedeutung des Geräts für den zu untersuchenden Sachverhalt gegeben ist, wobei eine potentielle Beweisrelevanz bereits ausreicht,

> vgl. zum Anfangsverdacht *Gerhold*, in: BeckOK StPO, 53. Edition, Stand: 1. Oktober 2024, StPO, § 94 Rn. 7 sowie zur potentiellen Beweisrelevanz BVerfGE 120, 274 (350).

Der Zugriff auf Telekommunikationsverbindungsdaten und Kommunikationsinhalten hat zudem immer auch zur Folge, dass persönliche Daten Dritter miterhoben werden, die darüber nicht in Kenntnis gesetzt werden. Dabei können die Daten weit in die Vergangenheit zurückreichen und eine große Menge an Kontakten betreffen. Gerade bei Journalist*innen besteht dabei eine hohe Wahrscheinlichkeit, dass auch vertrauliche Quellen umfasst sind. Auch die Kommunikation mit anderen Berufsgruppen, bei denen das Vertrauensverhältnis verfassungsrechtlich besonders geschützt ist, etwa Ärzt*innen, Geistliche, Journalist*innen oder Abgeordnete, kann erfasst sein. Hierdurch wird einerseits die Streubreite des Eingriffs erhöht und andererseits die – auch im Allgemeinwohl liegende – Möglichkeit der Bürger*innen beschränkt, an einer unbeobachteten und damit unbefangenen Fernkommunikation teilzunehmen, sodass die Eingriffsintensität insgesamt weiter erhöht wird,

> BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, - 1 BvR 595/07 -, juris, Rn. 233.

Zur Erhöhung der Eingriffsintensität trägt insbesondere bei, dass durch die Erfassung von Informationen über eine Vielzahl unbeteiligter dritter Kommunikationspartner*innen gleichzeitig in weitere Grundrechte eingegriffen werden kann. Je mehr grundrechtliche Schutzbereiche betroffen sind, desto intensiver ist tendenziell der gesamte Grundrechtseingriff einzustufen (sog. „*Schutzbereichsverstärkung*“),

> für die Durchsicht nach § 110 Abs. 1, Abs. 3 StPO vgl. *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 224 f. m.w.N.

So kann bei der Beschlagnahme eines Datenträgers von Journalist*innen oder von Datenträgern in Redaktionsräumen von Presse- oder Rundfunkunternehmen das Redaktionsgeheimnis oder der Quellenschutz und somit die Presse- bzw. Rundfunkfreiheit gem. Art. 5 Abs. 1 Satz 2 GG berührt sein. Wenn Daten aus einem Mandatsverhältnis zwischen Anwält*innen und Mandant*innen ausgewertet werden, würde das den Schutzgehalt der Berufsfreiheit aus Art. 12 GG betreffen und müsse besonders berücksichtigt werden,

> BVerfGE 113, 29 (48 ff.); BVerfG, Beschluss vom 11. Juli 2008 - 2 BvR 2016/06 -, NJW 2009, 281 (282).

Auch das Bundesverfassungsgericht hat bereits in seiner Entscheidung aus dem Jahr 2005 die Gefahren der hohen Streubreite und (potentiellen) Erfassung rechtlich geschützter Vertrauensverhältnisse erkannt und als eingriffsverstärkend angesehen:

> „*Die besondere Eingriffsintensität des Datenzugriffs ergibt sich daraus, dass die strafprozessuale Maßnahme wegen der Vielzahl verfahrensunerheblicher Daten eine Streubreite aufweist und daher zahlreiche Personen in den Wirkungsbereich der Maßnahme mit einbezogen werden, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 100, 313 [380] = NJW 2000, 55; BVerfGE 107, 299 [320f.] = NJW 2003, 1787). Hinzu kommt die besondere Schutzbedürftigkeit der von einem überschießenden Datenzugriff mitbetroffenen Vertrauensverhältnisse*“,
>
> BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1920).

Schließlich kann die Eingriffstiefe dadurch erhöht sein, dass durch die Vervielfältigung und Speicherung von Daten – insbesondere in einem IT-System der Strafverfolgungsbehörden – potentiell mehr Personen Zugriff auf die Daten erlangen und diese zudem maschinell einfacher ausgewertet werden können,

> *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 (2726 Rn. 5); *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 2023, 1070 (1074); vgl. BVerfG, Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, NJW 2023, 1196 (1201, 1205).

So können personenbezogene Daten aus Strafverfahren nach § 481 StPO grundsätzlich auch für sonstige polizeiliche Zwecke verwendet werden und § 98c StPO erlaubt unter anderem personenbezogene Daten aus einem Strafverfahren zur Aufklärung einer Straftat mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abzugleichen; dabei setzt § 98c StPO lediglich einen einfachen Tatverdacht voraus und enthält keine weiteren Eingriffsvoraussetzungen,

> *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 2023, 1070 (1074).

(4) Hohe Eingriffsintensität aufgrund fehlender Transparenz

Das Eingriffsgewicht wird auch dadurch erhöht, dass Betroffenen die Intensität der Maßnahme regelmäßig nicht bewusst sein wird. Die beschuldigte Person im Strafverfahren hat – von der Ausnahme des § 95a StPO abgesehen – zwar Kenntnis von der Beschlagnahme. Allerdings weiß die betroffene Person nicht, in welcher Weise und in welchem Umfang anschließend auf welche Daten zugegriffen wird. Sie hat auch faktisch keine Möglichkeit, den Datenzugriff sowie die anschließende Auswertung effektiv zu überwachen und kann somit nicht kontrollieren, welche Daten von gespeichert und durchgesehen, auf welche Weise oder in welcher Reihenfolge sie ausgewertet und interpretiert werden oder ab wann der Datenzugriff beginnt und bis wann er andauert. Dadurch verschwimmt bei solchen Ermittlungsmaßnahmen die Grenze zwischen offenem und verdecktem Vorgehen. Auch fehlt eine Kontrollmöglichkeit der betroffenen Person

darüber, ob die Ermittlungsbehörden die Integrität des Datensatzes wahren oder ob aus ihm Daten entfernt oder hinzugefügt werden,

> für die Durchsicht nach § 110 Abs. 1, Abs. 3 StPO vgl. *Hiéramente*, Umgang mit Smartphones im Strafprozess: Überlegungen zu den Reformideen des 74. Deutschen Juristentags 2024, StV 2024, 611 (613); *Greco*, Ermittlungsziel: Smartphone, StV 2024, 276 (278); *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 104 f., 227.

Zwar kann die Verwertung der Daten einem späteren Verwertungsverbot unterfallen, doch greift bereits der (potentielle) Zugang zu allen Daten und deren Sicherung schwerwiegend in die Persönlichkeitsrechte der Betroffenen ein und kann bereits ein Gefühl der Überwachung hervorrufen, das ein faktisches Hemmnis für die Ausübung von Freiheitsrechten schafft,

> vgl. VG Karlsruhe, Beschluss vom 21. März 2024 - 10 K 4632/23 -, S. 8 (**Anlage 11**).

In der Literatur wird insoweit von einem versteckten Geheimnischarakter der Beschlagnahme gesprochen,

> *Zerbes/Ghazanfari*, Stellungnahme im Auftrag des Instituts für Anwaltsrecht der Universität Wien zur Sicherstellung und Auswertung von Daten und Datenträgern, Österr. Anwaltsblatt, 2022, 640 (648), abrufbar unter https://www.oerak.at/fileadmin/user_upload/Anwaltsblatt/22_anwbl12.pdf (Letzter Abruf: 16. Juli 2025).

Aus diesem Grund sieht der österreichische Verfassungsgerichtshof in dem Datenzugriff auf ein beschlagnahmtes Handy keine

> „*tatsächlich ‚offene' Maßnahme* […]*, weil für den Betroffenen nicht ersichtlich ist, in welcher Form die Auswertung der auf dem Datenträger (extern oder lokal) gespeicherten Daten erfolgt (ob z.B. gelöschte Daten wiederhergestellt werden, eine Verknüpfung mit anderen Daten vorgenommen wird etc.)*",
>
> VfGH Österreich, Erkenntnis vom 14. Dezember 2023 - G 352/2021-46 -, BeckRS 2023, 36793 Rn. 75.

Zudem erhalten insbesondere Dritte, deren Daten auf einem ausgelesenen Mobiltelefon enthalten sind, regelmäßig überhaupt keine Kenntnis von dem Eingriff in ihre Daten. Diese erfahren dies allenfalls von der Person, bei dem der Datenzugriff erfolgte, nicht aber durch die Behörden. Dabei liegt auf der Hand, dass beispielsweise ein typischer WhatsApp-Chat für beide teilnehmende Personen gleichermaßen sensibel ist, sodass die Auswertung desselben zwangsläufig auch beide Personen betrifft,

> vgl. zu diesem Aspekt schon BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 233.

Jedenfalls gegenüber den vom Datenzugriff betroffenen Personen, die nicht unmittelbar durch die Behörden adressiert sind, erfolgt der Datenzugriff heimlich und ist durch eine hohe Intensität gekennzeichnet, da sich im Rahmen der vertrauten Kommunikation, möglicherweise über Jahre, eine Vielzahl von Daten findet,

> *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 13, 45; *Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen, NStZ 2012, 593 (598).

(5) Vergleichbarkeit der Eingriffsintensität mit verdeckten Überwachungsmaßnahmen

Jedenfalls ist ein Datenzugriff auf beschlagnahmte komplexe IT-Geräte – insbesondere auf Smartphones – in seiner Intensität vergleichbar mit geheimen Zugriffen wie die Online-Durchsuchung nach § 100b Abs. 1 StPO oder die Telekommunikationsüberwachung nach § 100a StPO.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Intensität des Eingriffs in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in erster Linie von der Art des Datenträgers abhängig und nicht von der Art des Datenzugriffs,

BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 203; eingehend *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 149.

Als Faktoren sind insbesondere die Quantität und Qualität der erfassten Daten entscheidend:

„*Das Eingriffsgewicht einer Befugnis zur Datenerhebung wird vor allem durch* ***Art, Umfang*** *und* ***denkbare Verwendung der Daten*** *sowie* ***die Gefahr ihres Missbrauchs*** *bestimmt. […] Auch die Heimlichkeit einer staatlichen Eingriffsmaßnahme erhöht das Eingriffsgewicht*“ [Hervorhebungen durch die Unterzeichnerin],

BVerfG, Beschluss vom 14. November 2024 - 1 BvL 3/22 -, juris, Rn. 93 zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung; ähnlich bereits BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -, juris, Rn. 129 zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis; eingehend *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 151 f.

Auch hat das Bundesverfassungsgericht die Gefahr gesehen, dass

„*bereits die Beschlagnahme oder Kopie von Speichermedien* […] *ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen* [aufweist]“,

BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 230.

In der strafrechtlichen Literatur wird für eine derart hohe Eingriffsintensität eines Datenzugriffs auf beschlagnahmte IT-Geräte wie Smartphones angenommen, dass sie kaum zu übertreffen sei. So führt *El-Ghazi* aus, dass „*nur wenige Eingriffe denkbar* [sind]*, die noch tiefgründiger in die Rechte des Betroffenen eingreifen. Kaum eine strafprozessuale Maßnahme ermöglicht in gleicher Weise den Zugriff auf einen potenziell so gehaltvollen und vielfältigen Datenbestand, mit dessen Hilfe das Leben des Betroffenen allumfassend analysiert werden kann*“,

El-Ghazi, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 68.

Der Informationsgehalt von Smartphonedaten entspricht hinsichtlich Art und Umfang im Wesentlichen dem einer Online-Durchsuchung und begründet dadurch die besonders hohe Eingriffsintensität eines Datenzugriffs,

> so auch *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 78, 1070 (1076); *Ludewig*, Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf?, KriPoZ 2019, 293 (297); *Momsen*, Entsperrung biometrischer Sicherungen im Strafverfahren, DRiZ 2018, 140.

Teilweise wird deshalb vertreten, dass eine Datenauswertung beschlagnahmter komplexer IT-Geräte nur nach den Vorgaben der Online-Durchsuchung aus § 100b StPO (analog) erfolgen kann,

> *Cornelius*: Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 Rn. 3 (2727 Rn. 11); *Greco*, Ermittlungsziel: Smartphone, StV 2024, 276 (280).

Überdies ermöglicht auch die Auswertung eines Datenträgers, insbesondere eines Mobiltelefons, wie die Praxis eindrucksvoll zeigt, eine Auswertung für einen langen Zeitraum. In dieser Hinsicht besteht der einzige Unterschied zur Mitverfolgung der Kommunikation im Rahmen verdeckter Überwachungsmaßnahmen lediglich darin, dass die Auswertung des Handys allein vergangenheitsgewandt ist. Dies führt aber weder hinsichtlich des Zeitraums noch des Umfangs dazu, dass weniger Daten ausgewertet werden. Während etwa bei einer Telefonkommunikationsüberwachung nach § 100a zwar laufend Daten abgefangen werden, beziehen sich diese aber allein auf die laufende Telekommunikation. Einen Zugriff auf vergangene Telekommunikation oder andere (auf dem Mobiltelefon gespeicherte Daten) ermöglicht die Maßnahme in technischer Hinsicht nicht,

> *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 68; ähnlich *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 (2727) und *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 261: „*Die Gefahr der Erstellung eines Persönlichkeitsprofils kann hier also ebenso, wenn nicht gar umso mehr bestehen als bei Überwachungsmaßnahmen, die erst in der Gegenwart bei Null ansetzen und dann nur noch in die Zukunft wirken*“.

Auch im Vergleich zur akustischen Wohnraumüberwachung nach § 100c StPO bleibt die Eingriffsintensität eines Datenzugriffs auf ein beschlagnahmtes Mobiltelefon nicht hinter der Schwere dieser zurück. Beim Zugriff auf Smartphonedaten lassen sich im Vergleich deutlich vielfältigere und tiefgreifendere Informationen über das Leben und die Persönlichkeit der betroffenen Person gewinnen. Auch der Umfang der erfassten Informationen unbeteiligter Dritter dürfte bei einem Zugriff auf den vollständigen Datenbestand eines Smartphones deutlich über das hinausgehen, was bei einer akustischen Wohnraumüberwachung typischerweise erfasst würde,

> *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 229.

Zudem ist zu befürchten, dass Menschen in Deutschland nicht mehr frei und unbeschwert digital kommunizieren, um zu verhindern, dass die Behörden Zugriff auf ihre höchstpersönlichen Daten bekommen,

> vgl. zu diesem „*chilling effect*“ schon BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 233.

Dementsprechend hat der Europäische Gerichtshof für Menschenrechte (EGMR) in seinem Urteil vom 6. Juni 2024 die Auswertung eines Mobiltelefons selbst dann als einen intensiven Eingriff in das Recht auf Privatsphäre und Familie nach den Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union eingestuft, wenn die betroffene Person den Datenträger freiwillig an die Behörden herausgibt,

> Redaktionelle Orientierungssätze in deutscher Sprache bei EGMR, Urteil vom 6. Juni 2024 - 36559/19 -, juris; Urteilsgründe in französischer Sprache abrufbar unter: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-234090%22]} (Letzter Abruf: 18. Juli 2025).

cc. Verfassungswidrigkeit des Datenzugriffs

Vor dem Hintergrund des besonders hohen Eingriffsgewichts ist ein auf die §§ 94 ff. StPO gestützter Datenzugriff auf komplexe IT-Geräte – insbesondere auf Smartphones – verfassungswidrig.

(1) Verstoß gegen die Wesentlichkeitstheorie sowie das Gebot der Normenklarheit und Normenbestimmtheit

Die §§ 94 ff. StPO stellen keine spezifische, hinreichend bestimmte Ermächtigungsgrundlage dar, die Zugriffe auf komplexe IT-Geräte – insbesondere auf Smartphones –, die schwerwiegende Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellen, rechtfertigen könnten.

(a) Maßstäbe des Grundgesetzes

Grundrechtseinschränkungen sind nur wirksam, wenn sie unter Wahrung des Gesetzesvorbehalts normenklar und hinreichend bestimmt sind,

> BVerfG, Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, Rn. 110 ff.

In ständiger Rechtsprechung hat das Bundesverfassungsgericht aus dem grundgesetzlichen Gesetzesvorbehalt und dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) sowie dem Demokratieprinzip (Art. 20 Abs. 1 und 2 GG) die Verpflichtung des Gesetzgebers abgeleitet, in allen grundlegenden normativen Bereichen die wesentlichen Entscheidungen selbst zu treffen,

> BVerfGE 150, 1 (96 Rn. 191 m.w.N.); grundlegend schon BVerfGE 33, 125 (159 ff., 163); BVerfGE 40, 237 (248 f. Rn. 45); BVerfGE 49, 89 (126 Rn. 76).

Er muss in diesen wesentlichen Bereichen, d.h. vor allem für die Verwirklichung der Grundrechte, Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festlegen,

BVerfGE 120, 274 (315 f.); BVerfGE 100, 313 (359 f.); BVerfGE 162, 378.

Eng mit der Wesentlichkeitstheorie verbunden sind das Gebot der Bestimmtheit und das aus Art. 20 Abs. 3 GG folgende Gebot der Normenklarheit. Ersteres verlangt, dass die Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine Rechtskontrolle durchführen können,

BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 209.

Beim Gebot der Normenklarheit steht die inhaltliche Verständlichkeit einer Regelung im Vordergrund, insbesondere damit Bürger*innen sich auf mögliche belastende Maßnahmen einstellen können,

BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 -, NVwZ-RR 2023, 1 (6 Rn. 110); *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 20 Rn. 89, 91.

Bei einer hohen Eingriffsintensität sind auch hohe Anforderungen an Bestimmtheit und Normenklarheit zu stellen,

BVerfG, Beschluss vom 8. August 1978 - 2 BvL 8/77 -, NJW 1979, 359 (360).

Speziell bezogen auf Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz zu den Anforderungen an die gesetzliche Bestimmtheit ausgeführt:

„*Bei der näheren Ausgestaltung der Einzelbefugnisse kommt es für deren Angemessenheit wie für die zu fordernde Bestimmtheit maßgeblich auf das Gewicht des jeweils normierten Eingriffs an. Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und berechtigte Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen*“,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1784 Rn. 105).

(b) Maßstäbe aus der Europäischen Menschenrechtskonvention

Darüber hinaus ergeben sich auch aus der Europäischen Menschenrechtskonvention (nachfolgend EMRK) bedingt durch die besonders hohe Eingriffsintensität eines solchen Datenzugriffs erhöhte Anforderungen an die hinreichende Bestimmtheit einer Ermächtigungsgrundlage.

Das Grundgesetz ist völkerrechtsfreundlich auszulegen. Wenngleich völkerrechtliche Verträge gem. Art. 59 Abs. 2 Satz 1 GG mittels Zustimmungsgesetz lediglich im Rang eines Bundesgesetzes in das deutsche Recht eingeführt werden und damit unterhalb der Verfassung stehen,

BVerfGE 151, 1 (26 f. Rn. 61 m.w.N.),

gebietet die Völkerrechtsfreundlichkeit des Grundgesetzes, dass sie als Auslegungshilfe für die Bestimmung des Inhalts und der Reichweite der Grundrechte heranzuziehen sind,

BVerfG, Beschluss vom 16. Dezember 2021 - 1 BvR 1541/20 -, juris, Rn. 102 m.w.N.; BVerfG, Beschluss vom 29. Januar 2019 - 2 BvC 62/14 -, juris, Rn. 62 m.w.N.

Die Sammlung und Speicherung von Daten bestimmter Personen durch die Sicherheitsbehörden kann einen Eingriff in dieses verfassungsgesetzlich gewährleistete Recht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK darstellen,

EGMR, Urteil vom 26. März 1987 - 9248/81 - (Leander ./. Schweden) Rn. 47 ff.; EGMR, Urteil vom 2. September 2010 - 35623/05 - (Uzun ./. Deutschland), Rn. 46 m.w.N.

Die Anforderungen an die Ermächtigungsgrundlage bei einem Eingriff in dem durch einen Datenzugriff berührten Art. 8 EMRK sind durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte konkretisiert. Der Ausdruck „gesetzlich vorgesehen“ in

Art. 8 Abs. 2 EMRK bedeutet, dass die innerstaatliche Rechtgrundlage rechtstaatlichen Anforderungen genügen muss,

> EGMR, Urteil vom 2. September 2010 - 35623/05 - (Uzun ./. Deutschland), Rn. 60 m.w.N.

Bisher hat der Europäische Gerichtshof für Menschenrechte diese Anforderungen an die Rechtsgrundlage insbesondere in Fällen von geheimen Überwachungsmaßnahmen herausgearbeitet. Aufgrund der vergleichbar hohen Eingriffsintensität sowie der faktischen Heimlichkeit des Datenzugriffs und der Datenauswertung (dazu oben **1.c.bb.(5)**) ist davon auszugehen, dass die nachfolgend angeführten Maßstäbe im Wesentlichen auch auf den Datenzugriff auf beschlagnahmte Datenträger zu übertragen sind.

Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte muss die gesetzliche Grundlage Schutz vor willkürlichen Eingriffen in die Rechte aus Art. 8 EMRK bieten. Hierfür muss das Gesetz inhaltliche Kriterien für das behördliche Einschreiten festlegen und verfahrensrechtliche Sicherungen gegen eine willkürliche Ausübung des Entscheidungsspielraums der Behörde vorsehen. Ob dieser Schutz gewahrt ist, hängt von Art, Umfang und Dauer der möglichen staatlichen Maßnahmen, die Gründe, aus denen sie angeordnet werden dürfen, das Verfahren der Genehmigung, Durchführung und Überwachung solcher Maßnahmen und die Art des nach innerstaatlichem Recht vorgesehenen Rechtsbehelfs ab,

> EGMR, Urteil vom 2. September 2010 - 35623/05 - (Uzun ./. Deutschland), Rn. 63 m.w.N.

Bei staatlichen Ermittlungsmaßnahmen muss das Gesetz auch festlegen, welche Personen adressiert sind und bei welchen konkreten Delikten die Maßnahme zulässig ist. Zudem müssen die zeitliche Dauer der Maßnahme und die Löschung von Daten gesetzlich festgelegt werden. Außerdem müssen Reichweite und Ausübung des Ermessens des*der zuständigen Untersuchungsrichter*in hinreichend begrenzt werden,

> EGMR, Urteil vom 24. April 1990 - 11801/85 - (Kruslin ./. Frankreich), Rn. 27 ff.

(c) Verstoß gegen verfassungsrechtliche Anforderungen

Ein auf die §§ 94 ff. StPO gestützter Datenzugriff genügt nicht den zuvor dargelegten verfassungsrechtlichen Anforderungen – insbesondere auch unter Mitberücksichtigung der Maßstäbe aus der EMRK an eine hinreichend bestimmte Ermächtigungsgrundlage, die für einen solchen Eingriff einzuhalten sind.

Der schwerwiegende Grundrechtseingriff wird auf eine gesetzliche Grundlage gestützt, die in ihrem Wortlaut den kompletten Zugriff auf und die umfassende Auswertung von Datenträgern, wovon auch komplexe informationstechnische Systeme wie Smartphones umfasst sind, überhaupt nicht regelt. Der Gesetzgeber hat diesbezüglich weder bestimmt, auf welche Art und Weise noch wie intensiv in welche konkreten Grundrechte eingegriffen werden darf. Insbesondere sind das Ausmaß und die Grenzen des Datenzugriffs, die Art der technischen Durchführung sowie Rückgabefristen gesetzlich nicht festgelegt. Auch schreibt der Gerichtsvorbehalt nach § 98 Abs. 1 StPO gesetzlich nicht vor, dass die Modalitäten des Datenzugriffs im Einzelfall im gerichtlichen Beschluss vorgegeben werden müssen. Dies spiegelt sich in der Praxis wider: Regelmäßig beziehen sich solche Anordnungen nur auf die Beschlagnahme an sich und erwähnen noch nicht einmal den anschließend möglichen Datenzugriff. Dies führt dazu, dass dieser im alleinigen Ermessen der Strafverfolgungsbehörden stehen.

Schließlich genügen die §§ 94 ff. StPO auch nicht den Anforderungen des EGMR an eine hinreichend bestimmte Gesetzesgrundlage zur Rechtfertigung eines derart schwerwiegenden Eingriffs, da weder gesetzlich vorgeschrieben ist, bei welchen konkreten Delikten die Maßnahme zulässig ist noch verfahrensrechtliche Sicherungen gegen eine willkürliche Ausübung des Entscheidungsspielraums der Behörde vorgesehen sind. Solche Verfahrensgarantien fehlen in den §§ 94 ff. StPO; die Vorschriften unterscheiden nicht zwischen einer Beschlagnahme und eines anschließenden Datenzugriffs auf Datenträgern von Privatpersonen oder besonders geschützten Berufsgruppen.

(d) Keine Übertragbarkeit früherer verfassungsrechtlicher Rechtsprechung

Sofern frühere Entscheidungen des angerufenen Gerichts – gemessen am Maßstab des Rechts auf informationelle Selbstbestimmung – in den §§ 94 ff. StPO eine hinreichend bestimmte

Ermächtigungsgrundlage für die Beschlagnahme, den Datenzugriff auf und die Auswertung von Datenträgern und Daten gesehen und für ausreichend gehalten hat, wenn der besonderen Eingriffsintensität im Einzelfall gerecht wird,

> BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917; BVerfG, Urteil vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, 976; BVerfG, Beschluss vom 25. Juli 2007 - 2 BvR 2282/06 -, NJW 2007, 3343,

ist dies anhand seiner neueren Rechtsprechung nicht mehr tragbar (dazu bereits oben **1.a.**).

(aa) Höhere Eingriffsintensität und veränderte Gefahrenlage

Bereits in seiner Grundsatzentscheidung im Jahr 2008 hat das angerufene Gericht in Bezug auf den Schutzgehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme festgestellt, dass

> „*der spezifische Grundrechtsschutz* […] *sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern* können [, erstreckt]“,
>
> BVerfGE 120, 274 (314).

Das angerufene Gericht hat bereits damaligen Mobiltelefonen einen großen Funktionsumfang und eine Vielfalt an gespeicherten Daten attestiert und diesbezüglich ein gesteigertes Schutzbedürfnis anerkannt. Diese Schutzbedürftigkeit gilt heute umso mehr: Moderne Smartphones übertreffen den Leistungsumfang und die Speichermöglichkeiten von Daten früherer Mobiltelefone um ein Vielfaches. Die mit einem Datenzugriff verbundenen Gefahren für die Persönlichkeitsrechte der Betroffenen hat sich dadurch mit der Zeit erheblich verschärft.

Bei der Beurteilung der Gefahrenlage ist daher insbesondere die technische Weiterentwicklung von Datenträgern und das damit einhergehende veränderte Nutzungsverhalten zu berücksichtigen. So hat auch das angerufene Gericht im Zusammenhang mit der verfassungsmäßigen

Ausgestaltung von Ermächtigungsgrundlagen für Überwachungsmaßnahmen ausdrücklich darauf hingewiesen, dass der Gesetzgeber bei der Abwägung zwischen dem Eingriffsgewicht und dem verfolgten Zweck die fortschreitende Entwicklung der Informationstechnik berücksichtigen muss. Diese dehne die Reichweite von Überwachungsmaßnahmen zunehmend aus, erleichtere ihre Durchführbarkeit und erlaube Verknüpfungen, die bis hin zu Erstellung von Persönlichkeitsprofilen reichten,

> BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1783 Rn. 99).

Datenzugriff auf komplexe IT-Geräte – insbesondere auf Smartphones – erfordern daher deutlich höhere und spezifisch auf die damit verbundenen Risiken abgestimmte Anforderungen an den Gesetzesvorbehalt, die Bestimmtheit und Normenklarheit, die nicht mit den Gefahren eines bloß punktuellen Zugriffs auf eingegrenzte persönliche Daten oder Kommunikationsinhalte, die dem Schutz des Grundrechts auf informationelle Selbstbestimmung bzw. dem Fernmeldegeheimnis unterliegen, vergleichbar sind.

(bb) Begrenzung auf Ermittlungszweck unzureichend

Auch reicht allein die Begrenzung der Maßnahme auf den Ermittlungszweck nicht (mehr) aus, den Anlass, Zweck und die Grenzen eines derartigen Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen.

Anlässlich der Beschlagnahme des elektronischen Datenbestandes einer Rechtsanwaltskanzlei und einer Steuerberatungsgesellschaft hat das angerufene Gericht in seiner damaligen Entscheidung aus dem Jahr 2005 für einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung festgestellt:

> *„c) Für den vom Datenzugriff Betroffenen ist hinreichend erkennbar, dass die §§ 94ff. StPO die Sicherstellung und Beschlagnahme des Datenträgers und der hierauf gespeicherten Daten ermöglichen. § 94 StPO erfasst grundsätzlich alle Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können. Eine nähere gesetzliche Eingrenzung ist wegen der Vielgestaltigkeit möglicher Sachverhalte nicht geboten. Die*

verfahrensbezogene Konkretisierung hat von Verfassungs wegen der Richter nach Möglichkeit im jeweiligen Durchsuchungs- oder Beschlagnahmebeschluss zu leisten […]. *d) Die strafprozessualen Beschlagnahmeregelungen genügen auch der insbesondere für das Recht auf informationelle Selbstbestimmung geltenden Vorgabe, wonach der Gesetzgeber den Verwendungszweck der erhobenen Daten bereichsspezifisch und präzise bestimmen muss* […]. *Der den Datenzugriff begrenzende Verwendungszweck ist unter Beachtung des Normzusammenhangs, in welchen die §§ 94ff. StPO eingebettet sind (vgl. §§ 152 II, 155 I, 160, 170, 244 II, 264 StPO), hinreichend präzise vorgegeben.*

Die Ermittlungsmethoden der StPO sind zwar im Hinblick auf die Datenerhebung und den Datenumfang weit gefasst. Die jeweiligen Eingriffsgrundlagen stehen aber unter einer strengen Begrenzung auf den Ermittlungszweck. Strafprozessuale Ermittlungsmaßnahmen sind nur zulässig, soweit dies zur Vorbereitung der anstehenden Entscheidungen im Hinblick auf die in Frage stehende Straftat nötig ist. Auf die Ermittlung anderer Lebenssachverhalte und Verhältnisse erstrecken sich die Eingriffsermächtigungen nicht.

[…]

Eine Ermittlung außerhalb dieses Zwecks hat keine gesetzliche Grundlage. Gelegentlich einer strafrechtlichen Ermittlung dürfen daher keine Sachverhalte und persönlichen Verhältnisse ausgeforscht werden, die für die Beurteilung der Täterschaft und für die Bemessung der Rechtsfolgen der Tat nicht von Bedeutung sind (vgl. § 244 III 2 Alt. 2 StPO)“,

BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1920).

In Bezug auf die Beschlagnahme eines Mobiltelefons zur Auswertung der darauf gespeicherten Telekommunikationsverbindungsdaten hat das angerufene Gericht mit einer Entscheidung aus dem Jahr 2006 ebenfalls am Maßstab des Rechts auf informationelle Selbstbestimmung unter Bezugnahme auf den oben angeführten Beschluss bestätigt, dass

„[d]*ie Vorschriften* […] *der vor allem für das Recht auf informationelle Selbstbestimmung geltenden Vorgabe* [entsprechen]*, 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 - insbesondere die Aufklärung der Straftat - Genüge getan*“,

BVerfG, Urteil vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, 976 (980 Rn. 94).

Auch in seiner Entscheidung vom 25. Juli 2007 - 2 BvR 2282/06 - verweist das angerufene Gericht auf die Ausführungen in seinem Beschluss aus dem Jahr 2005 und gibt sie wortgetreu wieder,

BVerfG, Beschluss vom 25. Juli 2007 - 2 BvR 2282/06 -, NJW 2007, 3343 (3344).

Mit der neuen verfassungsgerichtlichen Rechtsprechung, die mit Blick auf die mit dem technischen Fortschritt einhergehenden Gefahren für die Persönlichkeitsrechte einen Vertraulichkeits- und Integritätsschutz bestimmter informationstechnischer Systeme vorsieht, ist aber gerade nicht mehr davon auszugehen, dass der Verwendungszweck durch eine Begrenzung der Maßnahme auf den Ermittlungszweck, der sich einzig aus dem Normenzusammenhang ergebe, ausreichend sein könnte.

Die in den zuvor angeführten Entscheidungen vertretene Auffassung, dass es für die Betroffenen erkennbar sei, dass die §§ 94 ff. StPO zur Beschlagnahme eines Datenträgers und auch der darauf gespeicherten Daten ermächtigten, mag im Grundsatz zutreffen. Doch kann jedenfalls eine hinreichende Erkennbarkeit der Art und des Ausmaßes eines Datenzugriffs und der inhaltlichen Auswertung der Daten nicht angenommen werden. Die Modalitäten eines Datenzugriffs sind im Wortlaut der §§ 94 ff. StPO weder in inhaltlicher noch in verfahrenstechnischer Hinsicht geregelt. Die von der Maßnahme Betroffenen können nicht erkennen auf welche ihrer Daten in welcher Weise zugegriffen wird, ob gelöschte Daten wiederhergestellt werden, in welcher Form der Datenbestand durchsucht und ausgewertet wird, ob und welche Suchparameter dafür benutzt werden, ob die gewonnenen Daten manipulationsfrei sind oder ob und welche Verknüpfung mit anderen Daten vorgenommen wird.

Die fehlende Erkennbarkeit wird insbesondere in Fällen deutlich, in denen ein Datenträger eine Zugangssperre enthält und somit nur das Gerät als Ganzes mitsamt aller darauf gespeicherten Daten beschlagnahmt werden kann. Dies ist bei Smartphones, aber auch Computer regelmäßig der Fall. Nach der Beschlagnahme des Datenträgers muss dieser entsperrt werden, um auf die Daten zugreifen zu können. Mit der Entsperrung des Geräts wird den Strafverfolgungsbehörden der Zugang zu allen darauf gespeicherten Daten eröffnet sowie zu gelöschten Daten, die durch die benutzte forensische Auswertungssoftware wieder hergestellt werden können und vernetzten Daten, die auf einer Cloud gespeichert sind. Damit geht bereits die potentielle Gefahr einer Totalausforschung und die damit verbundene Abschreckungswirkung einher, denen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entgegenwirken soll. Berechtigte Vertraulichkeits- und Integritätserwartungen der Betroffenen werden zu diesem Zeitpunkt schon beeinträchtigt. Damit ist die Einschränkung auf den Ermittlungszweck besonders in solchen Fällen vollkommen ungeeignet, der Gefahr einer umfassenden Ausforschung der Persönlichkeit zu begegnen.

Die zuvor angeführten früheren Entscheidungen des angerufenen Gerichts tragen bei ihrer Beurteilung der hinreichenden Bestimmtheit und Erkennbarkeit derartigen Gefahren nicht hinreichend Rechnung. Dies ist auch dem Umstand geschuldet, dass diese Entscheidungen den Eingriff nur am Maßstab des Rechts auf informationelle Selbstbestimmung messen (konnten). Der mit der neueren Rechtsprechung entwickelte, weitergehende Schutz zielt jedoch gerade darauf ab, die Schutzlücken des Rechts auf informationelle Selbstbestimmung zu füllen. Letzteres vermag zwar bei einer gezielten und punktuellen Datenerhebung ausreichend Schutz gewährleisten, bietet jedoch keinen ausreichenden Schutz vor der mit einem Datenzugriff auf informationstechnische Systeme einhergehenden Gefahrenlage, mit dem sich **potentiell** ein äußerst großer und aussagekräftiger Datenbestand auf einmal verschafft werden kann.

Wenn anschließend der gesamte Datenbestand ausgelesen, zwischengespeichert und der inhaltlichen Auswertung zu Grunde gelegt wird, wird dieser Eingriff weiter vertieft. Die alleinige Beschränkung auf den Ermittlungszweck verhindert auch in diesem Stadium nicht, dass Strafverfolgungsbehörden zunächst den gesamten Datenbestand umfassend durchleuchten, um anschließend bewerten zu können, welchen Informationen eine Beweisrelevanz zukommt und welchen nicht. Die Frage der Beweisbedeutung lässt sich nämlich regelmäßig erst nach inhaltlicher Kenntnisnahme klären. Besonders Mobiltelefone enthalten eine Vielzahl sensibler und

kernbereichsnaher Daten, die potentiell für den Nachweis einer Straftat in Frage kommen und durchforstet werden können – etwa Geodaten, private Bilder, Videos und Kommunikationsinhalte. Die Datenmenge und -vielfalt haben sich in den letzten zwei Jahrzehnten erheblich ausgeweitet. In modernen Smartphones sind Informationen aus sämtlichen Lebensbereichen gespeichert, was sich insbesondere in der Nutzung spezialisierter Apps widerspiegelt. So finden sich etwa im Periodenkalender oder der Krankenversicherungs-Apps besonders schützenswerte Gesundheitsdaten, in Fotogalerien intime Aufnahmen, in Notizen-Apps höchstpersönliche Gedanken, Informationen zu sexuellen Vorlieben oder politischen Überzeugungen. Darüber hinaus speichern Mobiltelefone heutzutage auch zahlreiche Daten, auf die die Nutzer*innen für den alltäglichen Gebrauch angewiesen sind, etwa digitale Zahlungsmittel, Zugtickets oder elektronische Büroschlüssel.

Gerade aufgrund der geringen Eingriffsschwelle für Ermittlungsmaßnahmen nach §§ 94 ff. StPO (dazu oben **B.I.1.** sowie unter **(4)(a)** und **(4)(b)**) ist es somit auch unter der Einschränkung auf den Ermittlungszweck möglich, eine Vielzahl an höchstpersönlichen Informationen zur Kenntnis zu nehmen. Darüber hinaus ermöglichen moderne Analyseprogramme es, innerhalb einer kurzen Zeit riesige Datenbestände auszuwerten und können dabei auch Zufallsfunde erfassen, die auf die Verübung anderer Straftaten hindeuten und ebenfalls gesichert werden dürfen. Für einen derart weitreichenden Datenzugriff sind keine ausreichenden gesetzlichen Schranken vorgesehen.

Schließlich trägt in Fällen, in denen der Datenträger als Ganzes beschlagnahmt werden muss, auch die gerichtliche Beschlagnahmeanordnung nicht zu einer hinreichenden Bestimmtheit und Erkennbarkeit bei. Die gerichtliche Anordnung ist nur zu Beginn der Beschlagnahme einzuholen und erschöpft sich in der Beurteilung, ob der Datenträger als solcher Bedeutung für die Untersuchung hat. Dies wird bei Smartphones, aber auch Computern und Tablets aufgrund der Menge und Vielfalt der gespeicherten und miteinander verknüpften Daten regelmäßig der Fall sein. Dadurch ist die gerichtliche Anordnung nur in der Lage den Datenträger als Gegenstand der Beschlagnahme zu konkretisieren. Eine weitergehende Überprüfung in Bezug auf die Art und den Umfang des Datenzugriffs und der inhaltlichen Auswertung unterliegt keiner vorherigen gerichtlichen Kontrolle.

(cc) Allgemeiner Verhältnismäßigkeitsgrundsatz

Schließlich reicht entgegen der früheren Rechtsprechung des angerufenen Gerichts eine Korrektur über den allgemeinen Verhältnismäßigkeitsgrundsatz im Einzelfall nicht aus, um der hohen Eingriffsintensität Rechnung zu tragen (dazu ausführlich unter **(4)(c)**). Allein die Wesentlichkeitstheorie sowie die Gebote der Normenbestimmtheit und -klarheit gebieten bereits, dass der Gesetzgeber die Grenzen der staatlichen Befugnis eingriffsspezifisch selbständig regeln und gesetzlich Fälle ausschließen muss, in denen der Eingriff unverhältnismäßig wäre. Mit diesen Grundsätzen ist es unvereinbar, die Entscheidung über die Durchführung einer derart eingriffsintensiven Ermittlungsmaßnahme mangels gesetzlicher Vorgaben allein den Strafverfolgungsbehörden und Fachgerichten zu überlassen. Auch die vom Bundesgerichtshof sowie von früheren verfassungsgerichtlichen Entscheidungen aufgestellten Gesichtspunkte, die bei der Prüfung der Verhältnismäßigkeit im Einzelfall zu berücksichtigen sind, vermögen diesen Verstoß nicht zu beheben (zu den Gesichtspunkten siehe nachfolgend unter **(e)**). Jedenfalls sind sie zu unbestimmt und unterliegen einem weiten Auslegungsspielraum. Insbesondere ist dabei auch zu berücksichtigen, dass sich die aufgestellten Beurteilungsmaßstäbe in der Durchführung der Beschlagnahme an sich erschöpfen. Für die Art des anschließenden Datenzugriffs und die Durchführung der inhaltlichen Auswertung fehlt es an gerichtlich austarierten Kriterien zur Bewertung der Verhältnismäßigkeit – diese müssten jedenfalls durch den Gesetzgeber selbst festgelegt werden.

Daher bedarf es einer hinreichend bestimmten formell-gesetzlichen Grundlage, die spezifisch den Gefahren für die Vertraulichkeit und Integrität informationstechnischer Systeme in verhältnismäßiger Weise Rechnung trägt. Eine derartige gesetzliche Grundlage existiert nicht.

(e) Außerachtlassung verfassungsrechtlicher Maßstäbe durch den Bundesgerichtshof

Mit Beschluss vom 13. März 2025 - 2 StR 232/24 - überträgt der Bundesgerichtshof die aus den Jahren 2005 und 2006 stammende Rechtsprechung des angerufenen Gerichts auf den umfassenden Datenzugriff bei modernen Smartphones unter Missachtung der seitdem weiterentwickelten verfassungsrechtlichen Anforderungen,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 46 ff.

Damit verkennt der Bundesgerichtshof die durch neuere verfassungsgerichtliche Rechtsprechung etablierte besondere Schutzbedürftigkeit informationstechnischer Systeme und den damit einhergehenden strengen Anforderungen an die hinreichende Bestimmtheit und Verhältnismäßigkeit für Eingriffsermächtigungen.

So stellt er in seinem Beschluss unter fehlerhafter Anwendung der verfassungs- und unionsrechtlichen Maßstäbe fest, dass die

> „*§§ 94 ff. StPO und §§ 102 ff. StPO* […] *den verfassungsrechtlichen und den sich aus der RL 2016/680/EU ergebenden Anforderungen hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten* [genügen]“,
>
> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 45.

Zur Begründung verweist er auf die Entscheidungen des angerufenen Gerichts vom 12. April 2005 - 2 BvR 1027/02 - sowie vom 2. März 2006 - 2 BvR 2099/04 - und gibt die dortigen Ausführungen zur hinreichenden Bestimmtheit und Erkennbarkeit – gemessen am Maßstab des Grundrechts auf informationelle Selbstbestimmung – wörtlich wieder,

> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 46 f.

Wie bereits umfassend ausgeführt, berücksichtigen die in diesen beiden früheren verfassungsgerichtlichen Entscheidungen aufgestellten Erwägungen – insbesondere mit Blick auf die Beschränkung durch den Ermittlungszweck – jedoch nicht die weitergehenden Gefahren für die Vertraulichkeit und Integrität informationstechnischer Systeme, womit ein auf §§ 94 ff. StPO gestützter umfassender Datenzugriff und die anschließende Auswertung gerade diesbezüglich nicht hinreichend bereichsspezifisch, präzise und normenklar geregelt ist (dazu oben **(c)**).

Darüber hinaus lässt der Bundesgerichtshof die mit solchen besonders schwerwiegenden Eingriffen einhergehenden strengen verfassungsgerichtlich etablierten Anforderungen an die Verhältnismäßigkeit völlig unberücksichtigt.

Zwar erkennt er die (besonders) hohe Eingriffsintensität eines einwilligungslosen Zugriffs auf die auf einem Mobiltelefon gespeicherten Daten und zitiert zur Eingriffstiefe Ausführungen des angerufenen Gerichts aus seiner Entscheidung zur Online-Durchsuchung aus dem Jahr 2008. Der Bundesgerichthof führt dazu aus:

> „*Der einwilligungslose Zugriff auf die auf einem Mobiltelefon gespeicherten Daten stellt aber einen schwerwiegenden oder sogar besonders schwerwiegenden Eingriff in das Recht des Beschuldigten auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 GG) sowie in die auch von Art. 7 und 8 GRC verbürgten Grundrechte auf Achtung des Privat- und Familienlebens beziehungsweise auf Schutz personenbezogener Daten dar. Zwar erfolgt der Zugriff bei zwangsweisem Entsperren des Mobiltelefons mittels Fingerabdruck als offene Maßnahme, was es dem Beschuldigten ermöglicht, diesem entgegenzutreten und – etwa durch die Anrufung von Gerichten – zu überwachen (vgl. dazu BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06, BVerfGE 124, 43, 62, 65 f.; vgl. auch Neuhaus, StV 2020, 489 f.). Allerdings befindet sich im Speicher von Mobiltelefonen regelmäßig eine Vielzahl an vertraulichen und höchstpersönlichen Daten, etwa in Form von Kommunikation, Lichtbildern, Videoaufnahmen, Notizen oder Kalendereinträgen, die bei dem Zugriff auf ein Mobiltelefon potentiell der Kenntnisnahme der Ermittlungsbehörden unterliegen. Der Zugang auf solche auf einem Mobiltelefon gespeicherte Daten kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung eines Beschuldigten eröffnen oder genaue Schlüsse auf politische, religiöse oder weltanschauliche Überzeugungen zulassen. Der staatliche Zugriff auf einen solchen umfassenden Datenbestand ist folglich mit dem Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 323)*“,
>
> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 33.

Daraus wird ersichtlich, dass der Bundesgerichtshof ein vergleichbar hohes Gefahrenpotential wie bei verdeckten Überwachungsmaßnahmen annimmt. Gleichwohl wendet er in Folge dieser

Erkenntnis in verfassungswidriger Weise nicht die in diesem Zusammenhang entwickelten strengen Vorgaben an die Wahrung der Verhältnismäßigkeit an, die sich aus einem derart schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergeben,

> so auch *Mansouri/Rückert*, Touch me if you can – Die Zulässigkeit der zwangsweisen Entsperrung eines Mobiltelefons mittels Fingerabdrucks, JR 2025, 2064, S. 4, abrufbar unter: https://doi.org/10.1515/juru-2025-2064 (Letzter Abruf: 17. Juli 2025); *Jahn*, † Strafprozessrecht: Zwangsweise Entsperrung von Smartphones, JuS 2025, 791 (792 f.).

In der vom Bundesgerichtshof in Bezug auf die Eingriffstiefe selbst zitierten Entscheidung zur Online-Durchsuchung stellt das angerufene Gericht den Maßstab auf, dass

> „[e]*in derartiger Eingriff* […] *nur vorgesehen werden* [darf]*, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.*
>
> *Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die - wie hier - die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt*“,
>
> BVerfGE 120, 274 (328).

Auch in seiner nachfolgenden Entscheidung zum BKA-Gesetz hat das angerufene Gericht derart schwerwiegende Eingriffe auf den Schutz oder die Bewahrung hinreichend gewichtiger Rechtsgüter begrenzt. So führt es für repressive Maßnahmen aus:

> „*Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an, die der Gesetzgeber insoweit in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat*“,
>
> BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781, (1784 Rn. 107).

Eine Beschränkung des auf die §§ 94 ff. StPO gestützten Datenzugriff auf überragend wichtige Rechtsgüter oder zumindest auf Rechtsgüter von hinreichender Bedeutung sah der Bundesgerichtshof in seinem Beschluss entgegen den verfassungsrechtlichen Vorgaben als nicht erforderlich an. Das Gericht sieht die in §§ 94 ff. StPO enthaltenen niedrigen Eingriffsschwellen – namentlich den Anfangsverdacht bezüglich jeglicher Straftat sowie die einfache Beweisrelevanz – als ausreichend an, solange dem Grundsatz der Verhältnismäßigkeit im Einzelfall Rechnung getragen werde,

> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 48.

Für die Prüfung der Verhältnismäßigkeit stellt der Bundesgerichtshof folgende Kriterien auf:

> „*Bei der Abwägung (vgl. auch Nr. 73a RiStBV) sind einerseits das staatliche Interesse an einer wirksamen Strafverfolgung (die Sicherung des Rechtsfriedens durch Strafrecht, die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind seit jeher staatliche Kernaufgaben), andererseits die geschützten Rechtsgüter der von der Maßnahme Betroffenen gegenüber zu stellen. Hierbei ist der besonderen Eingriffsintensität beim Zugriff auf ein Mobiltelefon Rechnung zu tragen. Die Schwere der Straftat, die Gegenstand der Ermittlungen ist, stellt dabei einen zentralen Parameter dar. Maßgebend ist, wie sich das Gewicht der Straftat im Einzelfall darstellt. Bestimmende Gesichtspunkte*

sind daneben der Grad des Tatverdachtes und die potentielle Beweisbedeutung der auf dem Mobiltelefon vermuteten Daten. In Betracht zu ziehen ist auch, ob die in Rede stehenden Straftaten mittels eines Mobiltelefons begangen oder angebahnt wurden. Denn wenn der Beschuldigte bewusst ein Medium als Tatmittel seiner strafbaren Handlung einsetzt, muss er es eher hinnehmen, dass sich die Strafverfolgungsbehörden des darauf befindlichen Datenbestandes bedienen (vgl. BVerfG, Beschluss vom 17. Juni 2006 – 2 BvR 1085/05, 2 BvR 1189/05, NJW 2006, 3197, 3198 Rn. 17; vgl. auch Bäumerich, NJW 2017, 2718, 2722). Steht die zu ermittelnde Straftat in keinem Bezug zum Mobiltelefon und/oder den darauf zu vermutenden Daten oder ist der mittels zwangsweise herbeigeführtem Fingerabdruck erlangte Datenzugriff aus anderen Gründen unter Berücksichtigung der Schwere der Straftat und der Erfordernisse der Untersuchung nicht gerechtfertigt, ist er nach der Strafprozessordnung unzulässig“,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 48.

Damit verlagert er die Beurteilung der Verhältnismäßigkeit (im Einzelfall) – entgegen der Wesentlichkeitstheorie und dem Gebot der Normenbestimmtheit und Normenklarheit (dazu oben **(a)**) – in unzulässiger Weise auf die Exekutive bzw. Judikative. Nach den verfassungsrechtlichen Vorgaben ist jedoch bereits eine Beschränkung auf Straftaten mit einer gewissen Schwere gesetzlich vorzusehen (siehe dazu **(4)(a)**). Ein solch umfassender Datenzugriff ist in jedem Fall zur Verfolgung bloßer Ordnungswidrigkeiten oder Bagatellstraftaten unverhältnismäßig. Da dem allgemeinen Verhältnismäßigkeitsgrundsatz die Einzelfallbezogenheit immanent ist, trägt sie den strengen verfassungsrechtlichen Anforderungen an die Eingriffsschwellen für solch besonders schwerwiegende Eingriffe nicht ausreichend Rechnung. Auch erschöpft sich die nach den vom Bundesgerichtshof aufgestellten Kriterien zu erfolgende Verhältnismäßigkeitsprüfung im Einzelfall nur in der Beurteilung, ob eine Beschlagnahme überhaupt erst angeordnet bzw. durchgeführt werden soll. Wenn aber der durch eine Zugangssperre geschützte Datenträger als Ganzes beschlagnahmt wird, finden die aufgestellten Kriterien für einen nachfolgenden Datenzugriff keine Anwendung mehr.

Schließlich verkennt der Bundesgerichtshof auch die Anforderungen des Europäischen Gerichtshof an die hinreichende Bestimmtheit einer Ermächtigungsgrundlage sowie an den

Gerichtsvorbehalt, der spezifisch auf den Datenzugriff ausgerichtet sein muss (siehe zu beiden ausführlich unter **(2)**). Entgegen den Vorgaben des Europäischen Gerichtshofs,

EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 99,

enthalten die §§ 94 ff. StPO keine ausdrücklichen und präzise Vorgaben in Bezug auf die bei der Verhältnismäßigkeitsprüfung zu berücksichtigenden Gesichtspunkte, insbesondere keine gesetzliche Festlegung der Art oder Kategorien der betreffenden Straftaten (dazu unter **(2)(c)**).

Hinsichtlich des Gesetzesvorbehalts sieht der Bundesgerichtshof im Rahmen der Durchsuchung den § 105 Abs. 1 StPO als ausreichend an,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 51.

Doch wie auch der Gerichtsvorbehalt aus § 98 Abs. 1 StPO erschöpft sich dieser nur in der Umschreibung der aufzufindenden bzw. beschlagzunehmenden konkreten Gegenstände, die Bedeutung für die Untersuchung haben könnten. Vorgaben für die Modalitäten eines anschließenden Datenzugriffs und die inhaltliche Auswertung eines durch eine Zugangssperre versehenden Datenträgers enthält weder die gerichtliche Anordnung der Durchsuchung noch der Beschlagnahme und gewährleisten damit gerade nicht die vom Europäischen Gerichtshof als zwingend erforderlich angesehene vorherige gerichtliche Kontrolle, die in der Lage ist, den Datenzugriff auszuschließen oder zu beschränken (dazu unter **(2)(c)**).

(f) Neuregelung in Österreich

Auch der österreichische Gesetzgeber sah sich gezwungen die entsprechenden Vorschriften der Strafprozessordnung neu zu regeln. Der Verfassungsgerichtshof Österreich hat am 14. Dezember 2023 die Verfassungswidrigkeit der damals geltenden strafprozessualen Normen zur Beschlagnahme von Mobiltelefonen und des anschließenden Datenzugriffs und der Datenauswertung festgestellt,

VfGH Österreich, Erkenntnis vom 14. Dezember 2023, - G 352/2021-46 -, BeckRS 2023, 36793.

Anschließend hat der Nationalrat am 27. Dezember 2023 eine umfassende Neuregelung der entsprechenden Vorschriften verabschiedet. Diese Vorschriften sind am 1. Januar 2024 in Kraft getreten,

> BGBl. Nr. 631/1975, zuletzt geändert durch BGBl. I Nr. 157/2024, abrufbar unter: https://ris.bka.gv.at/eli/bgbl/1975/631/P115f/NOR40267211?Sort=1%7cDesc&Abfrage=Bundesnormen&FassungVom=05.02.2025 (Letzter Abruf: 18. Juli 2025).

Dabei wurde spezifisch für die Beschlagnahme von Datenträgern und Daten sowie dem anschließenden Datenzugriff ein ausdifferenziertes Sonderrechtsregime geschaffen – solche Regelungen lassen die §§ 94 ff. StPO gänzlich vermissen. So wird u.a. im neuen § 115f Abs. 1 der österreichischen Strafprozessordnung vorgesehen:

> *„(1) Die Beschlagnahme von **Datenträgern und Daten** ist zulässig, wenn sie aus Beweisgründen erforderlich scheint und aufgrund **bestimmter Tatsachen** anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat **wesentlich** sind.*“ [Hervorhebungen durch Unterzeichnerin].

Auch wurde in § 115f Abs. 2 und 3 der österreichischen Strafprozessordnung ein Gerichtsvorbehalt eingeführt, der gezielt auf die Gefahren eines Datenzugriffs ausgerichtet ist und dafür konkrete inhaltliche Vorgaben für die gerichtliche Anordnung und Bewilligung der Beschlagnahme und des anschließenden Datenzugriffs festgelegt:

> *„(2) Die Beschlagnahme von Datenträgern und Daten ist durch die Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen und von der Kriminalpolizei durchzuführen.*
> *(3) Die Anordnung und die gerichtliche Bewilligung der Beschlagnahme von Datenträgern und Daten haben die Bezeichnung des Verfahrens, den Namen des Beschuldigten, soweit dieser bekannt ist, die Tat, deren der Beschuldigte verdächtig ist, und ihre gesetzliche Bezeichnung sowie die **Tatsachen**, aus denen sich ergibt, dass die Anordnung und Bewilligung zur Aufklärung der Tat **erforderlich und verhältnismäßig** sind, anzuführen und **über die Rechte des von der Anordnung und Bewilligung Betroffenen zu***

***informieren**; darüber hinaus haben sie die **Umschreibung der Datenkategorien und Dateninhalte**, die zu beschlagnahmen sind, und in Bezug auf welchen **Zeitraum** dies zu erfolgen hat, zu enthalten. Die Beschlagnahme darf nur für jenen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks **voraussichtlich erforderlich** ist.*" [Hervorhebungen durch Unterzeichnerin].

Darüber hinaus wird in § 115h Abs. 1 der österreichischen Strafprozessordnung der Vorgang bei einer Aufbereitung von Daten präzise umschrieben und vorgegeben sowie umfassende Dokumentationspflichten in Form eines Aufbereitungsberichts festgelegt:

*„(1) Die ausschließlich für die forensische Aufbereitung von Datenträgern und Daten zuständige Organisationseinheit der Kriminalpolizei hat eine Originalsicherung (§ 109 Z 2c) herzustellen, eine Arbeitskopie (§ 109 Z 2d) zu erstellen und anhand dieser die Aufbereitung von Daten (§ 109 Z 2b) durchzuführen. Sie hat das Ergebnis der Datenaufbereitung (§ 109 Z 2e) in einem allgemein gebräuchlichen Dateiformat in strukturierter Form, sodass die Daten elektronisch weiterverarbeitet werden können, an die für die Führung des Ermittlungsverfahrens zuständige Organisationseinheit der Kriminalpolizei samt einem Aufbereitungsbericht zu übermitteln. Der **Aufbereitungsbericht** hat jedenfalls den **Umstand einer Wiederherstellung** von Daten sowie die **Kriterien für die erfolgte Einschränkung** von Daten festzuhalten.*" [Hervorhebungen durch Unterzeichnerin].

Schließlich enthält § 115i der österreichischen Strafprozessordnung detaillierte gesetzliche Vorgaben für die Datenauswertung und Verfahrensvorschriften:

*„(1) Die Staatsanwaltschaft und die Kriminalpolizei können Suchparameter zum Zweck der Auswertung des Ergebnisses der Datenaufbereitung (§ 109 Z 2d) festlegen. Die **Suchparameter** und die **Anzahl der durch diese erzielten Suchtreffer** sind im Akt zu **dokumentieren**. Die Staatsanwaltschaft hat diejenigen Ergebnisse der Auswertung zu den Akten zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§ 115j Abs. 1, § 144, § 157 Abs. 2).*"

(2) Der Beschuldigte und das Opfer haben das Recht, die Auswertung von Daten anhand weiterer Suchparameter zu beantragen (§ 55). Der Person, deren Datenträger und Daten beschlagnahmt wurden, ist zu ermöglichen, die Ergebnisse der Datenaufbereitung (§ 109 Z 2e) einzusehen; anderen Personen steht eine solche Einsichtnahme nicht zu.

(3) Auf Antrag des Beschuldigten sind weitere Ergebnisse der Auswertung zu den Akten zu nehmen, wenn diese für das weitere Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen (§ 115j Abs. 1, § 144, § 157 Abs. 2).

(4) Bei der Auswertung von Daten sind die ***Persönlichkeitsrechte*** *soweit wie möglich* ***zu wahren****; die Auswertung ist auf das* ***unvermeidbare Maß zu beschränken****. Die von der Auswertung der Daten betroffenen Personen haben das Recht, das Ergebnis der Auswertung von Daten insoweit einzusehen, als ihre Daten betroffen sind. Über dieses und das ihnen nach Abs. 5 zustehende Recht hat die Staatsanwaltschaft diese Personen, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist, zu informieren.*“ [Hervorhebungen durch Unterzeichnerin].

(2) Verstoß gegen unionsrechtliche Maßstäbe

Ein auf die §§ 94 ff. StPO gestützter Datenzugriff verstößt gegen unionsrechtliche Maßstäbe, insbesondere gegen die vom Europäischen Gerichtshof in seinem Urteil vom 4. Oktober 2024 (Az. C 548/21) aufgestellten Anforderungen an eine hinreichend bestimmte Ermächtigungsgrundlage und der Wahrung der Verhältnismäßigkeit,

EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830.

(a) Beurteilungsmaßstab des Bundesverfassungsgerichts

Bei der verfassungsgerichtlichen Prüfung einer Grundrechtsverletzung sind die unionsrechtlichen Maßstäbe zum Schutzniveau der Grundrechte aus der Charta der Europäischen Union (nachfolgend GRCh) mitzuberücksichtigen, soweit der Anwendungsbereich des Unionsrechts eröffnet ist.

Ein auf die §§ 94 ff. StPO gestützter Datenzugriff auf ein beschlagnahmtes Mobiltelefon unterfällt dem Anwendungsbereich der JI-Richtlinie. Diese gilt gem. ihrem Art. 1 Abs. 1 für die Verarbeitung personenbezogener Daten durch zuständige Behörden zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Der Begriff der „Verarbeitung“ ist nach Art. 3 Nr. 2 der JI-Richtlinie weit gefasst und umfasst unter anderem das Auslesen, Abfragen oder jede andere Form der Bereitstellung personenbezogener Daten. Der Europäische Gerichtshof stellt in seiner Rechtsprechung ausdrücklich klar, dass bereits der Versuch eines Zugriffs auf die Daten eines Mobiltelefons zum Zwecke der Strafverfolgung unter den Begriff der Verarbeitung fällt,

> vgl. EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 72 ff.; für einen auf die §§ 94 ff. StPO gestützten Datenzugriff so auch BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 29 ff., 45, 49 ff.

Zwar prüft das angerufene Gericht innerstaatliches Recht und dessen Anwendung grundsätzlich auch dann am Maßstab der Grundrechte des Grundgesetzes, wenn es im Anwendungsbereich des Unionsrechts liegt, dabei aber durch dieses nicht vollständig determiniert ist. Das ergibt sich schon aus Art. 1 Abs. 3, Art. 20 Abs. 3 und Art. 93 Abs. 1 Nr. 4a GG,

> BVerfG, Beschluss vom 6. November 2019 - 1 BvR 16/13 -, NJW 2020, 300 (301 Rn. 42).

Doch bedeutet die primäre Anwendung der Grundrechte des Grundgesetzes dabei nicht, dass insoweit die Grundrechtecharta ohne Berücksichtigung bleibt. Der Einbettung des Grundgesetzes wie auch der Charta in gemeinsame europäische Grundrechtsüberlieferungen entspricht es vielmehr, dass auch die Grundrechte des Grundgesetzes im Lichte der Charta auszulegen sind,

> BVerfG, Beschluss vom 6. November 2019 - 1 BvR 16/13 -, NJW 2020, 300 (301 Rn. 46, 303 Rn. 60).

Nach den Grundsätzen der Völker- und Europarechtsfreundlichkeit des Grundgesetzes, wie sie sich aus der Präambel sowie aus Art. 1 Abs. 2, Art. 23 Abs. 1, Art. 24, Art. 25, Art. 26, Art. 59 Abs. 2 GG ergeben, stellt das Grundgesetz die Auslegung der Grundrechte und die

Fortentwicklung des Grundrechtsschutzes in die Entwicklung des internationalen Menschenrechtsschutzes und insbesondere in die europäische Grundrechtstradition,

> BVerfG, Beschluss vom 6. November 2019 - 1 BvR 16/13 -, NJW 2020, 300 (303 Rn. 61 m.w.N.); stRspr.

Es ist dafür Sorge zu tragen, dass das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird, nicht beeinträchtigt wird. Dies ist bei der verfassungsgerichtlichen Kontrolle am Maßstab der Grundrechte zu berücksichtigen,

> BVerfG, Beschluss vom 6. November 2019 - 1 BvR 16/13 -, NJW 2020, 300 (301 f. Rn. 48).

(b) Anforderungen des Europäischen Gerichtshofs aus seiner „Bezirkshauptmannschaft Landeck“-Entscheidung

In seiner „Bezirkshauptmannschaft Landeck“-Entscheidung vom 4. Oktober 2024 - C 548/21 - entwickelt der Europäische Gerichtshof unionsrechtlich zwingende Anforderungen an die Vereinbarkeit des Datenzugriffs auf Mobiltelefone zur Strafverfolgung aus den Vorgaben der JI-Richtlinie hinsichtlich der Ausgestaltung der Rechtsgrundlage zur Rechtfertigung eines Eingriffs in Art. 7 und Art. 8 GRCh,

> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830.

In dieser Entscheidung stellt der Europäische Gerichtshof klar, dass eine gesetzliche Grundlage, die den Datenzugriff auf Mobiltelefone ermöglicht, nur dann einen Eingriff in die Art. 7 und Art. 8 GRCh rechtfertigen kann, wenn sie dem in Art. 4 Abs. 1 lit. c JI-Richtlinie angelegten Grundsatz der Datenminimierung entspricht, der im Lichte dieser Grundrechte auszulegen ist und im Einklang mit Art. 52 Abs. 2 GRCh stehen muss,

> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 81 ff.

Art. 7 und Art. 8 GRCH stehen in engem sachlichem Zusammenhang und sind soweit sich ihre Gewährleistungsbereiche berühren, gemeinsam und im Lichte der Rechtsprechung des EGMR zu Art. 8 EMRK anzuwenden,

> *Kingreen*, in: Calliess/Ruffert/Kingreen, 6. Aufl. 2022, EU-GRCharta Art. 8, Rn. 2,5; EuGH, Urteil vom 09. November 2010, Rs. C-92/09 und 93/09, Sig. 2010, 1-1117, Rn. 47.

Der Schutzbereich des Grundrechts auf Privatleben aus Art. 7 GRCh erstreckt sich auf die Freiheit der einzelnen Person, über die Gestaltung ihres persönlichen Lebens selbst zu entscheiden und darüber zu befinden, ob und in welchem Umfang dieses der Öffentlichkeit zugänglich gemacht wird. Eine zentrale Ausprägung dieses Schutzes ist das Grundrecht auf den Schutz personenbezogener Daten gem. Art. 8 GRCh, der sich insbesondere auf die Kontrolle über die eigenen personenbezogenen Daten erstreckt,

> *Kingreen*, in: Calliess/Ruffert/Kingreen, 6. Aufl. 2022, EU-GRCharta Art. 7, Rn. 3, 5, Art. 7 Rn. 10.

Die Datenauswertung stellt grundsätzlich einen schwerwiegenden, im Einzelfall besonders schwerwiegenden Eingriff in Art. 7, 8 GRCh dar. Der Zugriff auf die im Mobiltelefon gespeicherten Daten erlauben den Ermittlungsbehörden die Auswertung von Daten, die potentiell einen umfassenden Einblick und

> „*genaue Schlüsse auf das Privatleben der betroffenen Person zulassen*“,
>
> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 93; sowie bestätigend BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876 Rn. 33.

Ein besonders schwerwiegender Eingriff liegt vor, wenn besonders sensible personenbezogene Daten, die in Art. 10 der JI-Richtline mit besonderem Schutz bedacht werden, vom Zugriff bzw. Zugriffsversuch betroffen sind. Dies sind etwa solche von denen auf „rassische oder ethnische Herkunft, politische Meinungen und religiöse oder weltanschauliche Überzeugungen“ geschlossen werden kann,

EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 94; EuGH, Urteil vom 22. Juni 2021 - C-439/19 -, EU:C:2021:504, Rn. 74.

Nach der ständigen Rechtsprechung des Europäischen Gerichtshofs müssen bei solchen Grundrechtseinschränkungen die Anforderungen des Art. 52 Abs. 1 GRCh eingehalten, insbesondere der Grundsatz der Verhältnismäßigkeit gewahrt werden. Zu den Anforderungen führt das Gericht aus, dass

> „[n]*ach diesem Grundsatz* […] *Einschränkungen nur vorgenommen werden [dürfen], wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Sie müssen sich auf das absolut Notwendige beschränken, und die Regelung, die die fraglichen Einschränkungen enthält, muss klare und präzise Regeln für ihre Tragweite und ihre Anwendung vorsehen*“,
>
> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 84 f. m.w.N, 98 m.w.N.

In diesem Zusammenhang hat der Europäische Gerichtshof für eine gesetzliche Grundlage, die einen behördlichen Datenzugriff auf sichergestellte Mobiltelefone erlaubt, die spezifische Anforderung aufgestellt, dass

> „*der nationale Gesetzgeber die zu berücksichtigenden Gesichtspunkte**, insbesondere die Art oder die Kategorien der betreffenden Straftaten**, hinreichend präzise definieren [muss]*“ [Hervorhebungen durch Unterzeichnerin],
>
> EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 99.

Zu diesen Gesichtspunkten gehören,

> „*u. a. die Schwere der damit verbundenen Einschränkung der Ausübung der in Rede stehenden Grundrechte, die von der Natur und der Sensibilität der Daten abhängt, zu*

denen die zuständigen Polizeibehörden Zugang erlangen können, die Bedeutung des mit dieser Einschränkung verfolgten, dem Gemeinwohl dienenden Ziels, die Verbindung zwischen dem Eigentümer des Mobiltelefons und der in Rede stehenden Straftat oder die Relevanz der fraglichen Daten für die Feststellung des Sachverhalts“,

EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 90.

Ferner bedarf es nach der Rechtsprechung des Europäischen Gerichtshofs grundsätzlich einer dem Datenzugriff vorgelagerten unabhängigen Kontrolle. Dabei geht aus den Ausführungen des EuGH hervor, dass sich die vorherige Entscheidung durch ein Gericht oder eine unabhängige Verwaltungsstelle nicht lediglich auf die Beschlagnahme beziehen darf, sondern eigenständig (auch) den Datenzugriff und dessen Reichweite selbst umfassen muss. Der Europäische Gerichtshof führt dazu aus:

„Um namentlich sicherzustellen, dass der Grundsatz der Verhältnismäßigkeit in jedem Einzelfall durch eine Gewichtung aller relevanten Gesichtspunkte gewahrt wird, ist es von ***wesentlicher Bedeutung****, dass der Zugang der zuständigen nationalen Behörden zu personenbezogenen Daten, wenn er die Gefahr eines schwerwiegenden oder sogar besonders schwerwiegenden Eingriffs in die Grundrechte der betroffenen Person mit sich bringt, von einer* ***vorherigen Kontrolle durch ein Gericht*** *oder* ***eine unabhängige Verwaltungsstelle*** *abhängig gemacht wird.*

Diese vorherige Kontrolle setzt voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle über alle Befugnisse verfügt und alle Garantien bietet, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden berechtigten Interessen und Rechte in Einklang gebracht werden. Speziell im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass das Gericht oder die Stelle in der Lage ist, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen.

*Diese unabhängige Kontrolle muss in einer Situation wie der oben in Rn. 102 beschriebenen **vor jedem Versuch**, **Zugang zu den betreffenden Daten zu erlangen**, **erfolgen**, außer in hinreichend begründeten Eilfällen, in denen die Kontrolle kurzfristig erfolgen muss. Eine spätere Kontrolle würde es nämlich nicht ermöglichen, dem Ziel der vorherigen Kontrolle zu entsprechen, das darin besteht, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten gewährt wird.*

*Insbesondere müssen Gerichte oder unabhängige Verwaltungsstellen, die im Rahmen einer vorherigen Kontrolle im Anschluss an **einen mit Gründen versehenen Zugangsantrag** tätig werden, der in den Anwendungsbereich der Richtlinie 2016/680 fällt, befugt sein, diesen **Zugang zu verweigern oder einzuschränken**, wenn sie feststellen, dass der mit ihm verbundene Eingriff in die Grundrechte unter Berücksichtigung aller relevanten Gesichtspunkte unverhältnismäßig wäre.*

Der Zugang zu den auf einem Mobiltelefon gespeicherten Daten durch die zuständigen Polizeibehörden muss daher verweigert oder eingeschränkt werden, wenn unter Berücksichtigung der Schwere der Straftat und der Erfordernisse der Untersuchung ein Zugang zum Inhalt der Kommunikationen oder zu sensiblen Daten nicht gerechtfertigt erscheint“ [Hervorhebungen durch die Unterzeichnerin],

EuGH, Urteil vom 4. Oktober 2024 - C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 102 ff.

(c) Verstoß gegen die unionsrechtlichen Anforderungen

Die §§ 94 ff. StPO genügen nicht den unionsrechtlichen Anforderungen an eine hinreichend bestimmte Ermächtigungsgrundlage und den Gesetzesvorbehalt, um einen Datenzugriff auf beschlagnahmte Mobiltelefone rechtfertigen zu können.

Zum einen fehlt es in den §§ 94 ff. StPO an den vom Europäischen Gerichtshof geforderten, hinreichend präzise zu definierenden Kriterien, anhand die Verhältnismäßigkeit im Einzelfall zu beurteilen ist. Insbesondere fehlt es an der expliziten Aufzählung bzw. Kategorisierung von Straftaten, deren Verdacht einen Datenzugriff ermöglichen kann. Für einen Zugriff auf Daten

und deren Auswertung im Rahmen der §§ 94 ff. StPO reicht eine einfacher Anfangsverdacht bezüglich einer beliebigen Straftat sowie Ordnungswidrigkeiten (dazu oben **B.I.**).

Zwar hat der Bundesgerichtshof in seiner jüngsten Entscheidung zu einem Datenzugriff auf beschlagnahmte Datenträger keine Unvereinbarkeit der §§ 94 ff. StPO mit der Rechtsprechung des Europäischen Gerichtshofs gesehen und darauf verwiesen, dass der in Art. 52 Abs. 1 GRCh normierte Gesetzesvorbehalt grundsätzlich auch durch offen formulierte formelle Gesetze erfüllt werden kann, wenn durch die Rechtsprechung die Norm hinreichend konkretisiert sei, wie dies bei den §§ 94 ff. StPO der Fall sei,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 50.

Jedoch übersieht der Bundesgerichtshof, dass der Europäische Gerichtshof in seiner Entscheidung die allgemeinen Anforderungen an den Gesetzesvorbehalt für Datenzugriffe verschärft (dazu bereits oben **(1)(dd)**): Er verlangt ausdrücklich, dass der **Gesetzgeber** „Art oder die Kategorien der betreffenden Straftaten, hinreichend präzise definieren“ muss,

EuGH, Urteil vom 4. Oktober 2024 - C 548/21 -, C.G., ECLI:EU:C:2024:830, Rn. 99.

Diese zentrale Anforderung hat der Bundesgerichtshof in der oben benannten Entscheidung gänzlich übergangen und die Maßstäbe des Europäischen Gerichtshofs weder vollständig noch zutreffend angewandt.

Ferner mangelt es an einem vom Europäischen Gerichtshof als notwendig erachteten Gerichtsvorbehalt hinsichtlich des Datenzugriffs und der anschließenden Auswertung (dazu bereits oben **(1)(dd)**). Insoweit, als die §§ 94 ff. StPO einen gerichtlichen Beschluss für die Beschlagnahme anordnen, entspricht dies nicht den Vorgaben des Europäischen Gerichtshofs zur gesonderten vorherigen Überprüfung des Datenzugriffs durch eine unabhängige Stelle.

Der in § 98 Abs. 1 S. 1 StPO vorgesehene Gerichtsvorbehalt bezieht sich seinem Wortlaut nach ausschließlich auf die Anordnung der Beschlagnahme und enthält regelmäßig weder eine Aussage zur Zulässigkeit und Reichweite eines nachgelagerten Datenzugriffs und der anschließenden Datenauswertung noch eine Definition des Zwecks sowie keine Anweisung zur Art der

technischen Durchführung. Eine gerichtliche Kontrolle, die sich allein darauf beschränkt, die Beschlagnahme eines Datenträgers als Ganzes – mitsamt aller darauf gespeicherten Daten – anzuordnen bzw. zu bestätigen oder die Anordnung bzw. Bestätigung zu verweigern, verfehlt ihre Funktion als grundrechtlicher Schutzmechanismus. Es mangelt somit an einer gesetzlichen Verankerung, die den Schutz des Betroffenen vor einem (besonders) schweren Eingriff in Art. 7 und Art. 8 GRCh durch eine vorherige Überprüfung durch eine unabhängige Stelle sicherstellt.

Angesichts der weitgehenden Übereinstimmung des vorliegenden Sachverhalts mit demjenigen der Entscheidung der Bezirkshauptmannschaft Landeck ist von einer geklärten Rechtslage im Sinne eines acte éclairé auszugehen,

> vgl. zur ständigen Rechtsprechung zu acte éclairé auch: EuGH, verb. Rs. 28/62-30/62 (Da Costa), Slg. 1963, 31; EuGH, Rs. 66/80 (ICC), Slg. 1981, 1191; EuGH, Rs. C-337/95 (Parfums Christian Dior), Slg. 1997, I-6013; EuGH, Rs. C-421/06 (Fratelli Martini), Slg. 2007, I-152.

Daraus folgt, dass hinsichtlich der unionsrechtlichen Anforderungen an eine hinreichend bestimmte Ermächtigungsgrundlage für durch Strafverfolgungsbehörden erfolgende Datenzugriffe auf beschlagnahmte Mobiltelefone kein Auslegungsspielraum mehr besteht. Die vom Europäischen Gerichtshof aufgestellten Maßstäbe sind daher zwingend bei der verfassungsrechtlichen Bewertung der Bestimmtheit und Verhältnismäßigkeit entsprechender Ermächtigungsgrundlagen zu berücksichtigen.

(3) Fehlender Kernbereichsschutz

Für den im Rahmen der §§ 94 ff. StPO durchgeführten Datenzugriff fehlen gesetzliche Schutzvorkehrungen für den absolut geschützten Kernbereich privater Lebensgestaltung, die bei derart schwerwiegenden Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verfassungsrechtlich geboten sind.

Der Kernbereich privater Lebensgestaltung wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten i.V.m Art. 1 Abs. 1 GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1786 Rn. 120).

Er erfasst insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger*innen, Ärzt*innen, Geistliche und enge persönliche Freund*innen zählen,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1786 Rn. 121).

Der Schutz beschränkt sich jedoch nicht auf reine Kommunikationsakte, sondern alle Arten höchstpersönlicher Informationen,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, NJW 2016, 1781 (1787 Rn. 124 f.).

So können dem Bundesverfassungsgericht zufolge auch elektronische Dateien, in denen höchstpersönlicher Inhalt gespeichert ist, wie etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente sowie schriftliche Verkörperungen des höchstpersönlichen Erlebens einen solchen absoluten Schutz genießen,

BVerfGE 120, 274 (335 f. m.w.N.); so auch *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 2023, 1070 (1072); für Zugriffe auf nach § 48 Abs. 3 AufenthG sichergestellte Datenträger auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60.

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden,

BVerfGE 109, 279 (314); BVerfGE 120, 274 (339); stRspr.

Das Bundesverfassungsgericht hat für staatliche Überwachungsmaßnahmen, die mit einer besonders hohen Eingriffsintensität einhergehen, besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung gestellt, die zwingend einzuhalten sind. Die besondere Intensität eines solchen Eingriffs wird gerade durch die höchstpersönliche Natur der erhobenen Daten begründet, die sich insbesondere auch aus deren Verknüpfung ergibt,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1794 Rn. 210).

So hat es in seinen Entscheidungen zu geheimen Überwachungsmaßnahmen entschieden, dass die gesetzliche Grundlage dem Kernbereichsschutz zwingend auf zwei Ebenen Rechnung tragen muss. Erstens sind auf der Ebene der Datenerhebung Vorkehrungen im Sinne einer vorgelagerten Prüfung zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zweitens sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren,

vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 126); BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (347 Rn. 108).

Der Gesetzgeber kann zwar den Schutz des Kernbereichs privater Lebensgestaltung in Abhängigkeit von der Art der Befugnis und deren Nähe zum absolut geschützten Bereich privater Lebensgestaltung für verschiedene Überwachungsmaßnahmen verschieden ausgestalten. Er hat hierbei jedoch stets auf beiden Ebenen Vorkehrungen zu treffen,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 127).

Aus der Rechtsprechung des Bundesverfassungsgerichts ergibt sich, dass sich seine Anforderungen an gesetzliche Vorkehrungen zum Kernbereichsschutz nicht nur auf geheime

Überwachungsmaßnahmen beschränkt. So hat es explizit festgestellt, dass der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung beanspruche. Sobald eine Überwachungsmaßnahme typischerweise zur Erhebung kernbereichsrelevanter Daten führt, müsse der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten. Lediglich außerhalb solcher verletzungsgeneigten Befugnisse sei eine ausdrückliche Regelung nicht erforderlich,

> vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 123); BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (347 Rn. 108).

Das entscheidende Kriterium ist demnach die Verletzungsgeneigtheit einer staatlichen Maßnahme, d.h. die Qualität und Quantität der von der Maßnahme erfassten Daten; es kommt dabei nicht darauf an, ob sie heimlich oder offen erfolgt,

> so auch *El-Ghazi*, Beschlagnahme und Auswertung von Handys, Laptops & Co., NJW-Beil 2024, 46 (49 Rn. 16) und *Schneider*, Kernbereich privater Lebensgestaltung, JuS 2021, 29 (33); für die „offene" Datenauslesung und -auswertung nach dem Aufenthaltsgesetz so auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60.

Wie bereits oben umfassend ausgeführt, ist es nach einer Beschlagnahme nach § 94 Abs. 1, Abs. 2 StPO möglich, auf alle Daten zuzugreifen, die auf den beschlagnahmten Datenträgern vorhanden sind (dazu oben **bb.** und **cc.(1)(bb)**). Insbesondere enthalten Mobiltelefone typischerweise Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind (Kommunikationsinhalte, tagebuchartige Aufzeichnungen, intime Bilder und Videos etc.). Auch kann das Surfverhalten im Internet und die Nutzung von Apps Aufschluss über höchst sensible Daten wie politische oder sexuelle Vorlieben der betroffenen Personen sowie gesundheitsrelevante Daten geben,

> so auch *Hiéramente*, Umgang mit Smartphones im Strafprozess: Überlegungen zu den Reformideen des 74. Deutschen Juristentags 2024, StV 2024, 611 (616).

Das angerufene Gericht ging bereits in seiner Grundsatzentscheidung von 2008 davon aus, dass die betroffenen Personen

> „*das System [also das Handy etc.] dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartiger Aufzeichnungen oder privater Film- oder Tondokumente, anzulegen und zu speichern. Derartige Dateien können aber […] einen absoluten Schutz genießen*“,
>
> BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris, Rn. 272.

Etwas anderes kann allenfalls dann gelten, wenn auszuschließen ist, dass auch kernbereichsrelevante Informationen erfasst werden,

> vgl. *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 85 in Bezug auf BVerfG, Beschluss vom 16. Juni 2009, - 2 BvR 902/06 -, NJW 2009, 2431 (2436 f. Rn. 90).

Das ist beim Auslesen von komplexen IT-Geräten – insbesondere von Smartphones – gerade nicht der Fall.

Schließlich ist darauf hinzuweisen, dass der Gesetzgeber im Aufenthaltsrecht und Asylrecht selbst davon ausgegangen ist, dass eine auf diese Gesetze gestützte Datenauswertung von sichergestellten Datenträgern gesetzliche Regelungen zum Kernbereichsschutz bedarf. So hat er bei der Einführung bzw. Neufassung der § 48 Abs. 3b AufenthG und § 15a Abs. 2 AsylG jeweils in den Sätzen 2 – 5 festgelegt:

> „*Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch das Auswerten von Datenträgern allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch das Auswerten von Datenträgern erlangt werden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen. Die Datenträger dürfen*

nur von einem Bediensteten ausgewertet werden, der die Befähigung zum Richteramt hat.“

Zwar genügen auch diese gesetzlichen Vorgaben nicht den Anforderungen des angerufenen Gerichts an einen vorgelagerten und nachgelagerten Kernbereichsschutz; insbesondere stellt der „Volljurist*innenvorbehalt“ in § 48 Abs. 3b S. 5 AufenthG bzw. § 15a Abs. 2 S. 5 AsylG keine Sichtung der Daten durch eine unabhängige Stelle sicher,

> vgl. zu den verfassungsrechtlichen Defiziten dieser Kernbereichsregelungen ausführlich *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 53, 60; *Lehnert*, in: Huber/Mantel, Aufenthaltsgesetz/Asylgesetz, 4. Auflage 2025, § 48 Rn. 21; *Funke-Kaiser*, in: GK-AslylG, AsylG, § 15a Rn. 12; *Vasel/Heck*, KI-basierte Assistenzsysteme im Asylverfahren und ihre Verfassungskonformität, NVwZ 2024, 540 (546 f.); Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23. März 2017, S. 7; abrufbar unter: https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf (Letzter Abruf: 18. Juli 2025).

Daran zeigt sich jedoch, dass der Gesetzgeber die Gefahr eines Kernbereichseingriffs beim Datenzugriff auf sichergestellte Datenträger erkannt und auch für solche Konstellationen gesetzliche Schutzvorkehrungen für erforderlich gehalten hat.

(a) Anforderung an die Datenerhebung

Auf der ersten Ebene ist die Art der Datenerhebung so auszugestalten, dass die Erfassung von Kernbereichsdaten gar nicht erst erfolgt. Es ist zumindest vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch mit praktisch zu bewältigendem Aufwand möglich, unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen; können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt,

vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 219), BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (347 Rn. 109).

In seiner Entscheidung zur akustischen Wohnraumüberwachung hat das angerufene Gericht klargestellt, dass eine Überwachung in Situationen von vornherein unterbleiben müsse, in denen Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt wird,

BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 -, - 1 BvR 1084/99 -, NJW 2004, 999 (1003).

Auch sei schon auf Ebene der Datenerhebung der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 128).

Die §§ 94 ff. StPO enthalten keinerlei gesetzliche Vorgaben für einen vorgelagerten Kernbereichsschutz und genügen damit nicht den verfassungsrechtlichen Anforderungen,

so auch *El*-Ghazi, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 86; *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 (2726).

Die Strafverfolgungsbehörden können im Anschluss an die Beschlagnahme auf sämtliche auf dem Gerät befindlichen Daten zugreifen. In der Praxis wird insbesondere bei Smartphones der gesamte Datenbestand ausgelesen und steht zur inhaltlichen Auswertung zur Verfügung. Bereits die Möglichkeit auf alle Daten zugreifen zu können birgt eine hohe Missbrauchsgefahr. Darüber hinaus gibt es keine gesetzliche Einschränkung der Auswertung oder Differenzierung zwischen potentiell kernbereichsrelevanten und weniger sensiblen Daten oder bestimmten Datenkategorien. Die bloße Zweckbindung der Maßnahme an den Ermittlungszweck stellt dabei keine hinreichende Schutzvorkehrung dar (dazu ausführlich bereits oben **(1)(d)(bb)**).

Regelmäßig ist eine (umfassende) Durchsicht und inhaltliche Prüfung des Datenbestandes notwendig, um festzustellen, welchen Daten eine Beweisrelevanz zukommt. Dieser Vorgang geht mit der Gefahr einher, dass auch kernbereichsrelevante Inhalte zur Kenntnis genommen werden.

Zwingend erforderlich und ohne Weiteres möglich wäre eine Regelung entsprechend § 100d Abs. 1 und Abs. 3 Satz 1 StPO. Dieser enthält in seinem Abs. 1 und Abs. 3 Satz 1 gesetzliche Vorkehrungen für den vorgelagerten Kernbereichsschutz, indem er einen Datenzugriff ausschließt, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden und vorgibt, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(b) Anforderung an die Datenauswertung

Auf der zweiten Ebene der Auswertung hat der Gesetzgeber für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor der anschließenden Verwendung der Daten herausfiltert. Die Erforderlichkeit einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab. Dabei kann auf die Sichtung durch eine unabhängige Stelle umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt,

> vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 129 m.w.N.), BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (348 Rn. 117).

Für den Einsatz von Vertrauenspersonen hat das angerufene Gericht zum Kernbereichsschutz ausgeführt, dass sicherzustellen ist, dass in Zweifelsfällen eine Klärung der Kernbereichsrelevanz zumindest durch die behördlichen Datenschutzbeauftragten erfolgen müsse,

BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (349 Rn. 119).

Darüber hinaus stellt das angerufene Gericht die Anforderung auf, dass der Gesetzgeber vorzusehen habe, dass Informationen, die in irgendeiner Weise in Schrift, Bild, Ton oder auf sonstige Weise festgehalten worden seien und sich dann als kernbereichsrelevant erwiesen, sofort gelöscht oder sonst vernichtet und jegliche Verwendung unterlassen sowie in einer Weise dokumentiert wird, die eine spätere Kontrolle ermöglicht. Zudem müsse auch der Umstand dokumentiert werden, dass eine Überwachung in den Kernbereich vorgedrungen sei, auch wenn nichts festgehalten worden sei, und die Dokumentation müsse für die spätere gerichtliche Kontrolle zur Verfügung gestellt werden,

BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781 (1787 Rn. 129); BVerfG, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 -, ZD 2023, 346 (349 Rn. 119).

Da die §§ 94 ff. StPO keine gesetzlichen Vorkehrungen enthalten, die den Schutz des Kernbereichs schon im Vorfeld gewährleisten, ist eine Sichtung durch eine unabhängige Stelle unverzichtbar. Diese fehlt hier jedoch. Der in § 98 Abs. 1 StPO vorgesehene Gerichtsvorbehalt bezieht sich lediglich auf die Anordnung der Beschlagnahme an sich und trifft keine Vorgabe dazu, dass auch die anschließende Datenauswertung durch eine unabhängige Stelle durchgeführt werden müsste. Die Durchsicht und Auswertung der Daten verbleiben vielmehr vollständig in der Hand der Strafverfolgungsbehörden. Auch enthalten weder die Strafprozessordnung noch die auf sie anwendbaren Vorschriften der BDSG ausreichende Dokumentationspflichten in Bezug auf einen auf die §§ 94 ff. gestützten Datenzugriff und der anschließenden Datenauswertung – im Allgemeinen (dazu ausführlich unter **(4)(d)**), aber auch spezifisch hinsichtlich Informationen, die dem Kernbereich zugeordnet sind.

(4) Verhältnismäßigkeit

Ein auf §§ 94 ff. StPO gestützter Datenzugriff ist unverhältnismäßig. Zwar liegt in der Strafverfolgung ein legitimer Zweck, doch begründet die besonders hohe Eingriffsintensität hohe gesetzliche Anforderungen an die Wahrung der Verhältnismäßigkeit, denen die §§ 94 ff. StPO nicht

genügen. Die Vorschriften sehen weder Beschränkungen hinsichtlich der Anlasstat vor (dazu unter **(a)**) noch enthalten sie hinreichende Vorgaben zur erforderlichen Erfolgstauglichkeit (dazu unter **(b)**) oder angemessene Verfahrensvorschriften (dazu unter **(c)**).

(a) Beschränkung der Anlasstat

Die §§ 94 ff. StPO enthalten keine tatbestandlichen Beschränkungen in Bezug auf die Anlasstat und genügen damit nicht dem Verhältnismäßigkeitsgrundsatz. Der mit einem umfassenden Datenzugriff einhergehende tiefgreifende Grundrechtseingriff steht außer Verhältnis zur Verfolgung von Straftaten, die nicht zumindest eine erhebliche Bedeutung ausweisen.

Die besonders hohe Eingriffsintensität des Datenzugriffs wirkt sich dahingehend aus, dass die Maßnahme nur zum Schutz hinreichend gewichtiger Rechtsgüter dienen darf. Das angerufene Gericht hat in seinem Urteil zum BKA-Gesetz die Zulässigkeit der dort betroffenen Ermittlungs- und Überwachungsmaßnahmen vom Gewicht der verfolgten Straftaten abhängig gemacht und – gestaffelt nach der Eingriffsintensität – den Anwendungsbereich auf die Verfolgung besonders schwerer, schwerer sowie Straftaten von zumindest erheblicher Bedeutung beschränkt,

> BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, NJW 2016, 1781, (1784 Rn. 107).

Zur Wahrung der Verhältnismäßigkeit im engeren Sinne ist jedenfalls gesetzlich sicherzustellen, dass die Maßnahme nur für den Nachweis von Straftaten von erheblicher Bedeutung bzw. im Bereich der mittleren Kriminalität beschränkt ist und damit zumindest für Bagatellstraftaten und Straftaten, die dem Bereich leichter Kriminalität zuzuordnen sind, sowie für Ordnungswidrigkeiten ausgeschlossen sind, da die Eingriffsintensität, die mit dem Datenzugriff auf komplexe IT-Geräte und den damit verbundenen Gefahren für die Betroffenen einhergeht, deutlich höher ist als die Wirkungen, die von einer Beschlagnahme anderer Gegenstände ausgehen,

> so auch *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 76; *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 283: „*Straftat von auch im Einzelfall erheblicher Bedeutung*“; für die Durchsicht nach § 110 StPO ebenso schon *Hauser*, Das IT-Grundrecht, 2015, S. 285 f.; *Drallé*, das Grundrecht auf Gewährleistung der

Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 87, 131: „*neu justieren*“; „*anheben*“; *Böckenförde*, JZ 2008, 925 (931): „*Erhöhen der Eingriffsvoraussetzungen*“; für Österreich: *Zerbes/Ghazanfari*, Öster. AnwBl 2022, 640 (648 f.); zum Begriff der Straftat von erheblicher Bedeutung siehe *Eidam*, in: Rotsch/Saliger/Tsambikakis, Strafprozessordnung, 1. Auflage 2025, § 131 Rn. 19 f. m.w.N.

Darüber hinaus wird teilweise noch eine weitergehende Einschränkung auf besonders schwere Straftaten für notwendig erachtet und dies mit der Vergleichbarkeit der Eingriffsintensität mit verdeckten Überwachungsmaßnahmen wie die Online-Durchsuchung nach § 100b StPO und die Telekommunikationsüberwachung nach § 100a StPO begründet (dazu bereits ausführlich oben **(bb.(5)**),

Bäcker, in: FS Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, 2009, S. 1 (25 f.); *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 199; *Hermann*, Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 140 f.: „*Begrenzung auf schwere Straftaten und Delikte*“; *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 Rn. 3 (2727 Rn. 11); *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 201.

Eine verfassungsgemäße Regelung könnte sich für die Zulässigkeit der Maßnahme an dem jeweiligen Höchststrafrahmen orientieren. Der Datenzugriff könnte etwa für die Verfolgung von Straftaten ausgeschlossen werden, die einen Höchststrafrahmen von unter 5 Jahren haben,

dazu ausführlich *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 77 ff.

Dies wäre auch im Einklang mit der verfassungsgerichtlichen Rechtsprechung zur Einstufung von Straftaten nach ihrer Schwere. So seien dem angerufenen Gericht zufolge Straftaten, die „*im Höchstmaß mit Freiheitsstrafe unter fünf Jahren bedroht“* seien, nicht mehr *„ohne weiteres“* der mittleren Kriminalität zuzurechnen, wie das unerlaubte Entfernen vom Unfallort (§ 142 StGB), die § 185 ff. StGB oder die fahrlässige Körperverletzung (§ 229 StGB),

BVerfE 124, 43 (64).

(b) Qualifizierte Beweisrelevanz

Darüber hinaus fehlen in den §§ 94 ff. StPO hinreichende gesetzliche Vorgaben zur erforderlichen Erfolgstauglichkeit, die geeignet sind, die Wahrung der Verhältnismäßigkeit zu gewährleisten. Aufgrund der hohen Eingriffsintensität und der hohen Anfälligkeit der Beschlagnahme von komplexen IT-Geräten wie Smartphones ist eine über die einfache Beweisrelevanz hinausgehende Erfolgswahrscheinlichkeit verfassungsrechtlich geboten.

Um eine Ermittlungsmaßnahme nach den §§ 94 ff. StPO zu ergreifen, reicht es bereits aus, wenn der betroffene Gegenstand für die Untersuchung von Bedeutung sein kann (sog. einfache Beweisrelevanz). Diese liegt bereits vor, wenn allein bei einer ex ante-Betrachtung die nicht fernliegende Möglichkeit besteht, dass der Gegenstand im weiteren Verfahren zu Beweiszwecken verwendet werden kann,

> BVerfG, Beschluss vom 1. Oktober 1987 - 2 BvR 1178/86 - u. a., NJW 1988, 890 (894); BVerfG, Beschluss vom 16. August 1994 - 2 BvR 983, 1258/94 -, NJW 1995, 385; BGH, Beschluss vom 5. Januar 1979 - 1 BJs 226/78/StB -, - 246/78 -, NStZ 1981, 94.

Dabei reicht die Möglichkeit, dass der beschlagnahmte Gegenstand als Untersuchungsgegenstand verwendet werden kann; für welche Beweisführung es im Einzelnen in Betracht kommt, muss noch nicht feststehen,

> LG Hamburg, Beschluss vom 23. April 2020 - 620 Qs 1/20 -, BeckRS 2020, 15128 Rn. 16.

Aufgrund des umfangreichen und vielschichtigen Datenbestandes auf IT-Geräten liegt regelmäßig eine einfache Beweisrelevanz vor, was auch eine hohe Anfälligkeit für Beschlagnahme begründet, insbesondere bei Mobiltelefonen, die betroffene Personen in der Regel überall mit sich führen. Insbesondere bei komplexen IT-Geräten verliert die Eingriffsvoraussetzung der Beweisrelevanz damit letztlich ihre eingrenzende Wirkung und wird funktionslos,

> *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 21 f., C 80.

So kann etwa aufgrund gespeicherter Standortdaten, dem potentiellen Vorliegen von Kommunikationsinhalten über die Begehung oder Planung einer Straftat oder möglichen Aufzeichnungen darüber oder der im Mobiltelefon gespeicherten Suchhistorie im Webbrowser in den allermeisten Fällen aus ex-ante Sicht eine einfache Beweisrelevanz bejaht werden.

Daher ist es verfassungsrechtlich geboten, gesetzlich höhere Hürden an die Beweisrelevanz vorzusehen, um die Verhältnismäßigkeit abzusichern. Nur dadurch lässt sich eine (drohende) „Entgrenzung der Ermittlungsmaßnahme“ einfangen und der Gefahr von Ausforschungsmaßnahmen sowie einer missbräuchlichen Suche nach Zufallsfunden entgegenwirken,

> *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 80 f.; so auch *Heinson*, IT-Forensik, 2015, S. 204 f.; *von zur Mühlen*, Zugriff auf elektronische Kommunikation, 2019, S. 429; für die Durchsicht nach § 110 StPO vgl. *Rühs*, Durchsicht informationstechnischer Systeme, 2022, S. 286.

Gleichzeitig wird damit der Gefahr von Beschlagnahmen ins Blaue hinein, also Ausforschungsmaßnahmen, entgegengetreten,

> *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 81 f.

Eine gesetzliche Regelung zur Anhebung der Eingriffsschwelle erfordert eine „konkrete fallbezogene Erfolgstauglichkeit“ der Maßnahme wie etwa in den § 103 Abs. 1 Satz 1 und § 163d Abs. 1 Satz 1 StPO festgelegt. Dies bedeutet, dass tatsächliche Anhaltspunkte vorliegen müssen, die die Annahme rechtfertigen, dass durch die Durchführung der Maßnahme der verfolgte Zweck erreicht werden kann,

> *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 81 m.w.N.; näheres zur Erfolgstauglichkeit im Rahmen des § 103 Abs. 1 Satz 1 StPO vgl. *Hegmann*, in: BeckOK StPO mit RiStBV und MiStra, Graf, 55. Edition, Stand: 01. April 2025, § 103 Rn. 8; zur Erfolgstauglichkeit im Rahmen des § 163d Abs. 1 S. 1 StPO vgl. *Moldenhauer*, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage 2023, § 163d Rn. 15.

Auch der vom österreichischen Nationalrat neu eingeführte § 115 f. österreichische Strafprozessordnung enthält in seinem Absatz 1 in Bezug auf die Beweisrelevanz diese Strukturmerkmale:

> „*(1) Die Beschlagnahme von Datenträgern und Daten ist zulässig, wenn sie* ***aus Beweisgründen erforderlich scheint*** *und aufgrund* ***bestimmter Tatsachen*** *anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat* ***wesentlich*** *sind.*“ [Hervorhebungen durch Unterzeichnerin],
>
> § 115 f. Abs. 1 österreichische Strafprozessordnung in der Fassung vom 5. Februar 2025, BGBl. Nr. 631/1975 zuletzt geändert durch BGBl. I Nr. 157/2024, abrufbar unter: https://ris.bka.gv.at/eli/bgbl/1975/631/P115f/NOR40267211?Sort=1%7cDesc&Abfrage=Bundesnormen&FassungVom=05.02.2025 (Letzter Abruf: 18. Juli 2025).

(c) Keine Wahrung der Verhältnismäßigkeit durch Beachtung des Verhältnismäßigkeitsgrundsatzes im Einzelfall

Die Berücksichtigung des allgemeinen Verhältnismäßigkeitsgrundsatzes im Einzelfall ist nicht ausreichend, um die Wahrung der Verhältnismäßigkeit sicherzustellen. Das ergibt sich bereits aus der Wesentlichkeitstheorie sowie dem Gebot der Bestimmtheit und Normenklarheit (dazu oben **(1)(a)** und **(1)(d)(cc)**). Darüber hinaus ergibt sich dies aus dem Umstand, dass sich die Wahrung des Verhältnismäßigkeitsgrundsatzes bei der Beschlagnahme eines mit einer Zugangssperre versehenden Datenträgers in der Beurteilung erschöpft, ob eine Beschlagnahme des Geräts als Ganzes vorzunehmen ist oder nicht. Nicht erwogen werden hingegen Aspekte des Datenzugriffs und der Datenauswertung als solche. Denn in aller Regel wird nur zu prüfen sein, ob ein Anfangsverdacht vorliegt und der konkrete Beweis auch auf andere Weise erhoben werden kann als durch die Beschlagnahme des Datenträgers. Ist dies nicht der Fall, ist der Datenträger zu beschlagnahmen und es kann nach der Entsperrung auf den gesamten Datenbestand zugegriffen werden. Damit realisieren sich bereits die Gefahren für die Vertraulichkeit und Integrität der betroffenen Datenträger (dazu oben **1.b.**).

Zudem reicht auch der Gerichtsvorbehalt aus § 98 Abs. 1 StPO nicht aus, die Verhältnismäßigkeit des Datenzugriffs und der anschließenden Auswertung im Einzelfall zu wahren. Der

gerichtliche Anordnungs- bzw. Bestätigungsbeschluss erfolgt allein zu Beginn der Beschlagnahme. Der Datenzugriff und die Auswertung sind dieser nachgelagert und erfolgen – mit teils erheblichem zeitlichen Verzug – eigenständig durch die Strafverfolgungsbehörden, ohne dass dies einer weiteren vorherigen gerichtlichen Überprüfung oder Vorgaben unterliegt (dazu oben **B.I.2.** und **(2)(c)**). Dies begründet eine hohe Missbrauchsgefahr wie auch der vorliegende Fall exemplarisch zeigt: Es wurde eine Vielzahl an Daten ausgewertet, die in keinerlei Bezug zum Strafvorwurf standen und umfassende Informationen über politischen Einstellungen, Aktivitäten sowie Zugehörigkeiten des Beschwerdeführers zur Kenntnis genommen, bewertet und dokumentiert.

Auch kann die Verhältnismäßigkeit im Einzelfall nicht stets durch eine vorherige Datendurchsicht nach § 110 Abs. 1, Abs. 3 StPO gewahrt werden. Zwar hat das angerufene Gericht Letzteres als milderes, gleich geeignetes Mittel eingestuft, dass zwingend vor der endgültigen Beschlagnahme erfolgen müsse,

> BVerfG, Beschluss vom 12. 4. 2005 - 2 BvR 1027/02 -, NJW 2005, 1917 (1922).

Doch ist die Durchsicht nur möglich, wenn der Beschlagnahme eine Durchsuchung vorangeht (dazu oben **B.I.3.**). In Fällen, in denen eine Beschlagnahme unmittelbar durchgeführt wird, da etwa eine Durchsuchung nicht erforderlich war, um das Mobiltelefon zu finden oder nicht angeordnet wurde, ist eine vorherige Datendurchsicht nach § 110 Abs. 1, 3 StPO ausgeschlossen.

Darüber hinaus ist eine Durchsicht nach § 110 Abs. 1, 3 StPO aufgrund einer Zugangssperre oder der Datenmenge oft nicht direkt vor Ort möglich. Um eine Durchsicht durchzuführen, müsste der Datenträger zunächst mitgenommen und einbehalten werden und wenn es sich um einen verschlüsselten Datenträger handelt, forensisch entsperrt werden. Damit gehen aber dieselbe Eingriffsintensität eines solchen Zugriffs auf den gesamten Datenbestand eines Datenträgers einher wie auch bei einer Beschlagnahme; die Durchsicht ist damit – zumindest in den regelmäßigen Fällen von Verschlüsselungen und hoher Datenmengen – selbst ein gravierender Eingriff in die Persönlichkeitsrechte der Betroffenen,

> so auch *Stam*, Die strafprozessuale Beschlagnahme und Auswertung von Smartphones, JZ 2023, 1070 (1075).

Schließlich zeigt auch die gerichtliche Praxis, dass der allgemeine Verhältnismäßigkeitsgrundsatz nicht ausreichend ist, um die Verhältnismäßigkeit im Einzelfall zu gewährleisten. So haben Gerichte eine Beschlagnahme eines Mobiltelefons bereits aufgrund eines Verdachtes der Begehung einer Ordnungswidrigkeit angeordnet bzw. bestätigt,

> zum unerlaubten Fotografieren gem. Art. 83 Abs. 5 i.V.m. Art. 41 DSGVO vgl. AG Hamburg, Beschluss vom 3. Juli 2020 - 163 Gs 656/20 -, juris, Rn. 2 f.; zur unerlaubten Handynutzung im Verkehr nach §§ 49 Abs. 1 Nr. 22, 23 Abs. 1a StVO vgl. AG Pirna, Beschluss vom 05. Februar 2020 - 23 Gs 66/20 -, BeckRS 2020, 5134.

(d) Keine ausreichenden Dokumentationspflichten

Weiterhin bestehen keine ausreichenden verfahrensrechtlichen Vorkehrungen, die dem Eingriffsgewicht und den Anforderungen des Art. 19 Abs. 4 GG mit Blick auf Transparenz und Rechtsschutz hinreichend Rechnung tragen.

Die Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle folgen aus dem Verhältnismäßigkeitsgrundsatz,

> BVerfGE 165, 363 (412 f. Rn. 109 m.w.N.),

und ergeben sich aus dem jeweiligen Grundrecht in Verbindung mit Art. 19 Abs. 4 GG,

> BVerfGE 141, 220 (282 Rn. 134).

Um die notwendige Transparenz über den Auswertungsvorgang zu schaffen und damit auch effektiven Rechtsschutz im Sinne des Art. 19 Abs. 4 GG zu gewährleisten, ist es notwendig, dass gegenüber Beschuldigten und Verteidiger*innen offengelegt wird, welche Daten gesichtet werden. Dafür bedarf es detaillierter Protokollierungs- und Dokumentationspflichten.

Spezielle Protokollierungs- und Dokumentationspflichten sind in den §§ 94 ff. StPO nicht vorgesehen. Gem. § 500 StPO ist die Protokollierungspflicht nach § 76 BDSG anwendbar. Diese

betrifft aber nur wenige, sehr allgemeine Umstände der Datenverarbeitung (vgl. § 76 Abs. 1 BDSG). Zwar dürfen die Protokolle auch von der betroffenen Person zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung verwendet werden (§ 76 Abs. 3 BDSG), allerdings hat die betroffene Person keinen Anspruch auf Herausgabe, im Gegensatz zur Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (vgl. § 76 Abs. 5 BDSG),

Schwichtenberg, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, § 76 Rn. 9, 12.

Auch vom datenschutzrechtlichen Auskunftsanspruch nach § 57 BDSG werden Protokolldaten nicht erfasst,

Schwichtenberg, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, § 76 Rn. 9

§ 76 BDSG kann mithin keine ausreichende Transparenz gewährleisten, die es Betroffenen ermöglichen würde, nachzuvollziehen, welche Teile des Smartphones tatsächlich ausgelesen und ausgewertet werden.

Eine tatsächliche Kenntnisnahme ist regelmäßig erst im Nachhinein durch Akteneinsicht möglich. Diese ist jedoch lückenhaft, da lediglich die als ermittlungsrelevant eingestuften Daten dokumentiert werden. Aus der Akte geht weder hervor, in welchem Umfang das Gerät ausgewertet wurde, noch welche weiteren Daten zwar zur Kenntnis genommen, jedoch nicht in den Ermittlungsbericht aufgenommen wurden.

Die betroffene Person hat deshalb keine ausreichende Möglichkeit zu erfahren, auf welche Art und in welchem Umfang Daten erhoben und ausgewertet werden, und kann sich nicht effektiv gerichtlich zur Wehr setzen, sodass ein Verstoß gegen Art. 19 Abs. 4 GG vorliegt.

dd. Verfassungswidrigkeit der konkreten Maßnahme

Der Beschluss des Landgerichts Bamberg verletzt den Beschwerdeführer auch im konkreten Fall in seinem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, da der Datenzugriff sowie die Sicherung und Übermittlung des gesamten

Datenbestandes seines Mobiltelefons weder erforderlich (dazu unter **(1)**) noch angemessen (dazu unter **(2)**) waren.

Wie bereits oben ausgeführt, ist die Verhältnismäßigkeitsprüfung bei einem so schwerwiegenden Eingriff besonders sorgsam durchzuführen. Im Beschluss des Landgerichts Bamberg finden sich allein in Bezug auf die Durchführung der Beschlagnahme Erwägungen zur Verhältnismäßigkeit. Ausführungen zu Verhältnismäßigkeitserwägungen hinsichtlich des nachfolgenden Datenzugriffs, insbesondere bezüglich seines Umfangs und der Art der technischen Durchführung lassen sich hingegen gänzlich vermissen.

(1) Fehlende Erforderlichkeit

Die Maßnahme war bereits nicht erforderlich. Durch die Beschlagnahme sollte überprüft werden, ob sich auf dem Mobiltelefon des Beschwerdeführers eine Aufnahme des vermeintlich nichtöffentlich gesprochenen Wortes der Polizeibeamten befand. Der Tatvorwurf und auch das Tatmittel standen damit eindeutig fest. Es ging um eine konkrete Datei, einen begrenzten Kommunikationsausschnitt – nicht um ein umfassendes Kommunikationsnetzwerk, eine verdeckte Struktur oder andere komplexe Beweise.

Ein derart eng umgrenztes Ermittlungsziel hätte sich durch gezielte, milder ausgestaltete Maßnahmen erreichen lassen. Zu nennen sind die Sicherung einzelner (die den Tatvorwurf konkret betreffende) Audio- und Bildmaterialen vor Ort. So wäre es möglich und zumutbar gewesen, dem Beschwerdeführer zunächst eine selektive Sicherung der betreffenden Datei anzubieten – etwa durch die Übermittlung an eine offizielle behördliche Adresse per E-Mail oder eine Einsichtnahme vor Ort, ggf. unter Anwesenheit von Zeugen oder Protokollierung. Eine solche Vorgehensweise hätte die Ermittlungsbehörden in die Lage versetzt, den Sachverhalt aufzuklären, ohne einen vollständigen Zugriff auf das gesamte Mobiltelefon mit all seinen privaten und beruflichen Inhalten vorzunehmen.

Zwar hatte der Beschwerdeführer im Rahmen der Maßnahme erklärt, das Gerät nicht freiwillig herausgeben zu wollen. Dieses Verhalten war jedoch klar erkennbar auf die umfassende Sicherstellung des gesamten Geräts bezogen. Es ist nicht ersichtlich, dass sich der

Beschwerdeführer auch einer zielgerichteten, datenschutzschonenden Mitwirkung an der Sicherung der konkreten Datei verweigert hätte.

Selbst wenn eine solche Kooperation letztlich gescheitert wäre oder der Beschwerdeführer die Herausgabe der Datei verweigert hätte, hätte die Datenauslesung und -übermittlung sich auf die konkrete Sprachnotiz beschränken müssen. Technisch ist es möglich, nur bestimmte Formate (z. B. Audiodateien) aus einem bestimmten Zeitraum auszulesen oder auf bestimmte Ordner zuzugreifen. In solchen Fällen ist eine umfassende Sicherung des gesamten Datenträgers nicht erforderlich.

(2) Unangemessenheit

Jedenfalls fehlte es der Maßnahme an der Angemessenheit im engeren Sinne. Das Gewicht des Eingriffs in die Grundrechte des Beschwerdeführers steht außer Verhältnis zur geringen Bedeutung des verfolgten Straftatbestands und zum Erkenntnisgewinn der Maßnahme.

Gegenstand der Ermittlungen war ein möglicher Verstoß gegen § 201 Abs. 1 Nr. 1 StGB. Es handelt sich hierbei um ein minderschweres Ehrschutzdelikt, das regelmäßig mit Geldstrafe oder geringer Freiheitsstrafe sanktioniert wird. Die Vorschrift schützt das nichtöffentlich gesprochene Wort vor heimlicher Aufzeichnung und dient damit zwar dem Persönlichkeitsschutz, berührt jedoch keine hochrangigen Rechtsgüter wie Leib, Leben oder die Funktionsfähigkeit des Staates. Insbesondere bei dienstlicher Kommunikation von Amtsträgern im öffentlichen Raum ist das Gewicht des geschützten Interesses ohnehin reduziert,

vgl. LG Hamburg, Beschluss vom 21. Dezember 2021 - 610 Qs 37/21 jug -, juris.

Demgegenüber stand ein gravierender Eingriff: Die Sicherstellung eines gesamten Smartphones eröffnet den Ermittlungsbehörden nicht nur Zugriff auf einzelne Kommunikationsvorgänge, sondern auf die gesamte digitale Lebensrealität des Betroffenen. Die Maßnahme ermöglichte den Zugriff auf Chatverläufe, Standortdaten, Bilder, Kalender, Notizen, Passwörter, Gesundheitsdaten, berufliche Inhalte und weitere höchstpersönliche Daten – obwohl der Vorwurf lediglich eine mögliche Tonaufnahme eines Polizeigesprächs im öffentlichen Raum betraf. Die vollständige Sicherstellung und Durchsuchung eines Mobiltelefons ist ein besonders

eingriffsintensiver Akt, der das allgemeine Persönlichkeitsrecht in seinem Kernbereich berühren kann (dazu oben **c.bb.**). Das angerufene Gericht hat mehrfach betont, dass Mobiltelefone heute eine hohe Dichte an persönlichen, privaten und sensiblen Daten enthalten und daher besonders schutzbedürftig sind. Ein vollständiger Zugriff auf ein Mobiltelefon kann einer Vollausforschung der Persönlichkeit gleichkommen,

BVerfGE 120, 274 (320 ff.).

Ein derart unverhältnismäßiges Missverhältnis zwischen Tatwertigkeit und Eingriffsreichweite verletzt das verfassungsrechtlich verankerte Gebot des Übermaßverbots. Das Strafverfolgungsinteresse war im Vergleich zum Grundrechtseingriff gänzlich nachrangig. Es ist verfassungsrechtlich nicht hinnehmbar, dass zur Aufklärung eines derart geringfügigen, in tatsächlicher Hinsicht zweifelhaften Verdachts ein Grundrechtseingriff von solcher Tiefe und Reichweite vorgenommen wird. Maßnahmen mit solch schwerwiegendem Eingriffscharakter wie der Beschlagnahme von Smartphones können nur bei erheblicher Straftatenlage oder konkreter Gefahrenlage gerechtfertigt sein können (dazu bereits ausführlich oben **cc.(4)(a)(b)**).

Eine Vollzugriffsmaßnahme auf ein Smartphone zur Klärung eines bloßen Anfangsverdachts auf eine niedrigschwellige Persönlichkeitsverletzung ist mit den verfassungsrechtlichen Grundsätzen nicht vereinbar.

Die Maßnahme war damit unangemessen. Das staatliche Interesse an Strafverfolgung wog in der konkreten Konstellation deutlich weniger schwer als das Interesse des Beschwerdeführers, von einer Totaldurchleuchtung seiner persönlichen digitalen Lebenssphäre verschont zu bleiben. Die Maßnahme war unverhältnismäßig im engeren Sinne und damit verfassungswidrig.

2. Hilfsweise: Verletzung des Grundrechts auf informationelle Selbstbestimmung

Selbst wenn die erfolgte Maßnahme nicht als Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme zu werten wäre, läge jedenfalls – wie auch vom Bundesgerichtshof angenommen – ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung vor, der verfassungsrechtlich nicht gerechtfertigt werden kann,

BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 28.

Aufgrund des erheblichen Eingriffsgewichts (hierzu **a.**) ist die Maßnahme auch gemessen am Maßstab des Rechts auf informationelle Selbstbestimmung nicht gerechtfertigt. Es fehlt bereits an einer durch die besonders hohen Eingriffsintensität bedingten, hinreichend bestimmten Ermächtigungsgrundlage, die gesetzliche Vorkehrungen zum Kernbereichsschutz sowie strenge Vorgaben für die Wahrung der Verhältnismäßigkeit enthalten muss (hierzu **b.**). Auch wäre der Eingriff im konkreten Fall unverhältnismäßig.

a. Besonders hohe Eingriffsintensität

Die Kriterien zur Bewertung der Schwere eines Eingriffs in die informationelle Selbstbestimmung hat das angerufene Gericht wie folgt beschrieben:

> „*Generell wird das Gewicht eines Eingriffs in die informationelle Selbstbestimmung vor allem durch* ***Art, Umfang und denkbare Verwendung*** *der Daten sowie die* ***Gefahr ihres Missbrauchs*** *bestimmt. Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind also die Gestaltung der* ***Eingriffsschwellen****, die* ***Zahl der Betroffenen*** *und die* ***Intensität der individuellen Beeinträchtigung*** *im Übrigen. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden. Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme ebenso zur Erhöhung ihrer Intensität wie die faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist*“ [Hervorhebungen durch die Unterzeichnerin],
>
> BVerfGE165, 363 (399 f. Rn. 76) m.w.N.

Faktoren, die das Eingriffsgewicht besonders erhöhen, hat das angerufene Gericht wie folgt dargestellt:

> „*Das Eingriffsgewicht erhöht sich, wenn besonders **private Informationen** erlangt werden können. Besonders eingriffsintensiv ist auch, wenn sich das Verhalten einer Person, deren Gewohnheiten oder deren Lebensgestaltung räumlich und über längere Zeit hinweg nachvollziehen lassen, wenn also ein **Bewegungs- oder Verhaltensprofil** einer Person oder ein **umfassenderes Persönlichkeitsbild** entstehen kann (vgl. BVerfGE115, 320 [350f.]; 120, 378 [400f., 406f., 417]; 125, 260 [319f.]; 141, 220 [267 Rn. 99]; 150, 244 [284f. Rn. 100]; 162, 1 [130f. Rn. 287; 144ff. Rn. 321ff.]; 165, 1 [91f. Rn. 174f.] - Polizeiliche Befugnisse nach SOG MV). Das Eingriffsgewicht ist zudem höher, wenn die Polizei durch die Datenanalyse oder -auswertung Informationen über Personen erlangt und zum Ausgangspunkt weiterer operativer Maßnahmen macht, die **objektiv in keiner Beziehung zu einem konkreten Fehlverhalten** stehen und den polizeilichen Eingriff durch ihr Verhalten **nicht zurechenbar veranlasst** haben (vgl. dazu BVerfGE115, 320 [354f.]; 150, 244 [283 Rn. 98]), wenn also die automatisierte Aufklärungstechnik das Risiko für objektiv Unbeteiligte erhöht, Ziel weiterer polizeilicher Aufklärungsmaßnahmen zu werden (vgl. dazu BVerfGE115, 320 [351ff.]; 120, 378 [403]; 125, 260 [320])*“ [Hervorhebungen durch die Unterzeichnerin],
>
> BVerfGE165, 363 (400 f. Rn. 77).

Nach diesen Maßstäben liegt auch bezüglich des Grundrechts auf informationelle Selbstbestimmung – sowohl abstrakt als auch im konkreten Fall – ein besonders schwerwiegender Eingriff vor. Die obigen Ausführungen zur Intensität des Eingriffs in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (dazu oben **1.c.bb.**) beanspruchen nach diesen Maßstäben auch bezüglich des Grundrechts auf informationelle Selbstbestimmung Geltung: Die Beschlagnahme, Entsperrung und Auslesung eines Mobiltelefons führen – wie bereits dargestellt – zur Preisgabe eines kaum übertreffbaren Bestands persönlicher, privater und auch sensibler Daten. Aufgrund der Vielzahl und Art der auf komplexen IT-Systemen wie Smartphones gespeicherten Daten lassen sich erhebliche Rückschlüsse auf das Leben der Betroffenen ziehen. Das Verhalten der betroffenen Person, deren Gewohnheiten oder deren Lebensgestaltung lassen sich oftmals über sehr lange Zeit hinweg nachvollziehen; umfassende Bewegungs- und Verhaltensprofile sowie ein umfassendes Persönlichkeitsbild sind ebenfalls möglich. Ausgelesen wird dabei oftmals auch der Inhalt geschützter Kommunikation, beispielsweise mit Ärzt*innen, Rechtsanwält*innen oder journalistischen Quellen. Die Zahl der Betroffenen ist hoch: Betroffen sein können nicht nur alle Personen, gegen die ein einfacher Anfangsverdacht gem. § 152 Abs. 2 StPO vorliegt, sondern darüber hinaus auch viele Dritte, gegen die

nicht ermittelt wird, über die Informationen auf beschlagnahmten Geräten vorfindlich sind (siehe zu diesen Punkten bereits **1.c.bb.**).

Weder die unmittelbar von einer Beschlagnahme Betroffenen noch betroffene Dritten haben dabei für den regelmäßig erfolgenden umfassenden Zugriff einen hinreichenden Anlass gegeben: die unmittelbar Betroffenen nicht, da ihnen gegenüber regelmäßig ein gezielter, eingeschränkter Datenzugriff ausreichend wäre, Dritte nicht, da gegen sie von vornherein schon gar nicht ermittelt wird.

Allen Betroffenen drohen aufgrund der Maßnahme außerdem empfindliche weitere Nachteile. Wie auch der vorliegende Fall verdeutlicht, birgt der Zugriff auf Mobiltelefone immenses Missbrauchspotenzial. Polizeibeamte werden faktisch ermächtigt, das Privatleben betroffener Personen auszuleuchten und auf der Grundlage der gewonnenen Erkenntnisse weitere Maßnahmen, etwa erweiterte Ermittlungsmaßnahmen oder präventivpolizeiliche Maßnahmen wie Gefährderanschreiben, einzuleiten. Die Auswertung der auf einem Mobiltelefon befindlichen Daten kann also regelmäßig den Ausgangspunkt für weitere operative Maßnahmen darstellen, die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und die nicht zurechenbar veranlasst wurden. Auch das nicht maßnahmenbezogene Erstellen politischer Profile – wie es im vorliegenden Fall erfolgt ist – stellt bereits einen derartigen empfindlichen weiteren Nachteil dar, da es die Wahrscheinlichkeit weiterer polizeilicher Maßnahmen in der Zukunft erhöht. Die wachsende Verwendung automatisierter Datenauswertung steigert dieses Risikopotenzial sogar noch.

Außerdem handelt es sich um eine oftmals „faktisch heimliche“ Maßnahme, da die betroffene Person keine Möglichkeiten hat, zu erfahren, in welcher Weise und in welchem Umfang auf welche Daten zugegriffen wird, und wie diese ausgewertet wurden (dazu bereits oben **1.c.bb.(4)**). Für mittelbar betroffene Dritte ist der Eingriff sogar im Ganzen als heimlich zu qualifizieren, da sie regelmäßig überhaupt keine Kenntnis über den Zugriff auf ihre Daten erhalten (dazu bereits oben **1.c.bb.(4)**).

Wie bereits ausgeführt, hat auch der Bundesgerichtshof in seiner jüngsten Entscheidung einen solchen Datenzugriff als (im Einzelfall besonders) schwerwiegenden Eingriff eingestuft, dessen Gefahren mit der von verdeckten Überwachungsmaßnahmen wie die Online-Durchsuchung

vergleichbar ist – ohne dabei aber die damit einhergehenden, von der verfassungsrechtlichen Rechtsprechung aufgestellten strengen Maßstäbe an eine hinreichend bestimmte und verhältnismäßige Ermächtigungsgrundlage anzuwenden (dazu oben **1.c.cc.(e)**),

> BGH, Beschluss vom 13. März 2025 - 2 StR 232/24 -, BeckRS 2025, 9876, Rn. 33.

b. Verstoß gegen verfassungsrechtliche Anforderungen

(1) Verfassungsrechtlicher Maßstab

Der Rechtsprechung des angerufenen Gerichts nach obliegt es dem Gesetzgeber bei der Regelung von Eingriffsbefugnissen,

> *„Verwendungszwecke und Eingriffsschwellen sowie die für die Gewährleistung der Zweckbindung gegebenenfalls erforderlichen Folgeregelungen verbindlich festzulegen“,*
>
> BVerfGE 155, 119 (179 Rn. 130) m.w.N.

Des Weiteren sind bei einem derart schwerwiegenden Eingriff in die informationelle Selbstbestimmung hohe Anforderungen an das zu schützende Rechtsgut zu stellen. Solche Eingriffe sind nur zum Schutz besonders gewichtiger Rechtgüter zulässig,

> BVerfGE 165, 363 (410 Rn. 104 f. m.w.N).

Maßnahmen sind mit dem Grundsatz der Verhältnismäßigkeit

> *„nur vereinbar, wenn sie die Verwendungszwecke der einzelnen Befugnisse gemessen an ihrem Eingriffsgewicht selbst hinreichend normenklar begrenzen“*
>
> BVerfGE 155, 119 (178 Rn. 127).

Insofern hat das angerufene Gericht bereits entschieden, dass schon der Abruf von IP-Adressen zugeordneten Bestandsdaten – wobei es sich freilich im Vergleich zur vollständigen Auslesung

eines Mobiltelefons regelmäßig um eine ungleich begrenztere Datenerhebung handelt – nicht schon bei einem jeden Anfangsverdacht zulässig sein darf:

> *„Das maßgeblich aufgrund Art, Umfang und Verwendungsmöglichkeiten der verarbeiteten Daten erhöhte Eingriffsgewicht der Zuordnung von IP-Adressen erlaubt es indessen nicht, diese allgemein und uneingeschränkt auch zur Abwehr jeglicher Gefahren sowie zur Verfolgung oder Verhinderung jedweder Ordnungswidrigkeiten zuzulassen. Auch unter Berücksichtigung des gesteigerten Interesses an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung dem jeweiligen Akteur zuordnen zu können und der angesichts der zunehmenden Bedeutung des Internets für die verschiedenartigen Bereiche des täglichen Lebens erhöhten Gefahr seiner Nutzung für Straftaten und Rechtverletzungen vielfältiger Art, bedarf die Aufhebung der Anonymität des Internets zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließt Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es muss sich insoweit aber um - auch im Einzelfall - besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber zudem ausdrücklich benennen muss.“*
>
> BVerfGE 155, 119 (200 f. Rn. 177).

(2) Verstoß gegen verfassungsrechtliche Anforderungen

Die §§ 94 ff. StPO genügen diesen verfassungsrechtlichen Anforderungen nicht, soweit sie für den umfassenden Datenzugriff auf beschlagnahmte Datenträger sowie die Sicherung, Übermittlung und inhaltlicher Auswertung aller Daten angewendet werden.

Die §§ 94 ff. StPO ermöglichen den Zugriff auf und die vollständige Auslesung von Mobiltelefonen selbst beim Verdacht von Delikten oder Ordnungswidrigkeiten ganz untergeordneter Bedeutung (dazu oben **B.I.1.**). Damit fehlt es an der verfassungsrechtlich zu fordernden Einschränkung auf Straftaten angemessener Schwere sowie einer qualifizierten Beweisrelevanz. Die aus dem Regelungszusammenhang abzuleitende Beschränkung auf den Ermittlungszweck stellt gerade keine hinreichend bestimmte und normenklare Einschränkung dar (dazu oben

1.c.cc.(1)(d)(bb)). Darüber hinaus fehlt es auch an Vorschriften zum Kernbereichsschutz (dazu oben **1.c.cc.(3)**).

Wie bereits dargelegt, ist auch der Eingriff im konkreten Fall unverhältnismäßig, insbesondere wäre der umfassende Datenzugriff, die Sicherung des gesamten Datenbestandes sowie die Übermittlung aller Daten zum Zwecke der inhaltlichen Auswertung weder erforderlich noch angemessen gewesen (dazu oben **1.c.dd.**).

3. Verletzung des Grundrechts auf Eigentumsfreiheit

Aus denselben Umständen ergibt sich im konkreten Fall auch eine Verletzung des Grundrechts auf Eigentumsfreiheit des Beschwerdeführers, da sein Mobiltelefon beschlagnahmt und für eine erhebliche Zeit einbehalten wurde. Die Beschlagnahme seines Mobiltelefons mitsamt aller darauf gespeicherten Daten war weder erforderlich noch angemessen (dazu oben **1.c.dd.**).

Durch den Eigentumsentzug war der Beschwerdeführer in seiner Lebensführung erheblich beeinträchtigt. Für zahlreiche alltägliche Tätigkeiten war er auf die Nutzung seines Mobiltelefons angewiesen. So war es ihm etwa nicht mehr möglich, Überweisungen zu tätigen, da das dafür erforderliche pushTAN-Verfahren an sein Mobiltelefon gekoppelt war. Auch hatte er keinen Zugriff mehr auf die in seinem Mobiltelefon gespeicherten Kontakte, Bilder, Videos und Notizen. Zudem waren ihm seine Notizen, die er für einen journalistischen Beitrag über die am … September 2023 stattgefundenen Demonstration angefertigt hatte, nicht mehr zugänglich. Ihm war es dadurch nicht mehr möglich, den geplanten Artikel zu verfassen und zu veröffentlichen. Eine Ersatzbeschaffung und die anschließende Neueinstellung zentraler Dienste waren mit erheblichem Zeit- und Kostenaufwand verbunden. Zudem ermöglicht auch ein neues Gerät keinen Zugriff auf die in seinem beschlagnahmten Mobiltelefon gespeicherten Daten.

4. Verletzung der Pressefreiheit

Die angegriffene gerichtliche Entscheidung verletzt den Beschwerdeführer auch in seinem Recht auf Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG.

a. Schutzbereich

Der Schutzbereich der Pressefreiheit ist eröffnet.

Dies gilt zunächst in persönlicher Hinsicht, denn der Beschwerdeführer ist Journalist und damit vom persönlichen Schutzbereich der Pressefreiheit erfasst.

Träger der Grundrechte der Presse- und Rundfunkfreiheit sind alle Personen, die die von Art. 5 Abs. 1 Satz 2 GG geschützten Handlungen vornehmen. Der Begriff der Presse umfasst dabei jedenfalls Zeitungen und Zeitschriften, die dem Publikum allgemein zum Verkauf angeboten werden. Entscheidend ist, dass es sich um eine Publikation handelt, die grundsätzlich in gedruckter und zur Verbreitung geeigneter und bestimmter Form am Kommunikationsprozess teilnimmt, wobei stets von einem weiten und formalen Pressebegriff auszugehen ist,

BVerfGE 95, 28 Rn. 26; BVerfGE 34, 269 (283); BVerfGE 66, 116 (134).

…, das Magazin für das der Beschwerdeführer tätig ist, erfüllt diese Kriterien. Sie erscheint in gedruckter Ausgabe derzeit … im Jahr und kann von jedermann entgeltlich abonniert werden. …

Der Beschwerdeführer ist Redakteur der Publikation. Er war auch am hier gegenständlichen Datum, dem … September 2023, in dieser Funktion an der Demonstration und den der Demonstration nachfolgenden polizeilichen Aktivitäten beteiligt. Wie er dies schon zuvor bei anderen Demonstrationen handhabte, wollte der Beschwerdeführer die Geschehnisse auf der Demonstration dokumentieren, um anschließend über diese in … berichten zu können. Dies zeigen auch die von der Polizei ausgelesenen Dateien auf dem Mobiltelefon des Beschwerdeführers,

siehe Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 67-75 (**Anlage 3**).

Zu beachten ist insofern auch, dass zumindest manchen der an der Maßnahme beteiligten Polizeibeamten bekannt war, dass der Beschwerdeführer als Journalist tätig war, da sie seine

journalistische Tätigkeit schon bei früheren Demonstrationen als auch bei dem gegenständlichen Aufzug am … September 2023 wahrgenommen hatten (dazu oben **B.II.2.**),

> Ermittlungsakte der Staatsanwaltschaft Bamberg, S. 18, 36, 50 (**Anlage 3**);

Auch sachlich fällt das hier gegenständliche Verhalten des Beschwerdeführers, bei der er von der Ermittlungsmaßnahme betroffen wurde, in den geschützten Bereich des Grundrechts.

Geschützt von Art. 5 Abs. 1 Satz 2 GG ist die gesamte Presse- und Rundfunktätigkeit von der Beschaffung der Information bis zur Verbreitung der Nachricht,

> BVerfGE 107, 299 (329 Rn. 102); BVerfG, Urteil vom 24. Januar 2001 - 1 BvR 2623/95 -, BVerfGE 103, 44-81, Rn. 54 m.w.N.; BVerfGE 20, 162 (176, 187 ff.); BVerfGE 50, 234 (240); BVerfGE 77, 65; BVerfGE 66, 116 (130 ff.)

Geschützt ist zudem die Vertraulichkeit der Redaktionsarbeit. Diese verwehrt es staatlichen Stellen grundsätzlich, sich einen Einblick in die Vorgänge zu verschaffen, die zur Entstehung von Nachrichten oder Beiträgen führen, die in der Presse gedruckt oder im Rundfunk gesendet werden,

> BVerfGE 107, 299 (330 Rn. 104); BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 10. Dezember 2010 - 1 BvR 1739/04 -, Rn. 14 m.w.N.

Eine „intakte und gesicherte Vertraulichkeitssphäre der Presse“ ist demnach unerlässliche Voraussetzung für die Arbeit der Redaktion,

> BVerfG, Beschluss vom 10. Mai 1983 - 1 BvR 385/82 -, Rn. 16 f., ebenso BVerfGE 117, 244 Rn. 42.

Die Dokumentation des polizeilichen Vorgehens im Anschluss an eine Demonstration zum Zwecke der Berichterstattung stellt einen Vorgang der journalistischen Informationsbeschaffung dar, der als solcher integraler Bestandteil der Arbeit der Presse ist.

b. Eingriff und verfassungsrechtliche Rechtfertigung

Die Beschlagnahme des Mobiltelefons des Beschwerdeführers und dessen Entsperrung und Auslesung auf der Grundlage des §§ 94 ff. StPO sowie die gerichtliche Bestätigung dieser Maßnahmen stellt einen Eingriff dar, der verfassungsrechtlich nicht gerechtfertigt werden kann. Es lag bereits kein legitimer Zweck vor, da die Annahme eines Anfangsverdachts nach § 201 Abs. 1 Nr. 1 StGB auf einer grundsätzlich unrichtigen Anschauung der Pressefreiheit des Beschwerdeführers beruhte (dazu unter **aa.**). Darüber hinaus war die Maßnahme weder erforderlich noch angemessen (dazu unter **bb.**).

aa. Kein legitimer Zweck

Der einzige in Frage kommende legitime Zweck der konkreten Maßnahme ist das Strafverfolgungsinteresse – die Aufklärung eines möglichen Verstoßes gegen § 201 Abs. 1 Nr. 1 StGB. Bereits die Annahme eines Anfangsverdachts hinsichtlich des § 201 Abs. 1 Nr. 1 StGB war im konkreten Fall jedoch nicht tragfähig, weil es an tatsächlichen Anhaltspunkten für die Verwirklichung des objektiven Tatbestands von § 201 Abs. 1 Nr. 1 StGB fehlte und auf einer grundsätzlich unrichtigen Anschauung der Pressefreiheit des Beschwerdeführers beruhte.

Das angerufene Gericht überprüft die strafrechtliche Bewertung des Fachgerichts bei der Annahme eines Anfangsverdachts in rechtlicher Hinsicht nur darauf, ob die strafrechtliche Bewertung der Verdachtsgründe objektiv willkürlich ist oder Fehler erkennen lässt, die auf einer grundsätzlich unrichtigen Anschauung der Grundrechte des Beschwerdeführers beruhen. In tatsächlicher Hinsicht prüft das angerufene Gericht, ob der Tatverdacht auf konkrete Tatsachen gestützt ist,

> BVerfG, Beschluss vom 10. Juni 1964 - 1 BvR 37/63 -, NJW 1964, 1715 (1716); BVerfG, Beschluss vom 23. Januar 2004 - 2 BvR 766/03 -, NStZ-RR 2004, 143 f.; und Beschluss vom 21. Dezember 2001 – 2 BvR 1176/01, BeckRS 2002, 204; stRspr.

Gemessen daran liegt durch die Annahme eines Anfangsverdachts eine Verletzung der Pressefreiheit des Beschwerdeführers vor. Das LG Bamberg hat in seinem Beschluss bei der

Beurteilung des Vorliegens eines Anfangsverdachts in Bezug auf die journalistische Tätigkeit des Beschwerdeführers lediglich festgestellt:

> „*auch Medienvertreter haben insoweit keinen Sonderstatus und bedürfen zur Aufzeichnung der Einwilligung des Betroffenen (Münchener Kommentar zum StGB/Graf, 4. Aufl. 2021, StGB § 201 Rn. 17)*“,
>
> LG Bamberg, Beschluss vom 27. Juni 2025 - ... -, S. 5 (**Anlage 2**).

Damit hat das LG Bamberg die Bedeutung und Tragweite der Pressefreiheit grundlegend verkannt. Aufgabe der Presse ist es, umfassende Information zu ermöglichen, die Vielfalt der bestehenden Meinungen wiederzugeben und selbst Meinungen zu bilden und zu vertreten,

> BVerfGE 93, 266 (319, Rn. 119); BVerfGE 113, 63 (88, Rn. 51).

Gerade der Presse als *public watchdog* muss es möglich sein, sich kritisch mit dem behördlichen Handeln auseinanderzusetzen. Der Beschwerdeführer hat die zuvor stattgefundene Versammlung journalistisch begleitet, was auch eine Beobachtung und Dokumentation von Geschehnissen im unmittelbaren Anschluss der Versammlung umfasste, insbesondere im Zusammenhang mit repressiven polizeilichen Maßnahmen. Die Bedeutung seines journalistischen Informationsinteresses hat das LG Bamberg bei der Beurteilung des Vorliegens eines Anfangsverdachts vollständig unberücksichtigt gelassen, insbesondere den Umstand, dass ein erhebliches öffentliches Interesse an der Beobachtung und Dokumentation der Rechtmäßigkeit von polizeilichen Maßnahmen allgemein und besonders unmittelbar im Anschluss an Versammlungen besteht.

Aufgrund der Aufzeichnung einer polizeilichen Maßnahme ist zudem das Rechtsstaatsprinzip zu berücksichtigen. Polizeiliche Maßnahmen müssen kontrollierbar sein,

> BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, - 1 BvR 1140/09 -, Rn. 140.

Neben Kontrolle durch staatliche Stellen selbst spiegelt sich dies auch im Schutz der Pressefreiheit wider. Strafnormen, die dazu führen, dass journalistische Aufnahmen polizeilicher

Maßnahmen mit Strafe sanktioniert werden – darauf ging auch der vermeintliche vorliegende Anfangsverdacht –, können allenfalls in Ausnahmesituation verfassungsrechtlich gerechtfertigt werden.

Vor dem Hintergrund ist die Auslegung des Landgerichts nicht haltbar. Die polizeiliche Maßnahme erfolgte an einem öffentlich zugänglichen und stark frequentierten Ort, der auch für unbeteiligte Dritte frei zugänglich war (sog. faktische Öffentlichkeit). Im vorliegenden Fall waren auch der Beschwerdeführer und seine zwei Begleitpersonen in ihrer Funktion als Journalisten tatsächlich anwesend. Insbesondere mit Blick auf die Anwesenheit von Presseangehörigen konnten die Polizeibeamt*innen in der vorliegenden Situation nicht mit der Vertraulichkeit ihres gesprochenen Wortes im Rahmen der polizeilichen Maßnahme rechnen.

§ 201 StGB schützt bereits seinem Wortlaut nach nur das nichtöffentlich gesprochene Wort vor heimlicher Aufzeichnung. Eine verfassungskonforme Auslegung ergibt, dass sich die Nichtöffentlichkeit dabei nicht nach dem bloßen subjektiven Wunsch der Beteiligten bestimmen kann, sondern nach den objektiven Gegebenheiten der konkreten Kommunikationssituation. Maßgeblich ist, ob ein*e verständige Beobachter*in erkennen konnte, dass das Gespräch gegenüber Dritten abgeschirmt war und einem vertraulichen Rahmen zugeordnet werden durfte,

Eisele, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 201 Rn. 9.

Nichtöffentlich ist ein Gespräch also dann, wenn es nach dem erkennbaren Willen und den äußeren Umständen gegenüber Dritten abgeschirmt ist, also objektiv nicht zur Kenntnisnahme durch Dritte bestimmt oder geeignet ist. Es kommt nicht nur auf subjektive Vorstellungen der Sprecher*innen, sondern auf eine objektivierte Vertraulichkeitserwartung an,

Fischer/Anstötz, in: Fischer, StGB, 71. Auflage 2024, § 201 Rn. 4 ff.

Die Strafvorschrift kann demnach jedenfalls dann nicht eingreifen, wenn das gesprochene Wort in einer Situation geäußert wurde, die für Dritte ohne Weiteres zugänglich war, insbesondere im öffentlichen Raum ohne erkennbare Abschirmung,

Graf, in: Münchener Kommentar StGB, 4. Auflage 2022, § 201 Rn. 21 ff.,

wie das vorliegend auch der Fall war. Die Äußerungen der Polizeibeamten erfolgten im unmittelbaren Anschluss an eine Versammlung auf öffentlichem Straßenland, unter freiem Himmel und in Anwesenheit Dritter. Die Situation war räumlich offen, von allgemeiner Betriebsamkeit geprägt und für Außenstehende ohne weiteres zugänglich. Die offene Situation, die Sichtbarkeit der beteiligten Beamten, der fehlende Raumabschluss und die tatsächliche Anwesenheit anderer Personen schließen eine solche berechtigte Vertraulichkeitserwartung objektiv aus. Dass das Gespräch von einem Dritten überhaupt aufgezeichnet werden konnte, beweist gerade die Öffentlichkeit der Situation.

Auch nach überwiegender Ansicht in Rechtsprechung und Literatur steht dienstliche Kommunikation im öffentlichen Raum regelmäßig nicht unter dem Schutz des § 201 StGB, weil sie sich gerade an ein Beobachtungspotential in der Öffentlichkeit richtet,

LG Hamburg, Beschluss vom 21. Dezember 2021 – 610 Qs 37/21 jug -, juris.

Allein die Tatsache, dass sich das Gespräch in einer Dreiergruppe vollzog, genügt für die Annahme von Nichtöffentlichkeit nicht – jedenfalls nicht, wenn die äußeren Umstände gerade gegen Vertraulichkeit sprechen. Es wurden keinerlei Verhaltensweisen oder äußere Umstände festgestellt, die auf eine gewollte Abschottung oder Vertraulichkeit des Gesprächs hindeuteten: kein Flüstern, keine räumliche Distanz zu Umstehenden, keine verdeckten Handzeichen, keine Abschirmung durch Körperhaltung oder Positionierung.

In diese Richtung äußert sich auch das Landgericht Kassel in einem vergleichbaren Fall, in dem Polizeibeamte im öffentlichen Raum während eines Einsatzes gesprochen hatten. Das Gericht verneinte einen Anfangsverdacht nach § 201 StGB, da die Kommunikation sichtbar, nicht abgeschirmt und für Umstehende wahrnehmbar war. Der objektive Gesprächskontext sei entscheidend, nicht etwa das subjektive Stör- oder Unwohlsein der Sprechenden. Bloße dienstliche Kommunikation uniformierter Polizeibeamter in der Öffentlichkeit sei grundsätzlich nicht geschützt, solange keine besondere Abschirmung vorliegt,

LG Kassel, Beschluss vom 23. September 2019 - 2 Qs 111/19 -, juris.

Die Argumentation des LG Kassel unterstreicht die allgemein grundrechtliche gebotene Auslegung: Eine objektive Vertraulichkeitssituation ist nur dann anzunehmen, wenn die Beteiligten erkennbar und aktiv versuchen, sich der Wahrnehmung Dritter zu entziehen. Daran fehlte es im hiesigen Fall völlig.

Zudem liegt schon keine Heimlichkeit der Aufnahme vor. Ein heimliche Aufnahme setzt nach überwiegender Meinung voraus, dass der Täter die Aufzeichnung so vornimmt, dass die Gesprächsteilnehmer nach dem äußeren Anschein nicht mit einer Tonaufnahme rechnen mussten,

> *Eisele*, in: Tübinger Kommentar Strafgesetzbuch, 31. Auflage 2025, § 201 Rn. 6 ff.; *Heuchemer*, in: BeckOK StGB, 65. Auflage 2025, § 201 Rn. 5.

Daran fehlte es hier: Der Beschwerdeführer nahm die Situation offen auf, das Mobiltelefon war sichtbar, es wurde keine Aufnahmevorrichtung versteckt und keine Täuschung eingesetzt. Eine offen erkennbare Aufnahme spricht gegen eine strafrechtlich relevante Verletzung des höchstpersönlichen Lebensbereichs – insbesondere bei Amtsträgern in Uniform. Schon gar nicht ist die Schwelle zur Strafbarkeit überschritten, wenn die Betroffenen die Situation wahrnehmen konnten, aber nicht reagierten oder widersprachen,

> *Graf*, in: Münchener Kommentar StGB, 4. Auflage 2022, § 201 Rn. 21 ff.

Das gilt erst recht unter Berücksichtigung der Situation im Lichte der Pressefreiheit in Verbindung mit dem Rechtsstaatsprinzip.

bb. Fehlende Erforderlichkeit und Angemessenheit

Wie bereits ausgeführt, war die Maßnahme nicht erforderlich, da mildere, gleich geeignete Mittel vorlagen (dazu oben **1.c.dd.(1)**). Auch war sie unangemessen, da vorliegend ein schwerwiegender Eingriff in die Pressefreiheit des Beschwerdeführers vorliegt, der außer Verhältnis zum verfolgten Zweck steht.

Bei der Beschlagnahme eines Mobiltelefons, das zu journalistischen Zwecken eingesetzt wird und auf dem sich für die Pressearbeit relevante Quellenkontakte und Informationen finden, handelt es sich um einen besonders schwerwiegenden Eingriff in die Pressefreiheit,

vgl. auch BVerfGE 117, 244 (260).

Der vollständige Zugriff auf ein derartiges Gerät gibt gesammelte Informationen nämlich nicht nur in Gänze der staatlichen Kenntnisnahme preis, sondern greift auch in besonderem Maße in die Vertraulichkeit der Redaktionsarbeit und in ein etwaiges Vertrauensverhältnis zu Informanten ein.

Darüber hinaus gehen von derartigen Maßnahmen auch weitere Einschüchterungseffekte aus, die den Beschwerdeführer, aber auch andere Journalist*innen von der Berichterstattung über Demonstrationen im Allgemeinen und damit verbundenen polizeilichen Maßnahmen im Spezifischen abschrecken können.

Dieser Eingriffsschwere stehen keine überwiegenden gegenläufigen verfassungsrechtlichen Rechte oder Rechtsgüter gegenüber.

Zwar gebietet es die Verfassung nicht, Journalist*innen generell von strafprozessualen Maßnahmen auszunehmen,

BVerfGE 107, 299 (331).

Es müssen aber die mit der Strafverfolgung verfolgten Schutzgüter die Beschränkung der Pressefreiheit aufwiegen können,

BVerfGE 117, 244 (260).

Dies ist vorliegend nicht der Fall. Wie bereits das geringe Strafmaß des § 201 Abs. 1 StGB anzeigt, handelt es sich bei den von diesem geschützten Rechtsgütern nicht um besonders erhebliche Privat- oder Allgemeingüter.

Dies wird im konkreten Fall ganz erheblich noch dadurch verstärkt, dass vorliegend nur ganz geringfügige Persönlichkeitsinteressen der beteiligten Polizeibeamten in Betracht kommen. Polizeibeamte können nämlich, wenn sie in amtlicher Funktion auftreten und betroffene Personen im amtlicher Funktion ansprechen, nur in Ausnahmefällen durchgreifende Persönlichkeitsinteressen geltend machen. Amtlichen Äußerungen kommt als solchen regelmäßig kein erhöhter Persönlichkeitsbezug zu. Mit ihnen informieren Vertreter*innen des Staates betroffene Bürger*innen über ihre Rechte und Pflichten oder über sonstige für das Unterordnungsverhältnis relevante Informationen. Eine Persönlichkeitsrelevanz, die sogar die Kriminalisierung der Aufnahme derartiger Ansprachen rechtfertigen könnte, kann solchen Äußerungen allenfalls in absoluten Ausnahmefällen zukommen.

Ein derartiger Ausnahmefall lag hier aber nicht vor. Weshalb den polizeilichen Äußerungen irgendein Persönlichkeitsbezug zukommen sollte, wurde weder von den anordnenden Beamten noch im angegriffenen gerichtlichen Beschluss vorgetragen.

Aus diesen Gründen überwiegt im vorliegenden Fall die Pressefreiheit des Beschwerdeführers und die Ermittlungsmaßnahmen waren nicht angemessen.

5. Verletzung der Meinungsfreiheit

Die Beschlagnahme seines Mobiltelefons verletzt den Beschwerdeführer auch in seiner Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG.

a. Schutzbereich

Die Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG gewährleistet jedermann das Recht, seine Meinung frei zu äußern und zu verbreiten. Meinungen sind durch das Element der Stellungnahme und des Dafürhaltens im Rahmen einer geistigen Auseinandersetzung gekennzeichnet und durch die subjektive Beziehung des Einzelnen zum Inhalt seiner Aussage geprägt,

BVerfG, Beschluss vom 13. April 1994 – 1 BvR 23/94, NJW 1994, 1779 (1779); stRspr.

Auch Tatsachenbehauptungen sind durch die Meinungsfreiheit jedenfalls insoweit geschützt, als sie Voraussetzung für die Bildung von Meinungen sind, da sich Meinungen in der Regel auf tatsächliche Annahmen stützen oder zu tatsächlichen Verhältnissen Stellung beziehen,

BVerfG, Beschluss vom 13. April 1994 - 1 BvR 23/94 -, NJW 1994, 1779 (1779); stRspr.

Dementsprechend ist der Begriff der Meinung grundsätzlich weit zu verstehen: Sofern eine Äußerung durch die Elemente der Stellungnahme, des Dafürhaltens oder Meinens geprägt ist, fällt sie im Interesse eines wirksamen Grundrechtsschutzes auch dann in den Schutzbereich des Grundrechts, wenn sich diese Elemente mit Elementen einer Tatsachenbehauptung vermischen und sich von diesen nicht trennen lassen, weil anderenfalls eine wesentliche Verkürzung des Grundrechtsschutzes drohte,

BVerfG, Beschluss vom 22. Juni 1982 - 1 BvR 1376/79 -, NJW 1983, 1415 (1416); BVerfG, Beschluss vom 13. April 1994 - 1 BvR 23/94 -, NJW 1994, 1779 (1779).

Geschützt ist der Inhalt, aber auch die Form bzw. die Art und Weise der Äußerung,

BVerfGE 60, 234 (241); 76, 171 (192).

Dabei ist auch vom Schutz erfasst, diejenigen Umstände zu wählen, von denen sich die sich äußernde Person die größte Verbreitung oder die stärkste Wirkung der Meinungskundgabe verspricht,

BVerfG, Urteil vom 22. Februar 2011 - 1 BvR 699/06 -, BeckRS 2011, 47764, Rn. 97.

Erfasst werden auch begleitende Tätigkeiten, die den Zweck haben, die Wirkung der Äußerung zu verstärken,

BVerfGE 97, 391 (398).

Geschützt werden zudem die Voraussetzungen für die Herstellung und Aufrechterhaltung des Kommunikationsprozesses,

BVerfGE 97, 391 (399).

Geschützt wird jede Form der Meinungsäußerung und -verbreitung, auch mit Hilfe von Tonträgern und Bildern,

BVerfGE 30, 336 (352).

b. Eingriff

Durch die Beschlagnahme seines Mobiltelefons wird in die Meinungsfreiheit des Beschwerdeführers eingegriffen, da er dadurch den Zugriff zu seiner Dokumentation der polizeilichen Maßnahme, die sich gegen die drei Demonstrationsteilnehmenden richtete, verlor und er an der kritischen, mithilfe der Tonaufnahme erfolgenden Aussprache gegenüber seiner Auffassung nach willkürlichen und rechtswidrigen Polizeimaßnahmen gehindert war.

c. Verfassungsrechtliche Rechtfertigung

Der Eingriff in die Meinungsfreiheit ist verfassungsrechtlich nicht gerechtfertigt. Die Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG findet ihre Schranken gem. Art. 5 Abs. 2 GG in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre, wozu die §§ 94 ff. StPO zählen.

Es liegt bereits kein legitimer Zweck vor, da das LG Bamberg in seinem Beschluss bei der Annahme des Vorliegens eines Anfangsverdachts nach § 201 Abs.1 Nr. 1 StGB grundlegend auch die Bedeutung und Tragweite der Meinungsfreiheit des Beschwerdeführers verkannt hat (dazu unter **aa.**). Darüber hinaus war die Maßnahme weder erforderlich noch angemessen (dazu unter **bb.**).

aa. Legitimer Zweck

Neben dem Grundrecht auf Pressefreiheit hat das LG Bamberg in seinem Beschluss bei der Annahme eines Anfangsverdachts des § 201 Abs. 1 Nr. 1 StGB auch die grundlegende Bedeutung und Tragweite der Meinungsfreiheit des Beschwerdeführers verkannt.

Der Beschwerdeführer ist mit seinen zwei Begleitpersonen im unmittelbaren Anschluss der Versammlung zu einer polizeilichen Maßnahme gegenüber drei Demonstrationsteilnehmenden dazugestoßen. Da ihm die Vorgehensweise der anwesenden Polizeibeamt*innen aufgestoßen war, wollte er diese u.a. mithilfe einer Sprachnotiz dokumentieren, um anschließend sich kritisch dazu äußern zu können – sowohl öffentlich, als auch im Rahmen einer Dienstaufsichtsbeschwerde,

siehe Ermittlungsakte der Staatsanwaltschaft, S. 18, 23 (**Anlage 2**).

Bei der Beurteilung des Vorliegens eines Anfangsverdachts nach § 201 Abs. 1 Nr. 1 StGB haben zunächst die Beamten und dann das Landgericht Bamberg in seinem Beschluss das Interesse des Beschwerdeführers an der Dokumentation einer rechtswidrigen polizeilichen Maßnahme, um sie als Grundlage für seine anschließende Meinungsäußerung zu nehmen, vollständig unberücksichtigt gelassen. Insbesondere mit Blick auf das Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG und der gerichtlichen Geltendmachung von Rechtsverletzungen besteht ein erhebliches Interesse an der Dokumentation und öffentlicher Bekanntmachung von rechtswidrigen polizeilichen Maßnahmen. Die Aufnahme hatte informationsverschaffenden Charakter und diente der Vorbereitung von grundrechtlich geschützten Kommunikationskaten. Das bereits ausgeführte journalistische Informationsinteresse (dazu oben **4.b.**) gilt gleichermaßen für Privatpersonen, die im Rahmen ihres Grundrechts auf Meinungsäußerung solche Missstände anprangern wollen. Dies gilt umso mehr für Maßnahmen, die in der Öffentlichkeit unter Anwesenheit von unbeteiligten Dritten erfolgen. Unter diesen Umständen können Polizeibeamt*innen nicht berechtigterweise mit der Vertraulichkeit ihres gesprochenen Wortes rechnen (dazu bereits oben **4.b.aa.**).

bb. Fehlende Erforderlichkeit und Angemessenheit

Aufgrund der bereits zur Verletzung der Pressefreiheit ausgeführten Umstände (dazu oben **4.b.**) war die Maßnahme auch in Bezug auf einen Eingriff in die Meinungsfreiheit weder erforderlich noch angemessen. Aufgrund des geringen Strafmaßes handelt es sich bei § 201 Abs. 1 StGB nicht um ein besonders erhebliches Privat- oder Allgemeingut, insbesondere sind im vorliegenden Fall die Persönlichkeitsinteressen der Polizeibeamt*innen nur geringfügig betroffen, da sie eine Diensthandlung ausführten (dazu oben **4.b.bb.**). Dem steht ein schwerwiegender Eingriff in die Meinungsfreiheit des Beschwerdeführers gegenüber, der durch das erhebliche Interesse an der öffentlichen kritischen Auseinandersetzung von willkürlichen und rechtswidrigen polizeilichen Maßnahmen – insbesondere im Zusammenhang mit Versammlungen – begründet ist (dazu oben **4.b.**).

6. Verletzung der allgemeinen Handlungsfreiheit

Aus denselben Umständen ist der Beschwerdeführer jedenfalls in seiner allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG verletzt, da bei der Annahme eines Anfangsverdachts nach § 201 Abs. 1 StGB in Verbindung mit dem Rechtsstaatsprinzip sein erhebliches Interesse an der Dokumentation der polizeilichen Maßnahme durch den Beschluss des LG Bamberg grundlegend verkannt wurde und er dadurch in unverhältnismäßiger Weise in seinem Grundrecht verletzt wurde.

7. Verletzung des Rechts auf rechtliches Gehör

Indem das Landgericht Bamberg in seinen Entscheidungsgründen auf alle vom Beschwerdeführer vorgetragenen Aspekte zur Verfassungs- und Unionsrechtswidrigkeit, die für das Verfahren von zentraler Bedeutung sind, überhaupt nicht eingegangen ist sowie seinen Vortrag zum Nichtbestehen eines Anfangsverdachts vollkommen unberücksichtigt gelassen und seine wesentlichen Ausführungen zur Unverhältnismäßigkeit der gegen ihn ergangenen Maßnahmen übergangen hat, hat es ihn auch in seinem Recht auf rechtliches Gehör nach Art. 103 Abs. 1 GG verletzt.

a. Pflicht zur Auseinandersetzung mit den zentralen Argumenten

Der Anspruch auf rechtliches Gehör beinhaltet, dass das entscheidende Gericht die Ausführungen der Prozessbeteiligten zur Kenntnis nehmen und in Erwägung ziehen muss,

> BVerfGE 21, 191 (194); 96, 205 (216); stRspr.

Der in Art. 103 Abs. 1 GG verbürgte Anspruch steht in einem funktionalen Zusammenhang mit der Rechtsweggarantie des Art. 19 Abs. 4 GG. Beide dienen dem gleichen Ziel, nämlich der Gewährleistung eines wirkungsvollen Rechtsschutzes. Während die Rechtsschutzgarantie den Zugang zum Verfahren sichert, zielt Art. 103 Abs. 1 GG auf einen angemessenen Ablauf des Verfahrens: Wer bei Gericht formell ankommt, soll auch substantiell ankommen, also wirklich gehört werden,

> BVerfGE 107, 395 (409); BVerfG, Beschluss vom 29. November 1989 - 1 BvR 1011/88 -, juris, Rn. 19.

Dabei umfasst das Recht, gehört zu werden, sowohl tatsächliches Vorbringen der Beteiligten als auch Ausführungen zur Rechtslage,

> BVerfG, Beschluss vom 25. Juni 1992 - 1 BvR 600/92 -, juris, Rn. 12 m.w.N.; BVerfG, Beschluss vom 7. September 2007 - 2 BvR 1009/07 -, NStZ-RR 2008, 16.

Grundsätzlich ist davon auszugehen, dass ein Gericht das Vorbringen der Beteiligten zur Kenntnis genommen und in Erwägung gezogen hat, da es nicht verpflichtet ist, jedes Vorbringen in den Gründen seiner Entscheidung ausdrücklich zu verbescheiden. Art. 103 Abs. 1 GG ist nur dann verletzt, wenn im Einzelfall besondere Umstände deutlich machen, dass das Vorbringen eines Beteiligten entweder überhaupt nicht zur Kenntnis genommen oder bei der Entscheidung nicht erwogen worden ist,

> BVerfGE 65, 293 (295); 70, 288 (293) 86, 133 (145 f.).

Geht ein Gericht auf den wesentlichen Kern des Tatsachenvortrags eines Verfahrensbeteiligten zu einer Frage, die für das Verfahren von zentraler Bedeutung ist, in den Entscheidungsgründen nicht ein, so lässt dies auf die Nichtberücksichtigung des Vortrags schließen, sofern er nicht nach dem Rechtsstandpunkt des Gerichts unerheblich oder aber offensichtlich unsubstantiiert war,

> BVerfGE 86, 133 (146) m.w.N.

Wenn ein bestimmter Vortrag den Kern des Parteivorbringens darstellt und für den Prozessausgang eindeutig von entscheidender Bedeutung ist, besteht für das Gericht folglich eine Pflicht, die vorgebrachten Argumente zu erwägen. Ein Schweigen lässt hier den Schluss zu, dass der Vortrag der Prozesspartei entgegen Art. 103 Abs. 1 GG nicht beachtet worden ist,

> BVerfGE 47, 182 (188 f.); BVerfG, Beschluss vom 25. Juni 1992 - 1 BvR 600/92 -, juris, Rn. 11.

Das Maß der Erörterungspflicht des Gerichts wird dabei nicht nur durch die Bedeutung des Vortrags der Beteiligten für das Verfahren bestimmt, sondern auch durch die Schwere eines zur Überprüfung gestellten Grundrechtseingriffs,

> BVerfG, Beschluss vom 12. März 2019 - 1 BvR 2721/16 -, juris, Rn. 17; vgl. auch BVerfG, Beschluss vom 5. Februar 2004 - 2 BvR 1621/03 -, juris, Rn. 15.

Mit der Verfassungsbeschwerde kann die Verletzung von Art. 103 Abs. 1 GG schließlich nur geltend gemacht werden, wenn die angefochtene Entscheidung auf dem Gehörsverstoß beruht. Dies ist der Fall, wenn für den Fall der Gewährung rechtlichen Gehörs eine inhaltlich andere Entscheidung nicht ausgeschlossen werden kann,

> BVerfGE 86, 133 (147); 89, 381 (392).

b. Gehörsverletzung durch den Beschluss des Landgerichts Bamberg

Das Landgericht Bamberg hat in seinem Beschluss vom 27. Juni 2025 - ... - für den Prozessausgang wesentliche Teile der Beschwerdebegründung vom 19. Juni 2025, die zum Kern des Vorbringens gehören, übergangen und in seiner Entscheidung unberücksichtigt gelassen. Konkret hat das Gericht zentralen Vortrag zur Unionsrechts- und Verfassungswidrigkeit der in Anspruch genommenen Ermächtigungsgrundlagen (dazu unter **aa.**), zum Nichtbestehen eines Anfangsverdachts (dazu unter **bb.**) und zur Unverhältnismäßigkeit der Maßnahmen (dazu unter **cc.**) missachtet. Die Entscheidung beruht auch auf den Gehörsverstößen, da nicht auszuschließen ist, dass das Gericht anders entschieden hätte, wenn es den Vortrag beachtet hätte.

aa. Keine Berücksichtigung der Ausführungen des Beschwerdeführers zur Verfassungs- und Unionsrechtswidrigkeit

Das Landgericht Bamberg hat in seinem Beschluss ersichtlich keinen der in der Beschwerdebegründung ausgeführten rechtlichen Gesichtspunkte berücksichtigt, aus denen sich die Verfassungs- und Unionsrechtswidrigkeit eines auf §§ 94 ff. StPO gestützten Datenzugangs ergibt.

In seinem Beschwerdebeschluss vom 27. Juni 2025 (**Anlage 2**, S. 4) bejahte das Gericht unter pauschalem Verweis auf obergerichtliche Rechtsprechung lediglich in einem Satz die Verfassungs- und Unionsrechtmäßigkeit.

(1) Verfassungswidrigkeit

Das Landgericht Bamberg hat die in der Beschwerdebegründung vom 19. Juni 2025 (**Anlage 7,** S. 15 ff.) erfolgten Ausführungen zur Verfassungswidrigkeit des Datenzugangs vollständig unberücksichtigt gelassen. Es hat sich weder mit dem Fehlen einer hinreichend bestimmten Gesetzesgrundlage noch mit dem Erfordernis gesetzlicher Schutzvorkehrungen für den Kernbereich oder mit der Unverhältnismäßigkeit des Eingriffs auseinandergesetzt.

Der Beschwerdeführer hat in der Beschwerdebegründung (**Anlage** 7, S. 23) explizit zu einem Verstoß gegen das Gebot der Normenklarheit und Normenbestimmtheit vorgetragen und dargelegt, dass es sich um einen schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung

der Vertraulichkeit und Integrität informationstechnischer Systeme vorliegt (**Anlage 7**, S. 14 ff.). Der Beschwerdeführer hat sich dabei auch mit der bisherigen Rechtsprechung des angerufenen Gerichts im Kontext von Beschlagnahmen und Auswertung von Datenträgern auseinandergesetzt. Er hat in der Beschwerdebegründung erläutert, warum diese nicht auf Datenzugriffe auf moderne Smartphones übertragbar ist (**Anlage 7,** S. 23) und warum die BGH-Entscheidung vom 13. März 2025 - 2 Str 232/24 -, die wiederum selbst auf die überholte – teilweise fast 20 Jahre zurückliegende – Rechtsprechung des Bundesverfassungsgerichts verweist, unter verfassungsrechtlichen Gesichtspunkten nicht haltbar ist (**Anlage 7,** S. 24). Der Beschwerdebeschluss (**Anlage 2,** S. 4) begnügte sich hingegen damit, schlichtweg auf die genannte BGH-Entscheidung zu verweisen, ohne sich mit der Argumentation des Beschwerdeführers auch nur ansatzweise auseinanderzusetzen. Auch die Ausführungen des Beschwerdeführers zum Fehlen von Regelungen zum Kernbereichsschutz (**Anlage 7,** S. 25 ff.) ließ das Gericht unberücksichtigt.

Weiterhin hat sich das Gericht nicht mit dem Vortrag des Beschwerdeführers im Rahmen der Verhältnismäßigkeit (**Anlage 7,** S. 30 ff.), dass es einer gesetzlichen Beschränkung auf angemessene Anlasstaten sowie einer konkreten fallbezogenen Erfolgstauglichkeit bedarf, auseinandergesetzt. Auch hat es nicht den rechtlichen Vortrag gewürdigt, dass aufgrund der hohen Eingriffsintensität strenge Vorgaben hinsichtlich gerichtlicher Protokollierungspflichten und Eingrenzungsvorgaben geboten sind, die in den §§ 94 ff. StPO fehlten.

Die Entscheidung beruht auch auf diesem Gehörsverstoß, da die vorgetragenen Aspekte zentral für die Beurteilung der Rechtmäßigkeit der Ermittlungsmaßnahmen sind. Es ist jedenfalls möglich, dass das Gericht bei Berücksichtigung des Vortrags des Beschwerdeführers zu einem anderen Ergebnis gekommen wäre.

(2) Unionsrechtswidrigkeit

Das Landgericht Bamberg hat auch die von dem Beschwerdeführer vorgetragenen rechtlichen Gesichtspunkte, die zu der Unionsrechtswidrigkeit des Datenzugriffs führen, vollständig übergangen.

Ein zentrales Argument der Beschwerdebegründung ist die Unionsrechtswidrigkeit der Maßnahme (**Anlage 7,** S. 37 f.) Obwohl in der Beschwerdebegründung auch dazu ausgeführt wurde,

warum der BGH die unionsrechtlichen Maßstäbe in seinem Beschluss fehlerhaft angewendet hat (**Anlage 7,** S. 40), verweist das Beschwerdegericht – ohne eigene inhaltliche Befassung mit diesen Anforderungen und den Argumenten des Beschwerdeführers – schlichtweg auf die lückenhafte Auseinandersetzung mit den unionsrechtlichen Vorgaben in dem benannten BGH-Beschluss (**Anlage 2,** S.4).

Die Entscheidung beruht auch auf den Gehörsverstößen. Es kann nicht ausgeschlossen werden, dass das Gericht bei Berücksichtigung der unionsrechtlichen Anforderungen zu einem anderen Ergebnis gekommen wäre und die Rechtmäßigkeit des Datenzugangs verneint hätte.

bb. Keine Berücksichtigung der Ausführungen des Beschwerdeführers zum Nichtbestehen eines Anfangsverdachts

Weiter hat das Landgericht Bamberg die wesentlichen Ausführungen zum Nichtbestehen eines Anfangsverdachts nach § 201 Abs. 1 Nr. 1 StGB unbeachtet gelassen.

Zwar ist das Gericht in seinem Beschwerdebeschluss (**Anlage 2,** S. 5) auf Auslegungsfragen bezüglich § 201 Abs. 1 Nr. 1 StGB eingegangen. Allerdings hat sich das Gericht nicht damit auseinandergesetzt, warum ein Anfangsverdacht möglich war, obwohl die Äußerungen hier in einem öffentlichen Rahmen und unter offenkundiger Anwesenheit des Beschwerdeführers und anderer Dritter erfolgten. Konkret hat das Gericht nicht zu erkennen gegeben, warum die gegenständlichen Äußerungen der Polizeibeamten hier als „nicht-öffentlich gesprochenes Wort“ gelten konnten, obwohl sie in einer allgemein zugänglichen und wahrnehmbaren Situation erfolgten. Der Beschwerdeführer hat in seiner Beschwerdebegründung (**Anlage 7,** S. 41 f.) aber explizit zur Subsumtion unter § 201 Abs. 1 Nr. 1 StGB ausgeführt.

Es kann auch nicht ausgeschlossen werden, dass das Gericht in seiner Prüfung der Begründetheit der Beschwerde zu einem anderen Ergebnis gekommen wäre, hätte es den Vortrag des Beschwerdeführers insofern hinreichend beachtet. Insbesondere scheint möglich, dass das Gericht auch die Bestätigung der Beschlagnahme für rechtswidrig erklärt hätte.

cc. Keine Berücksichtigung der Ausführungen des Beschwerdeführers zur Unverhältnismäßigkeit der Maßnahmen im Einzelfall

Schließlich hat das Landgericht Bamberg wesentliche Ausführungen des Beschwerdeführers zur Unverhältnismäßigkeit der gegen ihn ergangenen Maßnahmen übergangen.

Insofern ist insbesondere zu beanstanden, dass das Gericht im Rahmen seiner Verhältnismäßigkeitsprüfung keine hinreichende Differenzierung der erfolgten Maßnahmen vorgenommen und den diesbezüglichen Vortrag des Beschwerdeführers nicht beachtet hat.

Das Gericht unterscheidet in seinem Beschwerdebeschluss (**Anlage 2,** 7 f.) maßgeblich nur zwischen der Beschlagnahme des Mobiltelefons (nach Meinung des Gerichts verhältnismäßig) und der inhaltlichen Auswertung des Mobiltelefons zur Erstellung eines politischen Profils des Beschwerdeführers (wegen Ablauf der Antragsfrist rechtswidrig). Andere erfolgte Eingriffsschritte bewertet das Gericht hingegen nicht eigenständig. Damit missachtet das Gericht, dass zwischen der (Bestätigung der) Beschlagnahme und der letztendlichen Auswertung des Dateninhalts des Mobiltelefons noch verschiedene weitere Eingriffsmaßnahmen erfolgten, die in ihrer Verhältnis- und Rechtmäßigkeit aufgrund der bestehenden verfassungsrechtlichen Vorgaben getrennt zu betrachten sind. Dazu hat der Beschwerdeführer aber an verschiedenen Stellen ausgeführt (**Anlage 7,** S. 14 f., S. 42, S. 45) und insbesondere angemahnt, dass schon in den Stadien vor der inhaltlichen Auswertung der Daten die Eingriffsmaßnahmen auf das notwendige Ausmaß hätten beschränkt werden müssen und kein völlig grenzenloser Zugriff auf das Mobiltelefon erfolgen hätte dürfen (**Anlage 7,** S. 45 f.). Mit diesen Differenzierungen hat sich das Beschwerdegericht nicht bzw. nicht hinreichend auseinandergesetzt. So hat es sich weder mit der Möglichkeit einer beschränkten Beschlagnahmebestätigung auseinandergesetzt noch erörtert, ob die der inhaltlichen Auswertung vorhergehenden Maßnahmen des Zugriffs auf das Mobiltelefon und der Speicherung und Übermittlung der gespeicherten Daten erforderlich oder angemessen waren. Damit genügt das Gericht auch seinen im Beschluss aufgestellten eigenen rechtlichen Maßstäben (vgl. **Anlage 2,** S.7) nicht, da es gegen den von ihm genannten Grundsatz verstößt, dass nicht erforderliche Datenzugriffe vermieden werden müssen:

Infolge der Verkennung der verschiedenen Zugriffsschritte, behauptet das Gericht fälschlich, dass eine Begrenzung des Datenzugriffs zwischen der Sicherstellung und dem Ablauf der

Strafantragsfrist nicht in Betracht gekommen sei, da die Datensicherung erst am … Dezember 2023 vorlag, obwohl sogar nach den eigenen Feststellungen des Gerichts in seinem Beschluss feststeht, dass eine (weder erforderliche noch verhältnismäßige) umfassende Kopie des auf dem Mobiltelefon befindlichen Datenbestands schon vor dem Ablauf der Antragsfrist am … Dezember 2023 um 24.00 Uhr erstellt war (**Anlage 2,** S.7).

Das Gericht hat sich auch mit weiteren zentralen Teilen des Vorbringens des Beschwerdeführers zur Unverhältnismäßigkeit der Maßnahmen nicht befasst. So hat es nicht zu erkennen gegeben, ob es seinen Einschätzungen zur Betroffenheit der Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 14 Abs. 1 GG folgt. Dies betrifft insbesondere auch die Frage der Betroffenheit des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in das schon mit dem Zugriff auf das Mobiltelefon eingegriffen war. Tatsächlich beschränken sich die Ausführungen des Gerichts in seinem Beschwerdebeschluss (**Anlage 2,** S. 6) insofern auf einen kurzen allgemeinen Hinweis zur Bedeutung der Grundrechte.
In der Beschwerdebegründung wurde hingegen umfangreich dargestellt, aus welchen Gründen in den Schutzbereich verschiedener Grundrechte eingegriffen ist und welche spezifischen verfassungsrechtlichen Vorgaben deshalb zu berücksichtigen sind (**Anlage 7,** S. 11 ff; S. 45 f.). Hat das Gericht diesen Vortrag unberücksichtigt gelassen, konnte es aber auch die anzuwendenden verfassungsrechtlichen Maßstäbe nicht richtig berücksichtigen.

Zudem hat das Gericht Aspekte, die für die Verhältnismäßigkeitsprüfung insgesamt zentral sind, nicht erkennbar in Betracht gezogen. So hat das Gericht unter anderem nicht festgestellt, dass mit dem Zugriff auf das Mobiltelefon auch auf besonders sensible Informationen zugegriffen wurde, dass Daten gespeichert wurden, die erkennbar keinen Bezug zum Untersuchungsziel haben konnten und der Eingriff von besonderer Schwere und Tiefe war.

Auch beruht die Entscheidung auf diesem Gehörsverstoß. Bezüglich der oben angeführten Gesichtspunkte kann nicht ausgeschlossen werden, dass das Gericht zu einer anderen Entscheidung gelangt wäre, wenn es den entsprechenden Vortrag des Beschwerdeführers unter Achtung des Anspruchs auf rechtliches Gehör gem. Art. 103 Abs. 1 GG berücksichtigt hätte.

8. Verletzung des Rechts auf gesetzliche*n Richter*in

Der Beschwerdeführer wird durch den Beschluss des Landgerichts Bamberg in seinem grundrechtsgleichen Recht auf den*die gesetzliche*n Richter*in aus Art. 101 Abs. 1 Satz 2 GG verletzt, da das Gericht seiner Vorlagepflicht nach Art. 267 AEUV nicht nachgekommen ist und damit seine Vorlagepflicht offensichtlich unhaltbar gehandhabt hat.

Der Europäische Gerichtshof ist gesetzlicher Richter im Sinne des Art. 101 Abs. 1 Satz 2 GG. Kommt ein deutsches Gericht seiner Pflicht zur Anrufung des Europäischen Gerichtshofs im Wege des Vorabentscheidungsverfahrens nach Art. 267 Abs. 3 AEUV nicht nach, kann dem Rechtsschutzsuchenden des Ausgangsrechtsstreits der gesetzliche Richter entzogen sein,

> BVerfG, Beschluss vom 6. Oktober 2017 - 2 BvR 987/16 -, juris, Rn. 3; stRspr.

Dabei beanstandet das angerufene Gericht die Auslegung und Anwendung von Normen, die die gerichtliche Zuständigkeitsverteilung regeln und zu denen Art. 267 Abs. 3 AEUV gehört, nur, wenn sie bei verständiger Würdigung der das Grundgesetz bestimmenden Gedanken nicht mehr verständlich erscheinen und offensichtlich unhaltbar sind,

> BVerfG, Beschluss vom 6. Oktober 2017 - 2 BvR 987/16 -, juris, Rn. 5 f.; stRspr.

Das angerufene Gericht hat Fallgruppen aufgestellt, in denen die Vorlagepflicht offensichtlich unhaltbar gehandhabt wird,

> BVerfG, Beschluss vom 6. Oktober 2017 - 2 BvR 987/16 -, juris, Rn. 7 ff. m.w.N.

Dem angerufenen Gericht zufolge wird

> „*die Vorlagepflicht nach Art. 267 Abs. 3 AEUV […] offensichtlich unhaltbar gehandhabt, wenn das letztinstanzliche Gericht offenkundig einschlägige Rechtsprechung des EuGH nicht auswertet. Um eine Kontrolle am Maßstab des Art. 101 Abs. 1 Satz 2 GG zu ermöglichen, hat es die Gründe für seine Entscheidung über die Vorlagepflicht anzugeben*“,

BVerfG, Beschluss vom 6. Oktober 2017 - 2 BvR 987/16 -, juris, Rn 7.

Eine weitere von der verfassungsrechtlichen Rechtsprechung anerkannte Konstellation ist die bewusste Abweichung von der Rechtsprechung des Europäischen Gerichtshofs zu entscheidungserheblichen Fragen,

vgl. BVerfG, Beschluss vom 6. Oktober 2017 - 2 BvR 987/16 -, juris, Rn. 8 m.w.N.

Vorliegend wurde im Beschluss des Landgerichts Bamberg die Vorlagepflicht unter Zugrundelegung der zuvor dargestellten Maßstäbe unhaltbar gehandhabt:

Das Landgericht Bamberg hat – als letztinstanzliches Gericht – seiner Pflicht, offenkundig einschlägige Rechtsprechung des Europäischen Gerichtshofs auszuwerten, nicht Genüge getan. In seinem Beschluss hat es in einem einzelnen Satz ohne weitere Begründung festgestellt, dass

> „*die §§ 94 ff. StPO den verfassungsrechtlichen und den sich aus der Richtlinie 2016/680/EU, auch unter Berücksichtigung des Urteils des EuGH vom 4. Oktober 2024, Az. C-548/21, ergebenden Anforderungen hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern – inklusive Mobiltelefonen – und den hierauf gespeicherten Daten* [entsprechen] *(vgl. BGH Beschl. v. 13.3.2025 - 2 StR 232/24, BeckRS 2025, 9876 m.w.N.)*“,
>
> LG Bamberg, Beschluss vom 27. Juni 2025 - ... -, S. 5 (**Anlage 2).**

Mir der Rechtsprechung des Europäischen Gerichtshofs hat es sich in seinem Beschluss nicht eigenständig auseinandergesetzt, sondern lediglich mit Verweis auf die jüngste BGH-Rechtsprechung die Vereinbarkeit mit dem Unionsrecht bejaht (dazu bereits oben **7.b.aa.(2)**). Auch hat es weder die Gründe für seine Entscheidung über eine Nichtvorlage angegeben noch seine Vorlagepflicht überhaupt thematisiert.

Darüber hinaus ist das Landgericht Bamberg in seinem Beschluss bewusst von der Rechtsprechung des Europäischen Gerichtshofs abgewichen, indem es die §§ 94 ff. StPO als

unionsrechtskonforme Ermächtigungsgrundlagen einstufte und dabei von den in dem Urteil des Europäischen Gerichtshofs vom 4. Oktober 2024 (Az. C-548/21) aufgestellten Vorgaben an eine hinreichend bestimmte Ermächtigungsgrundlage für einen Datenzugriff auf beschlagnahmte Mobiltelefone, die zumindest die Art oder Kategorien der Straftaten angeben muss, sowie das Erfordernis eines spezifisch auf den Datenzugriff und die Datenauswertung ausgerichteten Gerichtsvorbehalts abrückte. Wie bereits umfassend ausgeführt genügen die §§ 94 ff. StPO gerade nicht den Anforderungen des Europäischen Gerichtshofs (dazu bereits ausführlich oben **1.c.cc.(2)(c)**).

Pinar
Rechtsanwältin

Anlagenverzeichnis

...