TWP STRAF RECHTS KANZLEI
BÜROGEMEINSCHAFT

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

per beA

Landgericht Bamberg
Abteilung für Strafsachen
Wilhelmsplatz 1
96047 Bamberg

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: 19.06.2025 Unser Zeichen: [redacted]

[redacted]

In dem Strafverfahren

gegen

[redacted]

begründe ich nachfolgend die Beschwerde gegen den Beschluss des Amtsgerichts Bamberg vom [redacted] September 2023 ([redacted]), mit welchem die Beschlagnahme sowie der Zugriff und die Auswertung der auf dem Mobiltelefon des Beschwerdeführers befindlichen Daten bestätigt wurde.

Es wird beantragt,

1. **den Beschluss des Amtsgerichts Bamberg vom [redacted].09.2023 aufzuheben;**
2. **die Rechtswidrigkeit der Sicherstellung und Auswertung festzustellen;**
3. **die Löschung aller gesicherten Daten anzuordnen;**
4. **die Verfahrenskosten der Staatskasse aufzuerlegen.**

Begründung:

Die angegriffene Ermittlungsmaßnahme war weder vom Gesetz gedeckt noch im Sinne der Verhältnismäßigkeit geboten. Sie stellt einen strukturell gravierenden Eingriff in 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 S. 1 GG) sowie in die Pressefreiheit (Art. 5 Abs. 1 S. 2 Fall 1 GG) dar und verletzt elementare rechtsstaatliche Anforderungen an Eingriffsschwellen, Transparenz und Zweckbindung.

Der Beschwerdeführer rügt das Fehlen einer verfassungs- und unionsrechtskonformen Ermächtigungsgrundlage (dazu unter C. 1. und 2.), die Rechtswidrigkeit der Maßnahme in Ermangelung des Anfangsverdachtes (dazu unter C. 3. a.) und wegen des Verstoßes gegen den Verhältnismäßigkeitsgrundsatz (dazu unter C. 3. b.) sowie die Verletzung des Rechts auf effektive Verteidigung und faires Verfahren nach Art. 6 EMRK und Art. 103 Abs. 1 GG (dazu unter C. 4.) und das Recht auf Privatleben nach Art. 8 EMRK (dazu unter C. 5.).

Gliederung

A. Sachverhalt

Der Beschwerdeführer ist Gewerkschafter und veröffentlicht im Rahmen dieser Tätigkeit journalistische Beiträge, in denen er von Veranstaltungen und Demonstrationen berichtet. Aufgenommen hat er diese Tätigkeit im Frühjahr 2020, ….

Am ... September 2023 begleitete der Beschwerdeführer eine Versammlung der Organisation „Letzte Generation“ in Bamberg. Ziel des Beschwerdeführers war dabei, mit den Teilnehmenden ins Gespräch zu kommen und anschließend über die Versammlung in der Zeitschrift … zu berichten.

Nach Ende der Versammlung beobachte der Beschwerdeführer mehrere polizeiliche Maßnahmen gegen drei Personen, die zuvor an der Versammlung teilgenommen haben.

Einer der in die Maßnahmen involvierten Polizeibeamt*innen gab an, beobachtet zu haben, wie der Beschwerdeführer mit seinem Mobiltelefon eine Sprachnotiz über das Geschehen anfertigte und absandte (Bl. … der Akte). Nachdem ihm der Tatvorwurf nach § 201 StGB eröffnet wurde (Bl. … der Akte), forderten die Polizeibeamt*innen ihn dazu auf, sein Mobiltelefon freiwillig herauszugeben. Nachdem der Beschwerdeführer dieses herausgab, einer Sicherstellung aber nicht zustimmte, erfolgte eine Beschlagnahme seines Mobiltelefons. Einen PIN zur Entsperrung gab der Beschwerdeführer nicht an (Bl. … der Akte).

Das Amtsgericht Bamberg bestätigte die Beschlagnahme des Mobiltelefons mit Beschluss vom ... September 2023 (Bl. … der Akte). In dem Beschluss stellte das Gericht fest, dass die Aufnahme und das Zugänglichmachen der Sprachnachricht an andere eine Straftat nach §§ 201 Abs. 1 Nr. 2, 205 StGB darstelle. Das Mobiltelefon sei als Beweismittel potentiell von Bedeutung. Es seien Gründe für die Annahme vorhanden, dass die Voraussetzungen für die Einziehung nach § 201 Abs. 5 StGB vorliegen. Die Maßnahme stehe auch im angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts und sei für die Ermittlungen notwendig.

Das Mobiltelefon wurde am ... Dezember 2023 zur Auswertung der Daten an einen Sachbearbeiter übermittelt (Bl. … der Akte). Die Auswertung erfolgte mittels einer forensischen Extraktionssoftware des Herstellers Cellebrite (Bl. … der Akte). Es wurden der Akte insgesamt sieben Extraktionsberichte beigefügt.

Die Extraktionssoftware von Cellebrite, insbesondere das 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 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 Speicherdump 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 Geostandorte 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.

Aus dem Ermittlungsbericht (Bl. ... der Akte) sowie einem weiteren Bericht („Sonstige Erkenntnisse Handydatenauswertung", Bl. … der Akte), beide vom ... Dezember 2023, ergibt sich, dass Inhalte des Mobiltelefons ausgewertet wurden, die keinen Bezug zu den Geschehnissen am ... September 2023 hatten.

Der Verfasser der Berichte räumt selbst ein, dass das Hauptaugenmerk bei der Durchsicht der Daten **„zunächst"** darauf lag, den Nachweis für die möglicherweise begangene Straftat nach § 201 StGB zu erbringen.

Die Beamt*innen werteten hierfür einen Chat des Anbieters Signal, der bis auf den Beschwerdeführer keine weiteren Teilnehmer*innen enthielt und somit als digitales Notizbuch bzw. digitaler Merkzettel diente, vollständig aus. Dieser „Chat" enthielt 87 Einzelnachrichten, davon neun Sprachnotizen, die jeweils mit einem Datum versehen sind. In dem ersten Extraktionsbericht der Akte sind aber nicht nur Notizen vom ... September 2023 enthalten, sondern der gesamte Nachrichtenverlauf des Chats. Insbesondere wurden alle neun Sprachnachrichten auf einem Datenträger gesichert sowie unter der Überschrift „Verschriftung Inhalt tatrelevanter Daten" durch die Polizei transkribiert und an die Staatsanwaltschaft übersendet (Bl. … der Akte). Acht der neun Aufnahmen enthalten ausschließlich die Stimme des Beschwerdeführers und beziehen sich auf seine Kommentare zum allgemeinen Geschehen nach der Demonstration.

Außerdem fand eine zusätzliche, stichprobenartige Auswertung der weiteren, auf dem Mobiltelefon abrufbaren Daten statt, wie sich aus dem Bericht „Sonstige Erkenntnisse Handydatenauswertung" (Bl. … der Akte) ergibt. Der zweite Bericht dokumentierte seine politischen Aktivitäten und Zugehörigkeiten im Allgemeinen. Dass diese weitergehende Auswertung nur

stichprobenartig erfolgt ist, wird damit begründet, dass eine detaillierte Auswertung mehrere Wochen Zeit in Anspruch genommen hätte (vgl. Bl. … der Akte).

Ausgewertet wurden insbesondere Bilddaten aus der Galerie, verschiedene Chats (jedenfalls Signal, Instagram) mit Text- und Sprachnachrichten, Mitgliedschaften in Chatgruppen und Newslettern. Teile der Auswertung wurden auf einer Daten-DVD gespeichert oder sind als Extraktionsberichte der Akte beigefügt. In dem Bericht werden auch Kontakt-Mailadressen aus den Newslettern festgehalten. Teil der Auswertung ist auch eine Nachricht, in der der Beschwerdeführer eine andere Person danach fragt, ob er eine Demo journalistisch begleiten könne (Bl. … der Akte).

Der Verfasser des Berichts zieht verschiedene Schlüsse aus seiner Auswertung:

- der Beschwerdeführer ließe sich der „linken Szene“ Bambergs eindeutig zuordnen
- Engagement in politisch-linker Szene
- Zugehörigkeiten und Verhältnis zu verschiedenen politisch motivierten Gruppierungen
- Verfolgung „sämtlich politisch-angehauchter Themenbereiche im Raum Bamberg bzw. von diesem ausgehend, speziell im Interesse der linken Szene“
- Abneigung des Beschwerdeführers gegenüber der Polizei

Am ...09.2024 wurde dem Beschwerdeführer sein Mobiltelefon zurückgegeben (vgl. Bl. … der Akte). Am ...2024 überließ er es 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 (RSF Digital Security Lab – Forensische Analyse … – **Anlage**).

B. Zulässigkeit

Die Beschwerde ist zulässig.

1. Statthaftigkeit

Der Beschwerdeführer richtet sich gegen die Beschlagnahme und Auswertung seines Mobiltelefons.

Die Beschwerde gegen den Beschluss des Amtsgerichts Bamberg vom ... September 2023 (Bl. ... d. Akte), mit welchem die Beschlagnahme des Mobiltelefons (…) des Beschwerdeführers vom ... September 2023 nach § 98 Abs. 2 StPO bestätigt wurde, ist gemäß § 304 Abs. 1 StPO statthaft.

2. Beschwerdeberechtigung

Der Beschwerdeführer war Beschuldigter in dem der Maßnahme zu Grunde liegendem Ermittlungsverfahren und mithin nach § 296 Abs. 1 Alt. 2 StPO Rechtsmittelberechtigter.

3. Rechtsschutzbedürfnis

Es besteht auch ein Rechtsschutzbedürfnis.

Die Beschwer ist nicht entfallen. Der Beschwerdeführer ist nach wie vor beschwert, da sich auf seinem Mobiltelefon forensische Rückstände der Analysesoftware in Form von veränderten Einstellungen am Betriebssystem befinden (dazu ausführlich unter B.1.c.aa.(1)) und nach wie vor vom Mobiltelefon extrahierte Daten gespeichert sind.

Zudem liegt ein Rechtsschutzbedürfnis vor, da es sich bei der vorliegenden Datenauswertung eines Mobiltelefons um einen schwerwiegenden Grundrechtseingriff handelt,

> grundlegend zum Rechtsschutzbedürfnis bei schwerwiegenden Grundrechtseingriffen: BVerfGE 96, 27 = NJW 1997, 2163.

Dies ist insbesondere bei Fällen anzunehmen, 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. Effektiver Grundrechtsschutz gebietet es dann, dass der

Betroffene Gelegenheit erhält, die Berechtigung des schwerwiegenden – wenn auch tatsächlich nicht mehr fortwirkenden – Grundrechtseingriffs gerichtlich klären zu lassen,

BVerfG, NJW 2007, 1117, 1120 f. m.w.N.

Die Bejahung eines derartig tiefgreifenden Grundrechtseingriffs kommt vor allem bei Anordnungen in Betracht, die das Grundgesetz vorbeugend Richter*innen vorbehalten hat,

BVerfG, NJW 2007, 1117, 1121 m.w.N.

Auch darüber hinaus können ist aber bei besonders schweren Grundrechtseingriffen von einem Rechtsschutzinteresse auszugehen, unabhängig davon, ob sie heimlich oder offen erfolgen,

Löwe-Rosenberg in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, Vorbemerkungen, Rn. 72 m.w.N.

Bei Auswertung eines Mobiltelefons handelt es sich um einen schwerwiegenden Grundrechtseingriff, sodass ein Rechtsschutzbedürfnis auch nach prozessualer Überholung besteht. Dies ergibt sich bereits aus dem Richtervorbehalt der Beschlagnahme. Hinzu kommt, dass die Handydatenauswertung schwer in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, jedenfalls in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, dazu ausführlich unter C.1. und 3.b.bb.), in die Eigentumsfreiheit (Art. 14 GG, dazu ausführlich unter C.3.b.bb.) sowie in die Pressefreiheit eingreift (Art. 5 Abs. 1 S. 2 Fall 1 GG, dazu ausführlich unter C.3.b.aa.).

Auch in Bezug auf die Rechtsschutzmöglichkeiten sind die Anforderungen des Bundesverfassungsgerichts erfüllt. Insbesondere Beschlagnahmeanordnungen sind ihrer Natur nach häufig vor möglicher gerichtlicher Überprüfung schon wieder beendet,

vgl. BVerfG, NJW 2007, 1117, 1121.

Hinzu kommt, dass die Einlegung einer Beschwerde nach § 307 Abs. 1 StPO die Vollziehung grundsätzlich nicht hemmt. Zwar kann das Gericht, der*die Vorsitzende oder der*die Richter*in, dessen Entscheidung angefochten wird, sowie auch das Beschwerdegericht anordnen, dass die Vollziehung der angefochtenen Entscheidung auszusetzen ist. Allerdings käme eine Aussetzung der Vollziehung der Beschlagnahme auch im Falle der Anordnung zu spät, da diese schon vollzogen war.

Dass im Anschluss an die vollzogene Beschlagnahme auch eine Auswertung des Mobiltelefons erfolgen und in welchem Umfang die Auswertung stattfinden wird, war für den

Beschwerdeführer zunächst nicht erkenntlich. Denn der Auswertungsvorgang sowie der Auswertungsumfang werden Betroffenen erst kenntlich gemacht, wenn sie Akteneinsicht gewährt bekommen und die Auswertung bereits vollzogen ist, da diese weder über eine beabsichtigte Auswertung benachrichtigt werden noch ein weiterer gerichtlicher Beschluss nötig ist.

Auch der Umfang der Datenauswertung ist 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, sodass ein Feststellungsinteresse vorliegend gegeben ist.

C. Begründetheit

Die Beschwerde ist auch begründet, da die Durchsicht des Mobiltelefons und die Auswertung der Daten rechtswidrig war. Es fehlt bereits an einer spezifischen Gesetzesgrundlage, die verfassungs- und unionsrechtlichen Vorgaben genügt (dazu unter 1. und 2.). Des Weiteren lag kein Anfangsverdacht vor (dazu unter 3.a.) und die streitgegenständlichen Maßnahmen waren im konkreten Einzelfall unverhältnismäßig (dazu unter 3.b.). Schließlich wurde der Beschwerdeführer in seinem Recht auf effektive Verteidigung und ein faires Verfahren nach Art. 6 EMRK und Art. 103 Abs. 1 GG (dazu unter 4.) sowie in seinem Recht auf Privatleben nach Art. 8 EMRK verletzt (dazu unter 5.).

1. Verfassungsrechtlich unzureichende gesetzliche Grundlage

Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie in das Grundrecht auf informationelle Selbstbestimmung müssen auf einer hinreichend bestimmten Ermächtigungsgrundlage beruhen (dazu unter c.bb.) und sind nur unter strengen verfassungsrechtlichen Rechtfertigungsanforderungen zulässig, insbesondere muss der Kernbereichsschutz (dazu unter c.cc.) und die Wahrung der Verhältnismäßigkeit gewährleistet sein (dazu unter c.dd.). Auch bedarf es klarer verfahrensrechtlicher Schranken, etwa in Form gerichtlicher Protokollierungspflichten, Eingrenzungsvorgaben oder der Möglichkeit effektiver Beteiligung von Verteidiger*innen (dazu unter (c.dd.(3))). Diesen Anforderungen werden die §§ 94 ff. StPO nicht gerecht.

a. Maßgebliches Grundrecht und Schutzbereich

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****“,*
> BVerfGE 120, 274 (312f.) [Hervorhebung durch Unterzeichnerin].

Auch trete 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. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (824 Rn. 168).

Aus der Rechtsprechung des Bundesverfassungsgerichts 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 an 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*“,
> BVerfG, Urteil v. 27. Februar 2008 – 1 BvR 370/07, juris Rn. 180 [Hervorhebung durch Unterzeichnerin].

Die Auswertung von Handydaten 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 RSF Digital Security Lab – Forensische Analyse … – **Anlage**). Gerade solche Gefahren werden vom grundrechtlichen Schutz der Integrität informationstechnischer Systeme abgedeckt,

> vgl. *Hoffmann-Riem*, JZ 2009, 1009 (1012); *Böckenförde*, JZ 2008, 925 (928); BVerfGE 120, 274 (314); *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.).

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 offene Datenzugriffe auch *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 167; *Hornung*, CR 2008, 299 (303); *Michalke*, StraFo 2008, 287 (291); *Polenz*, in: Kilian/Heussen, Computerrechts-Handbuch, EL 29 Feb. 2011, Teil 13 Rn. 32, siehe auch OLG Bremen, Beschluss v. 8. Januar 2025 – 1 ORs 26/24, juris Rn. 13; LG Ravensburg, Beschluss v. 14. Februar 2023 – 2 Qs 9/23 jug, juris Rn. 17.

Sofern frühere Gerichtsentscheidungen den Datenzugriff auf und die anschließende Datenauswertung von beschlagnahmten Datenträgern allein am Grundrecht auf informationelle Selbstbestimmung gemessen haben, ist dem seit der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung im Jahr 2008 nicht mehr zu folgen,

> vgl. BVerfG, Beschluss vom 12. 4. 2005 - 2 BvR 1027/02, NJW 2005, 1917 (1918 ff.); BVerfG, Urteil vom 2. 3. 2006, - 2 BvR 2099/04, NJW 2006, 976 (979, Rn. 82 ff.).

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. Auch Art und Umfang der gespeicherten Daten unterschieden sich erheblich von den vielfältigen und sensiblen Informationen, die moderne Smartphones enthalten. Nur die Entscheidung des Bundesverfassungsgerichts vom 2. 3. 2006 (Az. 2 BvR 2099/04) betraf die Beschlagnahme eines Mobiltelefons. Dabei ging es jedoch ausschließlich um die Durchsicht und

Auswertung von Telekommunikationsverbindungsdaten, was einen deutlich weniger intensiven Eingriff darstellt als die umfassende Auswertung des Datenbestandes eines modernen Smartphones. Die den damaligen Entscheidungen zugrunde liegende Gefahrenlage für das allgemeine Persönlichkeitsrecht ist daher 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. 6. 2009 - 2 BvR 902/06, NJW 2009, 2431 (2432 Rn. 51); bestätigt in BVerfG NJW 2014, 3085.

Diese Bewertung lässt sich nicht auf den Zugriff und die Auswertung komplexer IT-Systeme – insbesondere von Smartphones – übertragen, da 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 hinausgehen, 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. Eingriffsqualität

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

> so auch OLG Bremen, Beschluss v. 8. Januar 2025 – 1 ORs 26/24, juris Rn. 13.

Der anschließenden Durchsicht, Auswertung und Speicherung der Daten durch Mitarbeitende der Strafverfolgungsbehörden kommt jeweils eigenständige Eingriffsqualität zu. Werden dokumentierte und gespeicherte Daten im Ermittlungsverfahren weiter genutzt, erfolgt ein weiterer, vertiefter Grundrechtseingriff dadurch, dass die zuständigen Behörden die Daten als Grundlage

für weitere strafprozessuale Maßnahmen heranziehen können. Die Informationen können insbesondere in Vernehmungen aufgegriffen und zur Entwicklung weiterführender Ermittlungsansätze herangezogen werden. Unter bestimmten gesetzlichen Voraussetzungen kann zudem anderen Behörden – etwa zur Gefahrenabwehr oder zur Verhinderung zukünftiger Straftaten – ein Zugriff auf die gespeicherten Daten gewährt werden. Dadurch erweitert sich der Kreis der potentiell zugriffsberechtigten Stellen erheblich.

c. Verfassungsrechtliche Rechtfertigung

Der mit dem Datenzugriff und der Datenauswertung einhergehende Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist verfassungsrechtlich nicht zu rechtfertigen. Es handelt sich um einen Eingriff mit einer besonders hohen Intensität (dazu unter aa.), für dessen Rechtfertigung es eine spezifische, hinreichend bestimmte Ermächtigungsgrundlage bedarf (dazu unter bb.), die Schutzvorkehrungen für den Kernbereichsschutz (dazu unter cc.) sowie strenge Vorgaben für die Wahrung der Verhältnismäßigkeit vorsehen muss (dazu unter dd.). Diesen Anforderungen werden die §§ 94 ff. StPO nicht gerecht.

aa. Besonders hohe Eingriffsintensität

Der Zugriff auf den gesamten Datenbestand eines beschlagnahmten Mobiltelefons und die anschließende Datenauswertung und -speicherung nach §§ 94 ff. StPO 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 Tombstones 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 RSF Digital Security Lab – Forensische Analyse … – **Anlage**).

Die Verwendung von forensischer Auswertungssoftware wie der von Cellebrite geht somit mit erheblichen Gefahren für die Integrität des betroffenen Geräts einher. Diese Gefahren bleiben für die betroffene Person – insbesondere ohne tiefere technische Kenntnisse oder eigene Auswertungsmöglichkeiten – oft vollständig unbemerkt und steigern die Eingriffsintensität erheblich.

(2) **Umfang und Vielfalt der Daten**

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 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.

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

T. W. Boonstra, M. E. Larsen, H. Christensen (2015): Mapping dynamic social networks in real life using participants' own smartphones, abrufbar unter: https://www.cell.com/action/showPdf?pii=S2405-8440%2815%2930056-6; *C. Stachl, S. Hilbert, J.-Q. Au, D. Buschek, A. De Luca, B. Bischl, H. Hussmann, M. Bühner* (2017): Personality Traits Predict Smartphone Usage. Eur. J. Pers., 31: 701 – 722, abrufbar unter: https://www.researchgate.net/publication/318879569_Personality_Traits_Predict_Smartphone_Usage.

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 oder vertrauliche Forschungsdaten. Auch ermöglicht es moderne KI-Analysesoftware, bestehende Datenbestände mit neu erlangten Daten zu verknüpfen, was wiederum umfassende und detaillierte Einblicke erlaubt,

> vgl. *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 Rn. 1 m.w.N.

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 jegliche Art von Datenträgern und Daten 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,

> vgl. *Hartmann*, in: HK-GS, 5. Aufl. 2022, StPO § 110 Rn. 5, beck-online; *Gerhold*, in: BeckOK StPO mit RiStBV und MiStra, Graf, 54. Edition, Stand: 01.01.2025, § 94 Rn. 3 f. m.w.N.

(3) **Erhebliche Streubreite und weitreichende Zugriffsmöglichkeit**

Der Eingriff hat zudem eine erhebliche Streubreite. Es können alle Personen 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. Ed. 1.10.2024, StPO § 94 Rn. 7 sowie zur potentiellen Beweisrelevanz BVerfGE 120, 274 – 350.

Die Erhebung von Telekommunikationsverbindungsdaten und Kommunikationsinhalten hat zudem immer auch zur Folge, dass persönliche Daten Dritter miterhoben 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 27.2.2008 – 1 BvR 370/07,1 BvR 595/07, Rn. 233 – juris.

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,

> vgl. *Cornelius*, Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 (2726 Rn. 5); *Stam*, JZ 2023, 1070 (1074); vgl. BVerfGE 165, 363 = NJW 2023, 1196 (1201, 1205).

(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, ob und welche Daten die Ermittlungsbehörden auswerten (wollen). 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.

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 14.12.2023 – G 352/2021-46, BeckRS 2023, 36793, Rn. 75.

Zudem erhalten insbesondere Dritte, deren Daten auf einem ausgelesenen Handy enthalten sind, regelmäßig überhaupt keine Kenntnis des Eingriffs in ihre Daten. Diese erfahren allenfalls von der adressierten Person von dem Datenzugriff, 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 v. 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, stellt sich der „offene" Datenzugriff als heimlich dar und ist durch eine hohe Intensität gekennzeichnet, da sich im Rahmen der vertrauten Kommunikation, möglicherweise über Jahre, eine Vielzahl von Daten findet,

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

(5) **Vergleichbarkeit der Eingriffsintensität**

Jedenfalls ist ein Datenzugriff auf beschlagnahmte Mobiltelefone 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 v. 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*",
> BVerfG, Beschluss v. 14. November 2024 – 1 BvL 3/22, juris Rn. 93 zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung

[Hervorhebungen durch die Unterzeichnerin]; ähnlich bereits BVerfG, Beschluss v. 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 v. 27. Februar 2008 – 1 BvR 370/07, juris Rn. 230.

In der strafrechtlichen Literatur wird 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.

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

vgl. *Cornelius*: Datenauswertung bei beschlagnahmten komplexen IT-Systemen, NJW 2024, 2725 Rn. 3 (2727 Rn. 11).

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

vgl. *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“.

Zudem ist zu befürchten, dass Menschen in Deutschland nicht mehr frei und unbeschwert digital kommunizieren, um zu verhindern, dass die Behörden an ihre Daten kommen können,

vgl. zu diesem „chilling effect“ schon BVerfG, Urteil v. 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 v. 6. Juni 2024 – 36559/19, juris; Urteilsgründe in französischer Sprache unter https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-234090%22]}.

bb. Rechtswidrigkeit der Maßnahme

Vor dem Hintergrund des hohen Eingriffsgewichts stellt sich die Maßnahme als rechtswidrig dar.

(1) **Verstoß gegen das Gebot der Normenklarheit und Normenbestimmtheit**

Für einen auf §§ 94 ff. StPO gestützten Datenzugriff und die anschließende Auswertung fehlt es an einer spezifischen, hinreichend bestimmten Ermächtigungsgrundlage, die den damit verbundenen schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme rechtfertigen könnte.

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

BVerfG, Urteil des Ersten Senats 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,

> z.B. BVerfGE 150, 1 (96 Rn. 191 m.w.N.); grundlegend schon BVerfGE 33, 125 (159 ff., insb. 163); BVerfGE 40, 237 (248 f. Rn. 45); BVerfGE 49, 89 (126 Rn. 76); *Denninger*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, B. Rn. 58.

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.); BVerGE 162, 378.

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

> BVerfG, Urteil v. 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 könnten,

> BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, 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 die Bestimmtheit zu stellen,

> vgl. BVerfG, Beschluss vom 8. 8. 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1784 Rn. 105).

Ein auf die §§ 94 ff. StPO gestützter Datenzugriff sowie die anschließende Datenauswertung genügen diesen Anforderungen nicht. Der schwerwiegende Grundrechtseingriff wird auf eine gesetzliche Grundlage gestützt, die in ihrem Wortlaut den kompletten Zugriff auf und die umfassende Auswertung von Daten, die sich auf beschlagnahmten Datenträgern befinden, überhaupt nicht regelt. Das Ausmaß und die Grenzen der Datenauswertung, die Art der technischen Durchführung sowie Rückgabefristen können derzeit lediglich im Einzelfall durch den Inhalt der gerichtlichen Beschlagnahmeanordnung nach § 98 Abs. 1 StPO bestimmt werden. Dabei handelt es sich aber nicht um eine verpflichtende Angabe. Dies spiegelt sich in der Praxis: Regelmäßig beziehen sich solche Anordnungen nur auf die Beschlagnahme an sich und erwähnen noch nicht einmal eine anschließend mögliche Datenauswertung. Dies führt dazu, dass diese im Ermessen der Strafverfolgungsbehörden stehen.

Sofern frühere gerichtliche Entscheidungen in den §§ 94 ff. StPO eine hinreichend bestimmte Ermächtigungsgrundlage für die Beschlagnahme und Auswertung von Datenträgern und Daten gesehen und für ausreichend gehalten hat, wenn der besonderen Eingriffsintensität im Einzelfall gerecht wird, ist dies anhand der neueren Rechtsprechung des Bundesverfassungsgerichts nicht mehr tragbar (siehe oben a.),

> vgl. BVerfG, Beschluss vom 12. 4. 2005 - 2 BvR 1027/02, NJW 2005, 1917; BVerfG, Urteil vom 2. 3. 2006, - 2 BvR 2099/04, NJW 2006, 976; BVerfG, Urteil vom 16. 6. 2009 - 2 BvR 902/06, NJW 2009, 2431; bestätigt in BVerfG NJW 2014, 3085.

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

Dabei ist bei der Beurteilung der Gefahrenlage insbesondere die technische Weiterentwicklung von Datenträgern und das damit einhergehende veränderte Nutzungsverhalten zu berücksichtigen. So hat auch das Bundesverfassungsgericht 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 , NJW 2016, 1781 (1783 Rn. 99).

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

Mit der neuen verfassungsgerichtlichen Rechtsprechung ist gerade nicht davon auszugehen, dass der Verwendungszweck durch eine Begrenzung der Maßnahme auf den Ermittlungszweck, der sich einzig aus dem Normenzusammenhang ergebe, ausreichend sein könnte,

entgegen BGH, Urteil vom 13. März 2025, 2 StR 232/24, Rn. 46.

Die Einschränkung auf den Ermittlungszweck ist bereits vollkommen ungeeignet ist, der Gefahr einer umfassenden Ausforschung der Persönlichkeit zu begegnen. Dieses Risiko realisiert sich bereits mit dem freien Zugang zum gesamten Datenbestand eines Datenträgers; berechtigte Vertraulichkeits- und Integritätserwartungen der Betroffenen werden zu diesem Zeitpunkt schon beeinträchtigt. Auch verhindert die Beschränkung auf den Ermittlungszweck nicht, dass Strafverfolgungsbehörden zunächst den gesamten Datenbestand umfassend durchleuchten, um anschließend bewerten zu können, welchen Informationen eine Beweisrelevanz zukommt und welchen nicht. Besonders Mobiltelefone enthalten eine Vielzahl (sensibler) Daten, die potentiell für den Nachweis einer Straftat in Frage kommen und durchforstet werden können (z.B. Geolokationsdaten, private Bilder, Videos und Kommunikationsinhalte). Moderne Analyseprogramme ermöglichen 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 eine derart weitreichende Durchsicht und Auswertung der Daten fehlen gesetzliche Schranken.

Ebenso reicht der allgemeine Verhältnismäßigkeitsgrundsatz gerade nicht aus, um der hohen Eingriffsintensität Rechnung zu tragen. Nach der Wesentlichkeitstheorie sowie dem Gebot der Normenbestimmtheit muss der Gesetzgeber die Grenzen der staatlichen Befugnis mit Blick auf den spezifischen Eingriff eigenständig regeln und Fälle ausschließen, in denen der Eingriff unverhältnismäßig wäre.

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

(2) **Fehlender Kernbereichsschutz**

Für den im Rahmen der §§ 94 ff. StPO durchgeführten Datenzugriff und die anschließende Datenauswertung 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 I GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen,

> BVerfG, Urteil vom 20.4.2016 – 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1786 Rn. 121).

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

> vgl. BVerfGE 109, 279 [314] = NJW 2004, 999; BVerfGE 120, 274 [339] = NJW 2008, 822; 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,

> vgl. BVerfG, Urteil vom 20.4.2016 – 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 = NJW 2016, 1781 (1787 Rn. 126); BVerfG, Beschluss vom 9.12.2022 – 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,

> vgl. BVerfG, Urteil vom 20.4.2016 – 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 = NJW 2016, 1781 (1787 Rn. 123); BVerfG, Beschluss vom 9.12.2022 – 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, erlauben die §§ 94 ff. StPO den Zugriff auf alle Daten, die auf den beschlagnahmten Datenträgern vorhanden sind (s.o. a. bb.). Insbesondere enthalten Mobiltelefone typischerweise Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind (Kommunikationsinhalte, intime Bilder und Videos etc.). Auch das Bundesverfassungsgericht ging bereits in der 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 v. 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 v. 16. Juni 2009 – 2 BvR 902/06, NJW 2009, 2431 (2436 f. Rn. 90).

Das ist beim Auslesen von Smartphones gerade nicht der Fall.

(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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09NJW 2016, 1781 (1787 Rn. 219), BVerfG, Beschluss vom 9.12.2022 – 1 BvR 1345/21, ZD 2023, 346 (347 Rn. 109.

In seiner Entscheidung zur akustischen Wohnraumüberwachung hat das Bundesverfassungsgericht 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. 3. 2004 - 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999 (1003).

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

> vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09NJW 2016, 1781 (1787 Rn. 128), Rn. 113 ff.

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*, NJW 2024, 2725, 2726.

Die Strafverfolgungsbehörden dürfen im Anschluss an die Beschlagnahme bzw. im Rahmen der Durchsicht sämtliche auf dem Datenträger gespeicherte Informationen auswerten, ohne zwischen potentiell kernbereichsrelevanten und weniger sensiblen Daten zu differenzieren. Die bloße Zweckbindung der Maßnahme an den Ermittlungszweck stellt dabei keine hinreichende Schutzvorkehrung dar. 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. Schließlich birgt bereits die Möglichkeit des Zugangs zum gesamten Datenbestand eine hohe Missbrauchsgefahr.

Zwingend erforderlich und ohne Weiteres möglich wäre eine Regelung entsprechend § 100d Abs. 1 und Abs. 3 Satz 1 StPO, welche einen wirksamen Kernbereichsschutz sicherstellt, indem der Datenzugriff ausgeschlossen wird, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch ihn allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden und 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 NJW 2016, 1781 (1787 Rn. 129 m.w.N.), BVerfG, Beschluss vom 9.12.2022 – 1 BvR 1345/21, ZD 2023, 346 (348 Rn. 117).

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

> BVerfG, Beschluss vom 9.12.2022 – 1 BvR 1345/21, ZD 2023, 346 (349 Rn. 119).

Darüber hinaus stellt das Bundesverfassungsgericht 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 sich dann als kernbereichsrelevant erwiesen, sofort gelöscht oder sonst vernichtet und jegliche Verwendung unterlassen sowie in einer Weise dokumentiert werden, die eine spätere Kontrolle ermögliche. 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 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 NJW 2016, 1781 (1787 Rn. 129); BVerfG, Beschluss vom 9.12.2022 – 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 die §§ 94 ff. StPO weder Löschungsverpflichtungen noch Verwendungsverbote oder Dokumentationspflichten.

(3) **Verhältnismäßigkeit**

Ein auf §§ 94 ff. StPO gestützter Datenzugriff und die anschließende Datenauswertung sind unverhältnismäßig, da die Vorschriften keine hinreichenden tatbestandlichen Begrenzungen auf angemessene Fälle vorsehen. Die hohe Eingriffstiefe und -intensität begründen hohe gesetzliche Anforderungen an die Wahrung der Verhältnismäßigkeit. Diesen genügen die §§ 94 ff. StPO nicht, da sie weder Beschränkungen hinsichtlich der Anlasstat vorsehen (dazu unter (a)) noch hinreichende Vorgaben zur erforderlichen Erfolgstauglichkeit enthalten (dazu unter (b)).

(a) **Beschränkung der Anlasstat**

Die §§ 94 ff. StPO enthalten keine tatbestandlichen Beschränkungen in Bezug auf die Anlasstat und genügen damit nicht dem Verhältnismäßigkeitsgrundsatz.

Die hohe Eingriffsintensität des Datenzugriffs und der Datenauswertung wirkt sich dahingehend aus, dass die Maßnahme nur zum Schutz hinreichend gewichtiger Rechtsgüter dienen darf. Das Bundesverfassungsgericht 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 20.4.2016 – 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 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“; *T. 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,

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).

(b) **Qualifizierte Beweisrelevanz**

Darüber hinaus fehlen in den §§ 94 ff. StPO hinreichende gesetzliche Vorgaben zur erforderlichen Erfolgstauglichkeit. Aufgrund der hohen Eingriffsintensität und der hohen Anfälligkeit der Beschlagnahme von komplexen IT-Geräten wie Smartphones ist eine über die einfache Beweisrelevanz hinausgehende Erfolgswahrscheinlichkeit im Sinne einer „konkreten fallbezogenen Erfolgstauglichkeit“ der Maßnahme verfassungsrechtlich geboten, um die Wahrung der Verhältnismäßigkeit zu gewährleisten. Dieser Grad der Erfolgstauglichkeit erfordert, dass Tatsachen die Annahme rechtfertigen, dass die Auswertung der Daten zur Ergreifung des Täters oder zur Aufklärung der Straftat führen kann,

vgl. *El-Ghazi*, Gutachten C zum 74. Deutschen Juristentag, 2024, S. C 81 m.w.N.; vgl. zum Erfordernis der konkreten fallbezogenen Erfolgstauglichkeit im Rahmen des § 163d Abs. 1 StPO *Moldenhauer*, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage 2023, § 163d Rn. 15.

Derzeit darf eine Beschlagnahme und die anschließende Datenauswertung nach §§ 94 ff. StPO bereits erfolgen, wenn das betroffene Gerät 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 1.10.1987 - 2 BvR 1178/86 u. a., NJW 1988, 890 (894); BVerfG, Beschluss vom 16.8.1994 - 2 BvR 983, 1258/94, NJW 1995, 385; BGH 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 23.04.2020 – 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,

vgl. *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,

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

(c) **Fehlende Auskunfts-, Löschungs-, Dokumentations- und Beteiligungspflichten**

Zur Wahrung der Verhältnismäßigkeit einer gesetzlichen Ermächtigung zur Datenverarbeitung bedarf es auch verfahrensrechtlicher Sicherungen, die die Transparenz der Datenverwendung und dadurch einen effektiven Rechtsschutz und effektive Sanktionen gewährleisten,

vgl. BVerfGE 65, 1 (46); 113, 29 (57 f.); 120, 351 (361).

Aufgrund der besonders hohen Eingriffsintensität gehören dazu auch strenge Vorgaben hinsichtlich gerichtlicher Protokollierungspflichten, Eingrenzungsvorgaben und der Möglichkeit effektiver Beteiligung von Verteidiger*innen.

So hat das Bundesverfassungsgericht bereits hinsichtlich Eingriffen in das Recht auf informationelle Selbstbestimmung ausgeführt, dass den Verfahrensgarantien seit jeher ein hoher Stellenwert eingeräumt werde,

BVerfG, Beschluss vom 12. 4. 2005 - 2 BvR 1027/02, NJW 2005, 1917 (1922 IV. 1.).

Darüber hinaus bestehe dem Gericht zufolge das Gebot,

> „*im Hinblick auf das Recht auf informationelle Selbstbestimmung die Entwicklung der Datenerhebung, Datenspeicherung und Datenverwertung zu beobachten und gegebenenfalls über ergänzende rechtliche Rahmenbedingungen nachzudenken* […]. *Der begrenzte Zweck der Datenerhebung gebietet jedenfalls grundsätzlich die Löschung aller nicht zur Zweckerreichung erforderlichen kopierten Daten. Um Verhältnismäßigkeitsgrundsatz und Verfahrensrechte nicht fruchtlos bleiben zu lassen, gebietet das Grundgesetz in bestimmten Fällen ein Verwertungsverbot*“,
> BVerfG, Beschluss vom 12.4.2005 - 2 BvR 1027/02, NJW 2005, 1917 (1922 IV. 1.).

Auch Art. 5 der Richtlinie (EU) 2016/680 (nachfolgend JI-Richtlinie) verpflichtet Mitgliedstaaten dazu, dass sie für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen haben und sie durch verfahrensrechtliche Vorkehrungen sicherstellen, dass diese Fristen eingehalten werden (zur Anwendbarkeit der JI-Richtlinie siehe unten 2.). Darüber hinaus müssen Mitgliedstaaten nach Art.14 der JI-Richtlinie gesetzlich vorsehen, dass die betroffene Person das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall hat die betroffene Person nach Art. 14 lit. d) und e) der JI-Richtlinie das Recht, Auskunft über personenbezogene Daten und u.a. zur, falls möglich, geplanten Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, der Kriterien für die Festlegung dieser Dauer und zum Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen zu erhalten.

In den §§ 94 ff. StPO fehlen solche Transparenz- und Auskunftspflichten sowie Protokollierungspflichten und Vorgaben zur Ermöglichung effektiver Beteiligung von Verteidiger*innen, die zur Wahrung der Verhältnismäßigkeit notwendig sind. Nachdem der Datenträger beschlagnahmt wurde, hat die betroffene Person keine unmittelbare Möglichkeit zu erfahren, auf welche Art und in welchem Umfang Daten erhoben und ausgewertet werden, und darauf Einfluss zu nehmen. 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. Da es sich gerade nicht um eine heimliche Maßnahme handelt, ist auch nicht ersichtlich, warum Transparenzanforderungen der Effektivität der Maßnahme entgegenstehen sollten. Würde den Betroffenen bekanntgegeben, welche Daten von ihnen erhoben werden, milderte dies die diffuse Bedrohlichkeit der Datenspeicherung ab,

vgl. BVerfGE 125, 260 (335).

d. Grundrecht auf informationelle Selbstbestimmung

Selbst wenn man vorgehend davon ausgehen würde, dass kein Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bestünde, würde dies nicht zur Rechtmäßigkeit von auf §§ 94 ff. StPO gestützte Handydatenauswertung führen. So besteht bereits unabhängig vom konkret betroffenen Grundrecht ein erhebliches Eingriffsgewicht, dass sich aus den technischen Eingriffs- und Verarbeitungsmöglichkeiten, dem Umfang, der Art und der Vielfalt der Daten, der erheblichen Streubreite und den weitreichenden Zugriffsmöglichkeiten sowie der fehlenden Transparenz hinsichtlich des Umfangs der Maßnahme ein mit Überwachungsmaßnahmen wie der Online-Durchsuchung vergleichbares Eingriffsgewicht. Dementsprechend sind auch vergleichbare verfassungsrechtliche Anforderungen zu stellen.

Darüber hinaus bestehen auch hinsichtlich Eingriffen in das Recht auf informationelle Selbstbestimmung nach neuerer verfassungsgerichtlicher Rechtsprechung höhere verfassungsrechtliche Anforderungen. Selbst abgesenkten Anforderungen werden die §§ 94 ff. StPO aber nicht gerecht. Vielmehr werden die Anforderungen an Bestimmtheit, Kernbereichsschutz und Verhältnismäßigkeit, insbesondere in Bezug an Ermittlungsschwelle und Kontroll- und Transparenznormen weit verfehlt.

2. Unionsrechtswidrigkeit

Die Anwendung der §§ 94 ff. StPO auf den Zugriff und die Auswertung der sich auf beschlagnahmten Mobiltelefonen befindlichen Daten verstößt gegen Art. 4 Abs. 1 lit. c der JI-Richtlinie und ist damit unionsrechtswidrig. Die Vorschriften entsprechen nicht den unionsrechtlichen Mindestanforderungen an eine gesetzliche Grundlage, die einen solchen Eingriff rechtfertigen könnte.

a. Anwendbarkeit Unionsrecht

Der Anwendungsbereich der JI-Richtlinie ist eröffnet. Sie gilt gemäß 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 EuGH 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 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 72 ff.

Der BGH bestätigte in seinem Beschluss vom 13.03.2025, dass solche Maßnahmen, die auf §§ 94 ff. StPO gestützt werden und dem Datenzugriff auf Mobiltelefone und der anschließenden Datenauslese und -auswertung dienten, als Verarbeitung im Sinne des Art. 3 Nr. 2 der JI-Richtlinie seinem Anwendungsbereich unterfallen,

> BGH, Beschluss vom 13.03.2025 – 2 StR 232/24, BeckRS 2025, 9876, Rn. 29 ff., 45, 49 ff.

Im vorliegenden Fall hat die zuständige Strafverfolgungsbehörde mithilfe einer forensischen Extraktionssoftware des Herstellers Cellebrite das Mobiltelefon des Beschwerdeführers entsperren lassen und dadurch einen Zugriff auf den gesamten Datenbestand erwirkt, welcher anschließend umfassend ausgewertet wurde. Eine Datenverarbeitung im Sinne des Art. 3 Nr. 2 der JI-Richtlinie ist somit zwingend anzunehmen,

> vergleiche bestätigende Auffassung, dass die §§ 94 ff. StPO und § 110 Abs. 3 StPO insbesondere hinsichtlich Zulässigkeitsvoraussetzungen, Verfahrensanforderungen und Eingriffsschwellen grundsätzlich dem Anwendungsbereich der Richtlinie unterfallen: *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 635ff, sowie BGH, Beschluss vom 13.03.2025 – 2 StR 232/24, BeckRS 2025, 9876, Rn. 28 ff.

b. Anforderungen des EuGH aus seiner „Bezirkshauptmannschaft Landeck“-Entscheidung

In seiner „Bezirkshauptmannschaft Landeck“-Entscheidung vom 4. Oktober 2024 entwickelt der EuGH unionsrechtliche Anforderungen an die Vereinbarkeit des Datenzugriffs auf Mobiltelefone aus den Vorgaben der JI-Richtlinie hinsichtlich der Ausgestaltung der Rechtsgrundlage (aa.), denen im vorliegenden Fall die §§ 94 ff. StPO nicht genügen (bb.).

aa. Maßstab

In seiner „Bezirkshauptmannschaft Landeck“-Entscheidung stellt der EuGH klar, dass eine gesetzliche Grundlage, die den Datenzugriff auf Mobiltelefone ermöglicht, nur dann mit der JI-Richtlinie vereinbar sei, wenn sie dem in Art. 4 Abs. 1 lit. c JI-Richtlinie angelegten Grundsatz der Datenminimierung entsprächen. Die Vorschrift sieht vor, dass personenbezogene Daten dem Verarbeitungszweck entsprechen müssen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind. Sie ist im Lichte der Art. 7, 8 GrCh sowie von Art. 52 Abs. 2 GrCH auszulegen,

> vgl. EuGH, Urteil vom 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 81 ff..

Art. 7, 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 09.11.2010, 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 gemäß 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 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 93; sowie bestätigend BGH, Beschluss vom 13.03.2025 – 2 StR 232/24, 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 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 94; EuGH, Urteil vom 22.06.2021, C-439/19, EU:C:2021:504, Rn. 74.

Nach der ständigen Rechtsprechung des EuGH müssen bei solchen Grundrechtseinschränkungen die Anforderungen des Art. 52 Abs. 1 GrCH eingehalten werden, 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 4.10.2024 – 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 EuGH für eine gesetzlichen 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]*“,

EuGH, Urteil vom 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 99 [Hervorhebungen durch Unterzeichnerin].

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 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 90.

Ferner bedarf es nach der Rechtsprechung des EuGH 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 nur auf die Beschlagnahme beziehen darf, sondern eigenständig (auch) den Datenzugriff und dessen Reichweite selbst umfassen muss. Der EuGH führt dazu Folgendes 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“,

EuGH, Urteil vom 4.10.2024 – C 548/21, C.G., ECLI:EU:C:2024:830, Rn. 102 ff. [Hervorhebungen durch die Unterzeichnerin].

bb. Unvereinbarkeit mit Unionsrecht

Die Anwendung der §§ 94 ff. StPO als Ermächtigungsgrundlagen für einen Datenzugriff und die anschließende Datenauswertung werden den Maßstäben des EuGH nicht gerecht. Zunächst 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 (s.o. 1.a.bb.). Zwar hat der Bundesgerichtshof in seiner jüngsten Entscheidung zu einem Datenzugriff auf beschlagnahmte Datenträger keine Unvereinbarkeit der §§ 94 ff. StPO mit der Rechtsprechung des EuGH 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 13.03.2025 – 2 StR 232/24, Rn. 50.

Jedoch übersieht der Bundesgerichtshof, dass der EuGH in seiner Entscheidung die allgemeinen Anforderungen an den Gesetzesvorbehalt für Datenzugriffe verschärft: Er verlangt ausdrücklich, dass der **Gesetzgeber** „Art oder die Kategorien der betreffenden Straftaten, hinreichend präzise definieren" muss,

EuGH, Urteil vom 4.10.2024 – 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 EuGH weder vollständig noch zutreffend angewandt.

Ferner mangelt es an einem Gerichtsvorbehalt hinsichtlich des Datenzugriffs und der anschließenden Auswertung. Insoweit, als die §§ 94 ff. StPO einen gerichtlichen Beschluss für die Beschlagnahme anordnen, entspricht dies nicht den Vorgaben des EuGH 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 richterliche Kontrolle, die sich auf eine bloße „blanket approval" beschränkt, 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, 8 GrCh durch eine vorherige Überprüfung durch eine unabhängige Stelle sicherstellt.

c. Rechtsfolge

Die §§ 94 ff. StPO sind mit Art. 4 Abs. 1 Buchst. c der JI-Richtlinie, der im Lichte der Art. 7, 8 GrCH und von Art. 52 Abs. 1 GrCH auszulegen ist, somit unvereinbar und als Rechtsgrundlage für einen Datenzugriff und die anschließende Auswertung im vorliegenden Falle unionrechtswidrig.

Selbst wenn das Gericht der Ansicht sein sollte, dass eine verfassungskonforme Rechtsgrundlage besteht, müssen diese in Bezug auf Smartphones unionrechtskonform ausgelegt und bei Handydatenauswertungen unangewendet bleiben.

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.

Hilfsweise wird zur Klärung etwaiger verbleibender unionsrechtlicher Zweifel um die Vorlage an den EuGH gem. Art. 267 AEUV angeregt.

3. Rechtswidrigkeit der konkreten Maßnahme

Im vorliegenden Fall war die Maßnahme auch in seiner konkreten Ausführung rechtswidrig. Es lag weder der Tatbestand vor (unter a.) noch wurde das Ermessen fehlerfrei ausgeübt (unter b.)

a. Fehlender Anfangsverdacht

Der zugrunde gelegte Anfangsverdacht einer Straftat gem. § 201 Abs. 1 Nr. 2 StGB ist nicht tragfähig. Für einen Verstoß gegen den § 202 Abs. 1 Nr. 2 StGB fehlte die „Nichtöffentlichkeit des gesprochenen Wortes“. Der Beschwerdeführer durfte das Gesagte aufnehmen. Die beanstandete Sprachaufzeichnung erfolgte während einer für jedermann sichtbaren und hörbaren polizeilichen Maßnahme auf offener Straße. Der Begriff des „nichtöffentlich gesprochenen Wortes“ im Sinne des § 201 Abs. 1 StGB setzt Vertraulichkeit voraus, die bei einer Aufnahme des im Rahmen einer polizeilichen Maßnahme durch die Beamt*innen gesprochenen Wortes im öffentlichen Raum nicht vorliegt; das Vorliegen einer faktischen Öffentlichkeit reicht dabei aus, d.h. der Umstand, dass beliebige andere Personen von frei zugänglichen öffentlichen Flächen oder allgemein zugänglichen Gebäuden und Räumen die Diensthandlungen hätten beobachten und akustisch wie optisch wahrnehmen können,

> so auch Landgericht Osnabrück, Beschluss vom 24.09.2021, Az. Qs 49/21; LG Kassel Beschluss vom 23.9.2019, Az. 2 Qs 111/19, BeckRS 2019, 38252; LG Aachen Beschluss vom 19.8.2020, Az. 60 Qs 34/20, BeckRS 2020, 43645; LG Köln, Beschluss vom

03.09.2020 – 111 Qs 45/20, BeckRS 2020, 43318; AG Frankenthal Beschluss vom 16.10.2020, Az. 4b Gs 1760/20, BeckRS 2020, 28894; AG Mainz, Beschluss vom 8. Januar 2021 – 409 Gs 3282/20; LG Essen Urteil vom 23.11.2021, Az. 31 Ns-57 Js 867/19-31/21, BeckRS 2021, 42833 sowie LG Hamburg, Beschluss vom 21.12.2021 – 610 Qs 37/21.

Auch im vorliegenden Fall war eine solche Vertraulichkeit ersichtlich nicht gegeben. Die Kommunikation erfolgte tagsüber, in öffentlicher, von zahlreichen Menschen frequentierter Umgebung unter Beteiligung mehrerer unbeteiligter Dritter. Bereits die Annahme des Anfangsverdachtes war daher willkürlich und rechtswidrig.

b. Verletzung des Verhältnismäßigkeitsgrundsatzes im Einzelfall

Jedenfalls aber war die Beschlagnahme des Mobiltelefons sowie der Zugriff, die Auswertung und die Speicherung der sich darauf befindlichen Daten im vorliegenden Fall nicht verhältnismäßig. Selbst wenn man einen Anfangsverdacht unterstellen würde, so wäre die Maßnahme weder erforderlich noch angemessen. Insbesondere lag eine erhebliche Verletzung der Pressefreiheit des Beschwerdeführers vor.

aa. Schwerwiegende Verletzung der Pressefreiheit

(1) Gravierender Eingriff in die Pressefreiheit

Der Beschwerdeführer ist in seiner Pressefreiheit nach Art. 5 Abs. 1 Satz 2 GG betroffen, da er als Journalist tätig ist und gerade in dieser Funktion am ... September 2023 in Bamberg als Demonstrationsbeobachter vor Ort war.

Der Schutzbereich der Pressefreiheit erstreckt sich auf alle wesensmäßig mit der Pressearbeit zusammenhängenden Tätigkeiten, die von der medienspezifischen Informationsbeschaffung bis zur Art und Weise der Verbreitung der Nachricht und Meinung reichen,

BVerfGE 103, 44/59; BVerfGE 20, 162/176; BVerfGE 91, 125/134; *Jarass*, in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, 18. Auflage 2024, GG Art. 5 Rn. 36.

Auch wird insbesondere das Vertrauensverhältnis zwischen Informant*innen und Presse geschützt,

BVerfGE 20, 162/176; BVerfGE 117, 244/259.

Die Beschlagnahme und umfassende Auswertung seines Smartphones sind gravierende Eingriffe in die Pressefreiheit des Beschwerdeführers. Der Staat erhält insbesondere Zugriff auf Informationen über seine journalistischen Quellen und auf seine vertrauliche Kommunikation mit diesen. Auch verhinderten die Beschlagnahme und Einbehaltung des Mobiltelefons die weitere Ausübung seiner journalistischen Tätigkeit.

(2) **Fehlende Erforderlichkeit und Angemessenheit**

Dieser Eingriff ist weder erforderlich noch angemessen. Der Zugriff auf und die Auswertung von Informationen, die Bezug zu seiner journalistischen Tätigkeit haben, stehen in keinem Zusammenhang zum Strafvorwurf. Darüber hinaus war es ihm durch die Beschlagnahme seines Mobiltelefons nicht mehr möglich, über die Demonstration medial zu berichten, da seine Aufzeichnungen auf dem Gerät gespeichert waren. Den Ermittlungsbehörden war bewusst, dass der Beschwerdeführer als Journalist tätig ist. Denn Teil der Auswertung war eine Nachricht, in der der Beschwerdeführer eine andere Person danach fragte, ob er eine Demo journalistisch begleiten könne (siehe oben unter A.). Spätestens in diesem Zeitpunkt hätte die Auswertung abgebrochen werden müssen. Dies war, jedenfalls so weit aus der Akte ersichtlich, nicht der Fall. Eine Auseinandersetzung mit der Pressefreiheit fand an keiner Stelle statt.

Im Rahmen der weiteren Auswertung zur Erstellung eines politischen Profils wurden vor allem Kontaktpersonen des Beschwerdeführers analysiert. Darunter befinden sich auch Personen, zu denen der Beschwerdeführer im Rahmen seiner journalistischen Tätigkeit Kontakt hält und die dem Quellenschutz unterliegen. Durch die Auswertung durch die Polizei wurde dieser Aspekt eklatant missachtet.

Eine derart weitgehende Ausforschung journalistischer Quellen und vertraulicher Kommunikationsinhalte kann eine starke abschreckende Wirkung auf potentielle Informant*innen entfalten (sog. „chilling effect“). Aus Furcht vor staatlicher Überwachung könnten diese künftig davon Abstand nehmen, Kontakt zur Presse aufzunehmen. Ein derartiger Vertrauensverlust gefährdet

nicht nur im konkreten Einzelfall, sondern auch generell die Funktionsfähigkeit freier und unabhängiger Berichterstattung.

Darüber hinaus stellt die Einbehaltung des Mobiltelefons über einen Zeitraum von mehr als einem Jahr eine erhebliche Beeinträchtigung der journalistischen Tätigkeit des Beschwerdeführers dar. Während dieser Zeit war ihm weder der Zugriff auf frühere Kommunikationsinhalte und Notizen noch auf bisherige geschäftliche Kontakte möglich, was seine berufliche Arbeit nachhaltig erschwert hat.

bb. Erhebliche Verletzung des allgemeinen Persönlichkeitsrechts sowie der Eigentumsfreiheit

(1) **Erheblicher Eingriff in das allgemeine Persönlichkeitsrecht sowie in die Eigentumsgarantie**

Die richterlich bestätigte Beschlagnahme und Auswertung des Mobiltelefons stellen auch im Einzelfall einen erheblichen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, siehe dazu oben 1.), jedenfalls in das Grundrecht auf informationelle Selbstbestimmung mit besonders hoher Intensität dar. Vorliegend haben sich die Ermittlungsbehörden mit Hilfe einer Forensik-Software Zugriff auf den gesamten Datenbestand des Mobiltelefons des Beschwerdeführers verschafft und im großen Rahmen sensible und vertrauliche Daten ausgewertet und gespeichert, u.a. private Fotos und Kommunikationsinhalte mit unbeteiligten Dritten (siehe oben unter A.).

Außerdem ist die Eigentumsgarantie des Beschwerdeführers aus Art. 14 Abs. 1 GG betroffen. Die Beschlagnahme des Geräts über einen derart langen Zeitraum (mehr als ein Jahr) hinweg kommt einer faktischen Enteignung gleich. Dem Beschwerdeführer wird dauerhaft der Zugriff auf ein essenzielles Gerät und alle darauf gespeicherten Daten wie Kontakte, Bilder und Dokumente entzogen. Da er das Mobiltelefon auch beruflich nutzte, wird dadurch seine Teilnahme sowohl am privaten als auch am geschäftlichen Verkehr erheblich gestört und er in seiner Lebensführung stark eingeschränkt. Eine solche Maßnahme bedarf besonderer Rechtfertigung, die hier weder im Beschluss dargelegt noch in der Durchführung beachtet wurde,

> vgl. für die vorläufige Sicherstellung im Rahmen des § 110 Abs. 3, 4 StPO *Bäcker*, in: MüKo-StPO, § 110 Rn. 36.

(2) **Unverhältnismäßigkeit im Einzelfall**

Die Eingriffe sind weder erforderlich noch angemessen. Wie bereits oben ausgeführt, ist die Verhältnismäßigkeitsprüfung bei einem so schwerwiegenden Eingriff besonders sorgsam durchzuführen. Vorliegend lässt weder der gerichtliche Beschluss noch die tatsächliche Durchführung der Beschlagnahme und Auswertung erkennen, ob überhaupt Verhältnismäßigkeitserwägungen vorgenommen wurden.

Dies wird unter folgenden Aspekten besonders deutlich:

(a) **Legitimer Zweck und Geeignetheit**

Wenn man fälschlicherweise davon ausgehen würde, dass ein Anfangsverdacht bezüglich einer Straftat nach § 201 Abs. 1 Nr. 2 StGB bestanden hätte, läge zwar ein legitimer Zweck vor. Auch könnten die Beschlagnahme, Durchsicht und Auswertung des Mobiltelefons in einem derartigen Fall unter Umständen geeignet sein, diesen Zweck zu erreichen. Jedenfalls aber war die Auswertung in dem hier vorliegenden Umfang nicht erforderlich.

(b) **Keine Erforderlichkeit hinsichtlich des Umfangs der Auswertung**

Weder durch die Ermittlungsbehörden noch durch das Amtsgericht wurde geprüft, ob ein weniger eingriffsintensives Mittel als die vollständige Einbehaltung und Auswertung des Geräts in Betracht gekommen wäre. Naheliegend wäre etwa die isolierte Spiegelung der konkret versendeten Sprachnachricht gewesen. Die konkrete Nachricht war bereits Gegenstand polizeilicher Beobachtung, ihre Existenz sowie ihr Versand standen nicht in Zweifel. Die vollständige Einbehaltung des Geräts für den gesamten Zeitraum des Ermittlungsverfahrens war zur Beweissicherung dieser einen Datei offensichtlich nicht erforderlich.

Die vollständige Auswertung des Mobiltelefons war erst recht nicht erforderlich. Den Ermittlungsbehörden war bekannt, wann die dem Tatvorwurf zu Grunde gelegte Sprachnachricht „abgesendet“ wurde. Es wäre also möglich gewesen, die Auswertung auf Sprachnachrichten mit einem bestimmten Zeitstempel zu beschränken. Vorliegend wurde aber weder durch das Amtsgericht in der Beschlagnahmeanordnung noch von den Ermittlungsbehörden in der konkreten Auswertung eine Beschränkung vorgenommen.

Der Beschluss hätte erkennen lassen müssen, dass sich die Durchsicht und Auswertung auf ein einziges Datenfragment – die Sprachnachricht – zu beschränken hatte. Er eröffnet hingegen den Zugriff auf sämtliche Daten, einschließlich historischer Kommunikation, Metadaten, Bilder, Standortverläufe und Zugangsinformationen. Das war ersichtlich überschießend und sachlich unbegründet. Für die Ermittlung, ob und wann die fragliche Sprachdatei aufgenommen und/oder

versendet wurde, ist zwingend die zeitliche Einschränkung auf den bekannten Tatzeitraum notwendig. Darüber hinaus wäre zumindest eine Beschränkung auf die Art der durchzusehenden Daten, nämlich Sprachnachrichten, vorzunehmen gewesen.

Weder der richterliche Beschluss noch die tatsächliche Auswertung enthielten eine inhaltliche, zeitliche oder technische Begrenzung hinsichtlich der auszuwertenden Daten.

(c) **Keine Verhältnismäßigkeit im engeren Sinne**

Die Auswertung war zudem nicht verhältnismäßig im engeren Sinne. Der Zweck stand vorliegend außer Verhältnis zur Schwere des Eingriffs.

(aa) Eingriff mit hoher Intensität

Im vorliegenden Fall haben sich die mit einem umfassenden Zugriff auf den gesamten Datenbestand eines modernen Smartphones einhergehenden Gefahren für die Persönlichkeitsrechte realisiert (zu den Gefahren im Allgemeinen und der hohen Eingriffsintensität siehe oben 1.c.aa.). Im konkreten Fall haben die Strafverfolgungsbehörden besonders schützenswerte Informationen über die politischen Anschauungen und Aktivitäten des Betroffenen weitreichend ausgewertet und inklusive einer Vielzahl an privaten Fotos und Textnachrichten gespeichert. Dies begründet vorliegend einen besonders tiefgreifenden Eingriff. Auch der Eigentumsentzug weist eine hohe Intensität auf, da der Beschwerdeführer während der Beschlagnahme den kompletten Zugriff auf sein Mobiltelefon verlor.

(bb) Unangemessene Dauer und Tiefe der Maßnahme

Die Maßnahme zog sich seit Monaten hin, ohne dass eine begrenzte oder abgeschlossene Auswertung kommuniziert worden wäre. Die vollständige und andauernde Entziehung eines zentralen Kommunikations- und Arbeitsmittels über ein Jahr lang ist besonders eingriffsintensiv. Smartphones sind Ausdruck individueller Lebensführung und Träger sensibelster Informationen. Der dauerhafte Zugriff darauf bedarf strikter zeitlicher Kontrolle, die hier fehlt.

Smartphones haben zahlreiche Funktionen, die sich in jeden Lebensbereich erstrecken und auf die die meisten Menschen angewiesen sind. So bezahlen inzwischen eine Vielzahl von Menschen per Smartphone, statt Kreditkarten oder Bargeld zu nutzen. Reisen werden damit gebucht, Terminkalender erstellt, Arzttermine gebucht usw. Ein dauerhafter Entzug stellt eine erhebliche Einschränkung dar.

(cc) Ausufernde Datenauswertung

Die konkrete Auswertung durch die Ermittlungsbehörden gingen weit über den Tatvorwurf hinaus. Lediglich zunächst stand bei der Auswertung der konkrete Tatvorwurf im Fokus. Allerdings wurden dann auch weitere Daten, zu denen Bilddateien, Chats, Text- und Sprachnachrichten, Mitgliedschaften in Chatgruppen und Newslettern gehörten, ausgewertet (siehe oben unter A.). Ziel und Ergebnis dieser weiteren Auswertung war die Erstellung eines umfassenden politischen Profils des Beschwerdeführers. Die Erstellung eines politischen Profils war für die Aufklärung des Tatvorwurfs nicht notwendig, sondern überschreitet evident die Grenzen der Verhältnismäßigkeit.

(dd) Geringfügigkeit des Tatvorwurfs

Diesen schwerwiegenden Grundrechteingriffen steht ein im Vergleich wenig gewichtiger Anlass entgegen. Die vermeintliche Verletzung der Vertraulichkeit des Wortes ist ein einfaches Vergehen mit niedriger Strafdrohung. Der Tatvorwurf wiegt gering. Dass für einen derart geringfügigen Vorwurf ein solch umfassender Grundrechtseingriff in Kauf genommen wird, ist evident unverhältnismäßig.

4. Verletzung des Rechts auf effektive Verteidigung und faires Verfahren nach Art. 6 EMRK und Art. 103 Abs. 1 GG

Der Beschwerdeführer und sein Verteidiger hatten zudem zu keinem Zeitpunkt die Möglichkeit, die Auswertung zu kontrollieren, deren Umfang zu erfahren oder eigene Auswertungsrechte geltend zu machen. Es fehlt an Transparenz, Protokollierung und Kontrollierbarkeit. Die Akteneinsicht ist in dieser Hinsicht unzureichend, da nur Ausschnitte der Auswertung Aktenbestandteil geworden sind. Das Gleichgewicht der Verfahrensbeteiligten ist dadurch in gravierender Weise gestört. Der Beschwerdeführer wird der Möglichkeit beraubt, sich effektiv gegen die Maßnahme zur Wehr zu setzen. Dies verletzt das Recht des Beschwerdeführers auf effektive Verteidigung und faires Verfahren, Art. 6 EMRK, Art. 103 Abs. 1 GG,

vgl. EGMR, Urt. v. 18.3.1997, Fitt v. United Kingdom, Nr. 29777/96.

5. Verletzung von Art. 8 EMRK

Nicht zuletzt werden die Grundsätze der EMRK verletzt. Art. 8 EMRK schützt das Recht auf Privatleben auch gegenüber staatlichen Ermittlungsmaßnahmen. Eingriffe in digitale Kommunikation und personenbezogene Daten bedürfen daher einer klaren gesetzlichen Grundlage, einer konkreten Zweckbindung, effektiver rechtsstaatlicher Kontrollen und der Wahrung des Prinzips der Erforderlichkeit,

EGMR, Urt. v. 4.12.2015, Roman Zakharov v. Russia, Nr. 47143/06.

Diese Voraussetzungen sind im vorliegenden Fall nicht erfüllt (siehe oben unter 1.c.bb. und 2.b.).

Pinar
Rechtsanwältin