Smarte Überführung?

Zum zwangsweisen Zugriff der Strafverfolgungsbehörden auf gesperrte Mobiltelefone

Von Prof. Dr. **Ken Eckstein**, Bochum*

Mit Beschluss vom 13.3.2025[1] *hat der Bundesgerichtshof (BGH) es für zulässig erklärt, dass die Strafverfolgungsbehörden zwangsweise einen Finger des Beschuldigten auf den Fingerabdrucksensor seines Mobiltelefons auflegen, um Zugang zu den Daten zu erhalten, die auf dem Mobiltelefon gespeichert sind. Diese Maßnahme soll auf § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO gestützt werden dürfen, wenn eine nach §§ 102, 105 Abs. 1 StPO richterlich angeordnete Durchsuchung dem Auffinden von Mobiltelefonen diente und der Datenzugriff verhältnismäßig ist (amtlicher Leitsatz).*

Bestärkt und herausgefordert fühlen konnte der BGH sich durch ein Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 4.10.2024[2] *– herausgefordert, weil der EuGH den Geltungsanspruch der europäischen Datenschutzordnung und der Grundrechtecharta der EU für den Zugriff der nationalen Strafverfolgungsbehörden auf Mobiltelefone ausformuliert,*[3] *und in der Sache bestärkt, weil der EuGH eine richterliche Anordnungskompetenz, die strikte Verhältnismäßigkeitsprüfung im Einzelfall und die Information des Betroffenen zur Ermöglichung nachträglichen Rechtsschutzes als Eingriffsvoraussetzungen genügen zu lassen scheint.*

Der BGH hat in der Folge ein kunstvolles Bauwerk aus drei Befugnisnormen errichtet, die in ihrer Zusammenschau eine Ermächtigung unter Richtervorbehalt ergeben: § 81b StPO i.V.m. §§ 94 ff. und 102 ff. StPO – smarte Überführung oder Flickschusterei?

I. Problemaufriss

Über die Zulässigkeit einer Entsperrung und Auswertung von Mobiltelefonen (oder ähnlichen Geräten wie Tablets und Notebooks) wird seit einiger Zeit kontrovers diskutiert.[4] Die Strafverfolgungsbehörden haben großes Interesse an einem Zugriff, weil Mobiltelefone eine Fundgrube für ermittlungsrelevante Informationen sind. Auf eine Gelegenheit zu warten, das schon entsperrte Mobiltelefon zu beschlagnahmen, dürfte wenig praktikabel sein. Vermutlich hilft den Strafverfolgungsbehörden nicht selten die Kooperationsbereitschaft Betroffener. In der Annahme, Widerstand sei zwecklos, oder auf den Hinweis hin, nur so könne eine langfristige Beschlagnahme zwecks Brute-force-Entschlüsselung vermieden werden, womöglich ergänzt um den fürsorglichen Fingerzeig, eine solche Entschlüsselung berge das Risiko einer Beschädigung,[5] werden nicht wenige Betroffene der Aufforderung nachkommen, das Mobiltelefon zu entsperren.[6] Der BGH erlaubt den Strafverfolgungsbehörden eine zwangsweise Entsperrung via Fingerabdrucksensor und bestätigt so, dass in der Praxis, jedenfalls für den Beschuldigten, denn nur auf ihn bezieht sich die Entscheidung, ein Finderabdrucksensor keinen effektiven Zugriffsschutz bietet.

In der zwangsweisen Entsperrung sieht der BGH keinen Verstoß gegen den Nemo-tenetur-Grundsatz (unten IV.).[7] Der BGH erkennt aber an, dass es sich beim nicht konsentierten Zugriff auf die Daten eines Mobiltelefons um einen „schwerwiegenden oder sogar besonders schwerwiegenden Eingriff"[8] in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) sowie in das Recht auf Achtung des Privat- und Familienlebens (Art. 7 Charta der Grundrechte der Europäischen Union [GrCh])[9] und das Recht auf Schutz personenbezogener Daten (Art. 8 GrCh) handle.[10] Auch sei der Anwendungsbereich der JI-Richtlinie (EU) 2016/680[11] eröffnet.[12] Das besondere Gewicht des Grundrechtseingriffs erkennt der BGH zutreffend darin, dass beim Zugriff auf ein Mobiltelefon eine Vielzahl an Daten auch vertraulicher oder gar höchstpersönlicher Natur zugänglich werden (Kommunikation, Lichtbilder, Videoaufnahmen, Notizen oder Kalendereinträge).[13] Über die §§ 81b, 94 ff., 102 ff. StPO hinausgehende Eingriffsvoraussetzungen leitet der BGH daraus jedoch nicht ab. Das erscheint fragwürdig (unten V.).

Näherer Untersuchung bedarf außerdem der methodische Umgang des BGH mit den Befugnisnormen der Strafprozessordnung. Nach Ansicht des BGH findet sich eine gesetzliche Eingriffsgrundlage für die Entsperrung von Mobiltelefonen des Beschuldigten in § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO.[14] Daran überrascht die Kumulation von Befugnisnormen. Sie führt zu der Frage, wie weit § 81b StPO legitimerweise reicht und ob nicht §§ 94 ff. StPO schon für sich

---

* Der *Verf.* ist Professor für Strafrecht und Strafprozessrecht an der Ruhr-Universität Bochum.

[1] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24 = NJW 2025, 2265 = NStZ 2025, 560 – vorgesehen für BGHSt.

[2] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321.

[3] Die von mir vorgeschlagene Restriktion des Anwendungsbereichs der Grundrechtecharta (*Eckstein*, ZIS 2013, 220 [224] m.w.N.) hat sich nicht durchgesetzt.

[4] Für Nachweise zum Streitstand siehe Fn. 53 ff. und 94 ff.

[5] *Rottmeier/Eckel*, NStZ 2020, 193 [194].

[6] Zu den Grenzen von Einwilligung und Freiwilligkeit i.S.v. § 51 BDSG *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 577 ff. m.w.N.

[7] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 32.

[8] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28, 33. Wortgleich EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325).

[9] ABl. EU 2016 Nr. C 202, S. 389 ff.

[10] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28, 33.

[11] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU 2016 Nr. L 119, S. 89 ff.).

[12] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28 f.

[13] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 33.

[14] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28.

genommen eine Annexkompetenz zu vorbereitenden Eingriffen implizieren. Der Rückgriff auf § 81b StPO wirft außerdem die Frage auf, ob und wie auf Mobiltelefone Nichtbeschuldigter zugegriffen werden darf, für die § 81b StPO seinem klaren Wortlaut nach nicht gilt (unten VI.).

Der BGH reichert seine Kumulation der Befugnisnormen sogar noch weiter an, indem er einschränkend hinzufügt, dass die Entsperrung jedenfalls dann von § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO gedeckt sei, wenn eine nach §§ 102, 105 Abs. 1 StPO richterlich angeordnete Durchsuchung dem Auffinden von Mobiltelefonen diente und der Datenzugriff verhältnismäßig ist.[15] Mit § 102 StPO kommt also eine dritte Befugnisnorm ins Spiel. Wohlgemerkt bezieht der BGH alle drei Befugnisnormen auf den „Versuch der Ermittlungsbehörden", durch Entsperrung „Zugang zu den auf einem Mobiltelefon […] gespeicherten Daten zu erlangen".[16] Zwar wechselt der BGH zwischendurch zu einer stärker analytischen Betrachtung der Abfolge von Eingriffen, wie sie insbesondere von *Rottmeier/Eckel* befürwortet wird:[17] Durchsuchung (§ 102 StPO) – Sicherstellung der Mobiltelefone – Entsperrung der Mobiltelefone (§ 81b Abs. 1 StPO) – Durchsicht der Daten (§ 110 StPO) – Beschlagnahme der verfahrensrelevanten Daten (§ 94 Abs. 2 StPO).[18] Der BGH hält diese analytische Betrachtung aber nicht durch, weil erst die Kumulation der Befugnisnormen ein Set an Eingriffsvoraussetzungen ergibt, wie der EuGH es in seinem Urteil vom 4.10.2024 zur Bedingung gemacht hat[19] (unten VI.).

Man wird die Entscheidung des BGH auf andere biometrische Sicherungen übertragen dürfen (Festhalten für die Gesichts- oder Iriserkennung). Dagegen bleibt das Erzwingen der PIN-Eingabe oder einer Stimm- oder Schrittprobe durch den Beschuldigten zwecks Entsperrung unzulässig (unten IV.). Auch ergibt sich aus der Entscheidung keine Befugnis für die verdeckte Benutzung des Mobiltelefons.[20] Im Übrigen wird vom BGH für das Problem des Zugriffs auf gesicherte Datenträger allenfalls eine punktuelle Lösung vorgeschlagen. Die Anforderungen, die BGH und EuGH aufstellen, verdeutlichen jedoch die weiterreichende Virulenz des Problems. Darf auch der Finger eines Toten oder eines anderen Nichtbeschuldigten aufgelegt werden, um ein Mobiltelefon zu entsperren?[21] Unter welchen Voraussetzungen darf eine Entsperrung mit technischen Mitteln (brute force) erfolgen?[22] Dürfen freiwillig zur Identitätsfeststellung abgegebene Fingerabdrücke nachträglich umgewidmet werden, um eine Fingerabdruck-Attrappe zu erstellen, mit der ein Mobiltelefon entsperrt wird (unten V., VI.)?[23] Die Regelungsbedürfnisse unterstreichen die Notwendigkeit einer gesetzlichen Neuregelung (unten V., VI.).

Bevor der Beitrag diesen Fragen im Einzelnen nachgeht, folgt im Anschluss ein Blick auf den Sachverhalt (unten II.) und auf eine Sonderfrage, die sich dem BGH in der vorliegenden Entscheidung stellte (unten III.).

II. Sachverhalt[24]

Zu entscheiden hatte der BGH über die Revision des Beschuldigten gegen eine Verurteilung wegen Herstellung und Besitz kinderpornographischer Inhalte (§ 184b StGB) sowie wegen Verstoßes gegen ein Berufsverbot (§ 145c StGB). Das Berufsverbot war in einem früheren Verfahren wegen Herstellung und Besitz kinderpornographischer Inhalte gegen den Beschuldigten verhängt worden und untersagte ihm lebenslang, als Sozialarbeiter, Sozialpädagoge, Erzieher, Pfleger und Betreuer von Kindern und Jugendlichen tätig zu werden.

Im März 2021 ordnete der Ermittlungsrichter auf Antrag der Staatsanwaltschaft wegen des Verdachts eines Verstoßes gegen das Berufsverbot (§ 145c StGB) die Durchsuchung der Wohnräume des Beschuldigten und seiner Person an. Aufgefunden werden sollten unter anderem Mobiltelefone, um die Anbahnung von Kinder-Betreuungsverhältnissen zu belegen. Am folgenden Tag wurde die Durchsuchung durchgeführt. Die Polizei fand zwei Mobiltelefone. Der Beschuldigte weigerte sich, diese freiwillig zu entsperren. Daraufhin ordnete ein Polizeibeamter an, unmittelbaren Zwang anzuwenden und auf diese Weise den rechten Zeigefinger des Beschuldigten auf die Fingerabdrucksensoren der Mobiltelefone aufzulegen. So wurden die Mobiltelefone entsperrt und anschließend einer Datensicherung unterzogen. Später wurde der Verteidiger des Beschuldigten angerufen. Dieser machte das Schweigerecht des Beschuldigten geltend und widersprach jeglicher Maßnahme.

Auf den Mobiltelefonen wurde kinderpornographisches Material gefunden.[25] Am ersten Hauptverhandlungstag widersprach der Verteidiger der Einführung dieses Materials in die Hauptverhandlung und der Verwertung als Beweismittel, weil eine Befugnisnorm für die zwangsweise Entsperrung von Mobiltelefonen fehle und die Selbstbelastungsfreiheit, der Fair-trial-Grundsatz und das Recht auf informationelle Selbst-

[15] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28.
[16] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28.
[17] *Rottmeier/Eckel*, NStZ 2020, 193 (194 ff.).
[18] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 42 ff.
[19] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321.
[20] Für § 110a StPO *Rottmeier/Eckel*, NStZ 2020, 193 (198). Richtigerweise bedarf es für die Verwendung der Identität des Betroffenen und die qualifizierte Täuschung einer speziellen Befugnisnorm, vgl. § 163g StPO-Entwurf in der Fassung durch Art. 5 Nr. 4 Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 27.3.2019, abrufbar unter http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf (28.9.2025).
[21] Vgl. *Sehl*, LTO v. 23.4.2018, abrufbar unter https://www.lto.de/persistent/a_id/28131 (28.9.2025).
[22] Zu den Möglichkeiten *Bäumerich*, NJW 2017, 2718 (2718 f.); *F. Horn*, Kriminalistik 2019, 641; *Rottmeier/Eckel*, NStZ 2020, 193 (194).
[23] Dazu *Rottmeier/Eckel*, NStZ 2020, 193 (200).
[24] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 1 ff.
[25] Der *Senat* befasst sich in diesem Zusammenhang auch mit der Abgrenzung von nicht kinderpornographischen Darstellungen sowie mit dem Begriff der prozessualen Tat bei Besitzdelikten und der Reichweite des Strafklageverbrauchs (BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 9 ff.).

bestimmung verletzt seien. Auf die Anordnung des Vorsitzenden hin, das Material in Augenschein zu nehmen, wurde eine Entscheidung der Strafkammer herbeigeführt, die diese Anordnung bestätigte (§ 238 StPO). Das Material wurde in Augenschein genommen und der Verurteilung zugrunde gelegt.

Die Revision des Beschuldigten stützt sich auf eine Verletzung des § 261 StPO durch Missachtung eines Beweisverwertungsverbots. Angeführt werden wiederum das Fehlen einer Befugnisnorm für die zwangsweise Entsperrung von Mobiltelefonen und ein Verstoß gegen die Selbstbelastungsfreiheit und den Fair-trial-Grundsatz. Außerdem – das macht die Verteidigung offenbar erstmals mit der Revision geltend – fehle ein richterlicher Beschlagnahmebeschluss.

III. Der fehlende Beschlagnahmebeschluss

Dass kein richterlicher Beschlagnahmebeschluss nach § 94 Abs. 2 StPO i.V.m. § 98 Abs. 2 S. 1 StPO erging, obwohl der Beschuldigte der Beschlagnahme widersprochen hatte, führt nach den in der Rechtsprechung geläufigen Voraussetzungen für ein Beweisverwertungsverbot für sich genommen nicht zur Unverwertbarkeit. Der BGH fasst sich insofern kurz.[26] Die zugrundeliegenden Maßstäbe sind freilich komplex (Abwägungslehre; absolute Grenze bei vorsätzlicher oder willkürlicher Rechtsverletzung; kein Verwertungsverbot, wenn ein Widerspruch in der Hauptverhandlung erforderlich gewesen wäre und nicht erfolgte).[27]

Die Rüge, es sei kein Beschlagnahmebeschluss ergangen, bezieht der BGH nicht auf die Mobiltelefone selbst, sondern auf die spätere Beschlagnahme von auf den Telefonen gespeicherten Daten.[28] Das Verfahren gestaltet sich insofern wie folgt: Die Durchsicht von Speichermedien gestattet § 110 Abs. 3 i.V.m. Abs. 1 StPO als Teil der Durchsuchung. Die vorläufige Datensicherung zur späteren Durchsicht unterliegt nach § 110 Abs. 4 StPO dem Verfahren des § 98 Abs. 2 StPO. Bei einem zeitlich gestreckten Vorgehen können also neben den Telefonen selbst sowohl die vorläufige Sicherung des gesamten Datenträgers als auch eine spätere Beschlagnahme einzelner Datensätze Bezugspunkt des § 98 StPO sein.

Entscheidend stellt der BGH darauf ab, dass die Verteidigung das Fehlen eines Beschlagnahmebeschlusses nicht schon in der Hauptverhandlung geltend gemacht hatte.[29] Das Gericht bringt also die Widerspruchslösung zur Anwendung, der zufolge bestimmte Verfahrensfehler nur dann die Revision begründen können, wenn die Verteidigung dem Verfahrensgang in der Hauptverhandlung rechtzeitig widersprochen hat, einer Beweisverwertung also im Zeitpunkt der Erklärung nach § 257 StPO bzw. gem. § 238 Abs. 2 StPO entgegengetreten ist.[30] Dass der BGH auch einzelne Bestandteile der Begründung für die Unverwertbarkeit dem Mechanismus der Rügepräklusion unterwirft, macht dieses Instrument besonders schneidig. Freilich erscheint das konsequent, wenn der Zweck des Widerspruchserfordernisses darin liegt, das Gericht vor Fehlern zu bewahren, die noch verhindert werden könnten. Dass die Widerspruchslösung zu Unrecht der Verteidigung die Verantwortung für die Rechtmäßigkeit des Verfahrens überbürdet, wurde von kritischen Literaturstimmen ausführlich begründet.[31]

Der BGH stellt fest, dass die Voraussetzungen für einen Beschlagnahmebeschluss noch in der Hauptverhandlung vorgelegen hätten (§ 98 Abs. 2 S. 3 StPO i.V.m. § 162 Abs. 3 S. 1 StPO).[32] Mit einer solchen Heilungsmöglichkeit rekurriert das Gericht auf die Hypothese rechtmäßiger Beweisgewinnung. Überdies sei das Fehlen eines Beschlagnahmebeschlusses nach § 98 StPO für sich genommen kein hinreichend gravierender Verfahrensfehler.[33] Aufhorchen lässt die einschränkende Formulierung, dass das jedenfalls und regelmäßig dann gelte, wenn „die Sichtung der Daten auf einem Mobiltelefon von § 110 StPO gedeckt war".[34] Diese Begründung verweist auf die Kumulation der Befugnisnormen, durch die der BGH sich eine Verschleifung von Eingriffsvoraussetzungen ermöglicht: Der fehlende Beschlagnahmebeschluss wird durch den richterlichen Durchsuchungsbeschluss ersetzt. Deutlich wird schon an dieser Stelle, dass die fluide Konstruktion des BGH dem Richtervorbehalt nicht gerecht wird, den der EuGH für die Entsperrung eines Mobiltelefons statuiert.

IV. Selbstbelastungsfreiheit und Fair-trial-Grundsatz

Der Nemo-tenetur-Grundsatz verbietet es den Strafverfolgungsbehörden, Zwang anzuwenden, der bewirkt, dass der Betroffene sich aktiv selbst belastet.[35] Eine Beschränkung auf den Kernbereich der Aussagefreiheit findet in Deutschland überwiegend nicht statt.[36] Inwieweit generell die Eigen-

[26] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25.

[27] Vgl. dazu BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 60 f.; BGH, Urt. v. 18.4.2007 – 5 StR 546/06 = NJW 2007, 2269 (2271 ff.).

[28] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25.

[29] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25.

[30] BGH, Beschl. v. 21.11.2024 – 4 StR 270/24 = NStZ 2025, 179; BGH, Beschl. v. 27.2.1992 – 5 StR 190/91 = NJW 1992, 1463 (1466); für die Durchsuchung BGH, Urt. v. 9.5.2018 – 5 StR 17/18 = NJW 2018, 2279 (2279 f.); kritisch BGH, Urt. v. 6.10.2016 – 2 StR 46/15 = NStZ 2017, 367 (368 f.).

[31] *Eschelbach*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, StPO, Stand: 1.7.2025, § 257 Rn. 30 ff. m.w.N.

[32] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25.

[33] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25 unter Berufung auf *Menges*, in: Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3/1, 27. Aufl. 2019, StPO § 98 Rn. 77.

[34] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 25.

[35] BVerfG, Beschl. v. 13.1.1981 – 1 BvR 116/77 = BVerfGE 56, 37 (42 f.); BVerfG, Urt. v. 19.3.2013 – 2 BvR 2628/10, 2 BvR 2883/10, 2 BvR 2155/11 = NJW 2013, 1058 (1061). Zu den Rechtsgrundlagen *Eckstein*, Ermittlungen zu Lasten Dritter, 2013, S. 54 f. m.w.N. zum Streitstand.

[36] A.A. *Bosch*, in: Satzger/Schluckebier/Werner (Hrsg.), StPO, Kommentar, 6. Aufl. 2025, § 81b Rn. 8. Zu anderen Rechtsordnungen *F. Horn*, Kriminalistik 2019, 641 (644) m.w.N. Für eine Beschränkung auf Mitwirkungshandlungen, die einen unmittelbaren Bezug zur Persönlichkeit des Beschuldigten haben, *Schrott*, NSW 2024, 286 (290) m.w.N.

verantwortlichkeit der Entscheidung, sich selbst zu belasten, garantiert wird[37] und inwieweit schon das passive Dulden von Zwang mit selbstbelastender Wirkung die Selbstbelastungsfreiheit verletzt,[38] ist umstritten. Der BGH folgt der engeren Lesart, die das passive Dulden von Zwang nicht der Selbstbelastungsfreiheit zuordnet, auch wenn der Körper des Beschuldigten dadurch zum Mittel der Überführung werden kann.[39]

Das erscheint mir überzeugend. Denn die Reichweite des Nemo-tenetur-Grundsatzes sollte schon aus systematischen Gründen einschränkend so ausgestaltet werden, dass die eigenständige Bedeutung der Selbstbelastungsfreiheit als absolute, abwägungsfeste Gewährleistung gewahrt bleibt. Ergänzenden relativen Schutz vor sonstigen Zugriffen der Strafverfolgungsbehörden auf Tatwissen und überführungsrelevante Informationen (Irrtum, Täuschung, Unwissenheit, erzwungenes Dulden) leisten andere Rechtsgarantien, die gesetzliche Eingriffe zulassen und begrenzen.

Nicht übersehen werden darf dabei, dass diese Sichtweise in einem Spannungsverhältnis zu europarechtlichen Tendenzen steht, den Nemo-tenetur-Grundsatz am Fair-trial-Prinzip (Art. 6 EMRK) auszurichten[40] und dadurch zu erweitern und zu relativieren. So unterscheidet der Europäische Gerichtshof für Menschenrechte (EGMR) bei Beweismitteln, die unabhängig vom Willen des Beschuldigten vorhanden sind (Schriftstücke, Körperproben etc.), nach der Zielrichtung erzwungenen Duldens (Beweiserlangung), nach dem Grad des Zwanges und nach der ausgelösten Körperreaktion (Ausnutzen normaler Körperfunktionen versus Auslösen einer pathologischen Reaktion)[41] – und nimmt je nach den Umständen des Einzelfalls einen Verstoß gegen den Nemo-tenetur-Grundsatz an.

Die Verselbständigung des Nemo-tenetur-Grundsatzes als absolute, abwägungsfeste Gewährleistung erscheint mir dennoch vorzugswürdig. Sie bedeutet inhaltlich eine Rückbindung an den unantastbaren Menschenwürdegehalt des Nemo-tenetur-Grundsatzes. Absolut geschützt ist der Betroffene davor, durch Zwang (oder zwangsgleiche Einwirkung) in einen Entscheidungskonflikt gebracht zu werden, in dem er vor der Wahl steht, entweder aktiv an der eigenen Überführung mitzuwirken oder aufgezwungene Nachteile in Kauf zu nehmen.[42] Der Fair-trial-Grundsatz behält daneben seine Auffangfunktion und gewährleistet relativen Schutz nach Maßgabe einer Overall-fairness-Prüfung.[43]

So verstanden, ist der Nemo-tenetur-Grundsatz im Ausgangsfall nicht betroffen. Auch ein Verstoß gegen den Fair-trial-Grundsatz liegt fern, falls eine Rechtsgrundlage für das Vorgehen der Strafverfolgungsbehörden besteht. Ebenso wenig verbietet der Nemo-tenetur-Grundsatz das Festhalten für die Gesichts- oder Iris-Erkennung[44] oder das Auflegen des Fingers eines Toten auf den Fingerabdrucksensor eines Mobiltelefons. Dasselbe gilt letztlich für die zweckändernde Benutzung bereits vorliegender Fingerabdrücke, auch wenn der Betroffene bei der Aufnahme – ohne Zwang (oder zwangsgleiche Einwirkung) – aktiv mitgewirkt hat. Denn der Nemo-tenetur-Grundsatz verbietet nicht schlechthin die aktive Mitwirkung und ein Entscheidungskonflikt kann nicht rückwirkend entstehen.[45] Unzulässig wäre dagegen die Anwendung von Zwang, damit der Betroffene aktiv einen bestimmten Gesichtsausdruck annimmt, selbst eine PIN eingibt, selbst den Finger auflegt oder eine Stimm- oder Schrittprobe abgibt.[46] Dass alle diese Sachverhaltskonstellationen sich zu ähneln scheinen, ändert nichts an ihrer rechtlichen Verschiedenheit mit Blick auf den Entscheidungskonflikt, vor dem der Nemo-tenetur-Grundsatz schützt.

V. Grundrechte und Verhältnismäßigkeit

Der Zugriff auf ein Mobiltelefon greift für sich genommen nicht in Art. 10 GG ein, weil nicht die Vertraulichkeit im Herrschaftsbereich des Netzbetreibers in Rede steht.[47] Betrof-

[37] Dafür z.B. *Neuhaus*, StV 2020, 489 (491); *Roxin*, NStZ 1997, 18 (18 ff.); *Schrott*, NSW 2024, 286 (288). Näher zu dieser Streitfrage *Eckstein* (Fn. 35), S. 55 ff. m.w.N.

[38] Unter dem Gesichtspunkt der Umgehung *Hecken/Ziegler*, jurisPR-ITR 10/2023 Anm. 5; ähnlich *Nicolai*, StV Spezial 2023, 148. Grundlegend gegen die Unterscheidung nach Aktivität und Passivität *Bosch*, Aspekte des nemo-tenetur-Prinzips aus verfassungsrechtlicher und strafprozessualer Sicht, 1998, S. 277 ff.; weiter differenzierend *Satzger/Sarfraz*, NStZ 2025, 566 (vorausliegende bewusste Willensentscheidung zur Verschlüsselung).

[39] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 32. Ebenso *Bock/Fülscher*, StraFo 2023, 386 (390); *Nadeborn/Irscheid*, StraFo 2019, 274 (275); *Neuhaus*, StV 2020, 489 (491); *Rottmeier/Eckel*, NStZ 2020, 193 (199).

[40] Zum Verhältnis zwischen Fair-Trial- und Nemo-tenetur-Grundsatz *Jung*, GA 2013, 90 (93 f., 97: Nemo-tenetur-Grundsatz als Unterfall des Fair-Trial-Grundsatzes).

[41] EGMR (Große Kammer), Urt. v. 11.7.2006 – 54810/00 (Jalloh ./. Deutschland) = NJW 2006, 3117 (3123 f.) – Verabreichung von Brechmitteln.

[42] Näher dazu *Eckstein* (Fn. 35), S. 59 m.w.N.

[43] Näher dazu *Eckstein*, in: Schroeder/Kudratov (Hrsg.), Die strafprozessuale Hauptverhandlung zwischen inquisitorischem und adversatorischem Modell, 2014, S. 219 (222 f.) m.w.N.

[44] Zu § 136a StPO und Art. 3 EMRK als Grenzen *Wegner*, in: Beulke/Jahn/Schmitt-Leonardy/Bertheau/Müller-Jacobsen (Hrsg.), Strafrecht und Strafverteidigung in Geschichte, Praxis und Politik, Festschrift für Alexander Ignor zum 70. Geburtstag, 2023, S. 853 (861); vgl. auch *Schrott*, NSW 2024, 286 (289).

[45] Zu den Voraussetzungen zweckändernder Datenverwendung *Rückert* (Fn. 6), S. 525 ff.

[46] *Bäumerich*, NJW 2017, 2718 (2720): § 136a StPO. Anschaulich *Kudlich*, JA 2025, 697: zulässige vis absoluta versus unzulässige vis compulsiva. Zu § 163g StPO-Entwurf (Fn. 20: Pflicht, Zugangsdaten herauszugeben, kompensiert durch ein Verwertungsverbot) *Nadeborn/Irscheid*, StraFo 2019, 274 (275 ff.).

[47] *El-Ghazi*, in: Verhandlungen des 74. Deutschen Juristentages Stuttgart 2024, Band I, 2024, C 47 f. m.w.N.: Auch nicht, wenn während der Sicherstellung weitere Nachrichten auf dem Telefon eingehen, anders bei der Online-Durchsicht

fen sind jedoch, gegebenenfalls neben Art. 14 GG,[48] das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) und von Fall zu Fall besondere Datenschutz-Garantien (Art. 4, 5, 6, 12 GG),[49] bei unmittelbarem Zwang zur Durchsetzung der Entsperrung die allgemeine Handlungsfreiheit und gegebenenfalls das Recht auf körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG)[50] sowie das Recht auf Achtung des Privat- und Familienlebens (Art. 7 GrCh) und das Recht auf Schutz personenbezogener Daten (Art. 8 GrCh).[51] Dem Recht auf informationelle Selbstbestimmung geht allerdings das IT-System-Grundrecht (auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) als lex specialis vor. Auch der offene Zugriff auf eigengenutzte IT-Systeme greift in das IT-System-Grundrecht ein. Nur für Daten Dritter bleibt es beim Schutz durch das Recht auf informationelle Selbstbestimmung.[52] Art und Menge der Daten auf einem Mobiltelefon begründen das besondere Gewicht des Eingriffs. Dass ein Eingriff in das IT-System-Grundrecht stattfindet, hat der BGH übersehen.

Der besonderen Eingriffstiefe wegen werden zu Recht von vielen Stimmen für den Beschlagnahmezugriff insbesondere auf Mobiltelefone gegenüber §§ 94 ff. StPO erhöhte Eingriffsvoraussetzungen und besondere Schutzvorschriften gefordert, teilweise in Anlehnung an die Regelungen für heimliche Maßnahmen in den §§ 100a, 100b StPO.[53] Teilweise werden technische Mittel zur Entsperrung sowie die Erstellung und Auswertung von Datenkopien schon heute nur nach § 100b StPO für zulässig erachtet.[54] In der Praxis dagegen wird im Kern auf §§ 94 ff., 110 Abs. 3 StPO zurückgegriffen.[55] Dass ergänzende Verfahrensregeln erforderlich werden könnten, neben den Auskunfts- und Löschungspflichten gem. §§ 483 ff., 489, 491 StPO beispielsweise ein Anwesenheitsrecht, hat das Bundesverfassungsgericht (BVerfG) 2005 angemerkt.[56] Seitdem sind die Vorgaben in § 500 StPO i.V.m. §§ 45 ff. BDSG hinzugekommen.[57] Einen detaillierten Vorschlag zu Beschlagnahme und Auswertung de lege ferenda hat *El-Ghazi* in seinem Gutachten für den 74. Deutschen Juristentag 2024 vorgelegt: Anlasstatenschwelle (Mindesthöchststrafe von mehr als drei Jahren Freiheitsstrafe oder IT-Gerät Tatmittel), durch ein Tatsachenerfordernis qualifizierte Erfolgsaussicht, Regelung zum Schutz des Kernbereichs privater Lebensgestaltung, Möglichkeit der Vollzugshemmung bei gerichtlicher Überprüfung, Durchführungsvorschriften (wenn möglich Datensicherung statt Gerätebeschlagnahme, sonst Rückgabefrist mit Verlängerungsmöglichkeiten und unverzügliche Überlassung einer Datenkopie, Regelungen zum Schutz von Integrität und Authentizität, Dokumentation).[58]

Der BGH führt zum Gewicht des Eingriffs einerseits aus, dass es sich um eine offene Maßnahme handle, so dass der Betroffene jederzeit Rechtsschutz erlangen könne.[59] Andererseits erkennt der BGH an, dass angesichts der Vielzahl an Daten auch vertraulicher oder höchstpersönlicher Natur (Kommunikation, Lichtbilder, Videoaufnahmen, Notizen oder Kalendereinträge), die beim Zugriff auf ein Mobiltelefon zugänglich werden, ein gravierender Eingriff in Rede steht.[60] Der BGH sieht die Gefahr einer Ausforschung zahlreicher Aspekte der Persönlichkeit bis hin zur Ableitung von Verhaltens- und Kommunikationsprofilen.[61] Die generelle Unzulässigkeit der Maßnahme folgt daraus richtigerweise nicht.[62] Anderenfalls würde schon die nicht auszuschließende Möglichkeit des Auffindens kernbereichsrelevanter Informationen zur Ermittlungssperre. Das würde Wohnungsdurchsuchungen sehr weitgehend in Frage stellen. Das BVerfG erklärt nur die zielgerichtete Ausforschung des Kernbereichs privater Lebens-

nach § 110 Abs. 3 S. 2 StPO; *Neuhaus*, StV 2020, 489: z.B. E-Mail-Abruf vom Server des Providers.

[48] *Hiéramente*, StV 2024, 611 (612) – Entziehung des Geräts.

[49] Vgl. dazu *Eckstein*, in: Rotsch/Saliger/Tsambikakis (Hrsg.), Nomos Kommentar, StPO, Bd. 1, 2025, § 100a Rn. 37, 56 m.w.N.

[50] *Rottmeier/Eckel*, NStZ 2020, 193 (199).

[51] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28, 33.

[52] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I) = BeckRS 2025, 19412 Rn. 96 ff.; BVerfG, Beschl. v. 24.6. 2025 – 1 BvR 180/23 (Trojaner II) = BeckRS 2025, 19413 Rn. 173, 227 ff.; LG Ravensburg, Beschl. v. 14.2.2023 – 2 Qs 9/23 jug. = BeckRS 2023, 3879 Rn. 17; *El-Ghazi* (Fn. 47), C 56 ff.; *Horter*, NStZ 2023, 447 (448); *Jahn*, JuS 2025, 791 (792); *Neuhaus*, StV 2020, 489. A.A. mangels Heimlichkeit *Brodowski*, JZ 2024, 750 (752 f.); *F. Horn*, Kriminalistik 2019, 641 (642).

[53] *Cornelius*, NJW 2024, 2725 (2727 f.); *Greco*, StV 2024, 276 (280); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (122); *F. Horn*, Kriminalistik 2019, 641 (643 f.); *Momsen*, DRiZ 2018, 140 (142 f.); *Ruppert*, StV 2025, 565 (567); *Stam*, JZ 2023, 1070 (1076 f.); differenzierend (Beschlagnahmezugriff beim Telekommunikationsdienstleister oder anderweitig) *Eckstein* (Fn. 49), Vor §§ 100a–101 Rn. 28 und § 100a Rn. 23, 83; für das Auslesen einer SIM-Karte auch BVerfG, Beschl. v. 4.2.2005 – 2 BvR 308/04 = NStZ 2005, 337.

[54] *Cornelius*, NJW 2024, 2725 (2726 f.); *Greco*, StV 2024, 276 (280); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (120 ff.) – Zu den Grenzen des § 100b StPO unten VI.

[55] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 44 m.w.N.

[56] BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02 = NJW 2005, 1917 (1922). Näher dazu *Hiéramente*, StV 2024, 611 (613).

[57] Grundlegend dazu *Rückert* (Fn. 6), S. 515 ff.

[58] *El-Ghazi* (Fn. 47), C 79, 81, 86, 90, 94, 97 ff.; kritisch zur Beschränkung der Anlasstaten *Knauer/Schmorl*, AnwBl 2024, 252 (253), die ergänzend eine zeitliche Beschränkung der Durchsicht fordern (a.a.O. S. 254).

[59] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 33. Ebenso *Neuhaus*, StV 2020, 489 (489 f.).

[60] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 33. Anders z.B. *Rottmeier/Eckel*, NStZ 2020, 193 (200): geringfügiger Eingriff.

[61] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 33.

[62] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 34.

gestaltung für schlechthin ausgeschlossen.[63] Auch eine explizite Regelung zum Schutz des Kernbereichs verlangt der BGH nicht. Das überzeugt zwar nicht,[64] steht aber ebenfalls in Einklang mit der Rechtsprechung des BVerfG, die eine Regelung zum Schutz des Kernbereichs bei heimlichen Ermittlungsmaßnahmen fordert, bei denen der Betroffene keine Möglichkeit hat, die Strafverfolgungsbehörden dazu anzuhalten, den Kernbereich privater Lebensgestaltung zu achten.[65] Wenn der BGH zur Begrenzung des Eingriffs auf die Beweiserheblichkeit im Einzelfall verweist,[66] also auf den Grundsatz der Verhältnismäßigkeit als die Beweiserhebung limitierenden Faktor, wird auch das der Rechtsprechung zum Kernbereichsschutz letztlich gerecht. Denn absoluten Kernbereichsschutz verlangt das BVerfG erst auf Beweisverwertungsebene.[67]

Dem Eingriffsgewicht zum Trotz weist der BGH kritische Stimmen[68] zurück, die eine andere, speziellere, enger gefasste Eingriffsgrundlage als § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO fordern.[69] Einer auf bestimmte, schwere Straftaten beschränkten Befugnisnorm bedürfe es nicht.[70] Die Regelung in den §§ 94 ff., 102 ff. StPO genüge verfassungsrechtlichen wie europarechtlichen Vorgaben.[71] Insbesondere ergebe sich die Befugnis zur Datenerhebung nach Anlass, Umfang und Zweck hinreichend bestimmt aus den Vorschriften über die Beschlagnahme im Regelungszusammenhang mit dem Zweck der Ermittlungen (§§ 152, 155, 160, 170, 244, 264 StPO) und der Verhältnismäßigkeitsprüfung im Einzelfall.[72] Eine genauere Bestimmung sei der Vielgestaltigkeit möglicher Sachverhalte wegen nicht geboten.[73] Anzumerken ist, dass eine genauere Bestimmung sich auch nicht aus § 81b Abs. 1 StPO ergibt. Diese Sichtweise wird vom BVerfG gebilligt.[74] Noch ungeklärt ist aber, ob der EuGH dieser großzügigen Sichtweise folgt.

Der Idee, den Beschlagnahmezugriff auf die Daten eines Mobiltelefons durch eine Anlasstatenregelung auf die Bekämpfung schwerer Kriminalität zu beschränken, hat auch der EuGH eine Absage erteilt. Der EuGH verweist stattdessen auf eine Einzelfallprüfung der Verhältnismäßigkeit, wie sie das deutsche Recht ohne Weiteres vorsieht.[75] Anderenfalls sei eine erhöhte Gefahr der Straflosigkeit sonstiger Taten zu befürchten.[76] Freilich folgert der EuGH aus Art. 4 Abs. 1 Richtlinie (EU) 2016/680 und Art. 52 Abs. 1 GrCh die Notwendigkeit gesetzlicher Bestimmtheit dergestalt, dass „die Rechtsgrundlage, die eine solche Einschränkung gestattet, deren Tragweite hinreichend klar und präzise definieren muss".[77] Dazu müsse der nationale Gesetzgeber „die zu berücksichtigenden Gesichtspunkte, insbesondere die Art oder die Kategorien der betreffenden Straftaten, hinreichend präzise definieren".[78] Der BGH reagiert darauf mit einer Variation des Arguments, es genügten gesetzliche Bestimmbarkeit und eine Auslegung durch die Rechtsprechung, die zu Bestimmtheit führe.[79] Um eine hinreichend bestimmte Auslegung nachzuweisen, erläutert der BGH die Parameter einer die Datenerhebung nach Anlass, Umfang und Zweck begrenzenden Verhältnismäßigkeitsprüfung in allen Einzelheiten.[80] Das alles kann aber nicht überzeugen. Zwar ist in der europäischen Rechtsprechung ungeschriebenes Recht anerkannt.[81] Das wird man aber auf Common-law-Systeme zu beziehen haben.[82] Und eine Auslegung ohne konkreten Anhaltspunkt in der Strafprozessordnung als „gesetzlich vorgesehene Einschränkung" i.S.v. Art. 52 Abs. 1 GrCh auszugeben, hieße, den Gesetzesvorbehalt vollständig zu entwerten.

Mit Blick auf die entscheidende Weichenstellung schon im Vorfeld der Datenauswertung ist daher ist aus der Entscheidung des EuGH abzuleiten, dass eine Befugnis zur Entsperrung von Mobiltelefonen gesetzlicher Regelung bedarf und dass diese Regelung die Tragweite des Eingriffs und die wesentlichen zu berücksichtigenden Gesichtspunkte, insbesondere die Art und die Kategorien von Straftaten, hinreichend präzise bestimmen muss.[83] Dafür streiten auch die

[63] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II) = BeckRS 2025, 19413 Rn. 125.
[64] *Eckstein* (Fn. 49), § 100d Rn. 10, 41 ff.; *Rückert* (Fn. 6), S. 146 ff., 499 ff., 743.
[65] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370, 595/07 = BVerfGE 120, 274 (336 f.).
[66] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 34.
[67] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II) = BeckRS 2025, 19413 Rn. 125 f.
[68] Nachweise in Fn. 53 ff., 96.
[69] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 35, 42 ff.
[70] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 42.
[71] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 45 ff.
[72] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 46 ff.
[73] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 46.
[74] Vgl. nur BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06 = BVerfGE 124, 43 (60 ff.); BVerfG, Urt. v. 2.3.2006 – 2 BvR 2099/04 = BVerfGE 115, 166 (191 ff.); BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02 = BVerfGE 113, 29 (50 ff.).
[75] Die Verhältnismäßigkeitsprüfung wird in Art. 52 Abs. 1 GrCh durch Ausformulierung der Zwecksetzung angereichert: von der Union anerkannte, dem Gemeinwohl dienende Zielsetzungen oder Erfordernisse des Schutzes der Rechte und Freiheiten anderer.
[76] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (324 f.). Kritisch *Rataj*, NStZ 2025, 398 (402).
[77] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325).
[78] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325).
[79] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 50. Vgl. für das materielle Strafrecht BVerfG, Beschl. v. 9.2.2022 – 2 BvL 1/20 = BVerfGE 160, 284 (319 ff.).
[80] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 46 ff. m.w.N.
[81] EuG, Urt. v. 27.4.2022 – T-710/21, T-722/21, T-723/21 = BeckRS 2022, 8458 Rn. 81.
[82] *Schwerdtfeger*, in: Meyer/Hölscheidt (Hrsg.), Charta der Grundrechte der Europäischen Union, 6. Aufl. 2024, Art. 52 Rn. 33.
[83] Für eine gesetzliche Regelung auch *Cornelius*, NJW 2025, 2270 (2271); *Luh/Grosmann*, ZD 2025, 457 (458): bislang fehlende Definition der Anlassstraftaten und fehlender expli-

erforderlichen Vorkehrungen zum Schutz biometrischer Daten gem. § 500 StPO i.V.m. §§ 48, 46 Nr. 14 lit. c BDSG.[84] Die Regelung sollte auf sonstige zugriffsgeschützte Datenträger erstreckt werden und für alle Zugriffsarten gelten, die nicht gegen den Nemo-tenetur-Grundsatz verstoßen (z.B. brute force; oben IV. und unten VI.). § 110 Abs. 3 S. 2 StPO sollte darauf Bezug nehmen. De lege ferenda werden Bagatelldelikte auszunehmen sein – wenn auch nicht alle Ordnungswidrigkeiten (§§ 130, 30 OWiG)[85] – es sei denn, das Mobiltelefon ist Teil der Tatbegehung. Eine höhere Anlasstatenschwelle wird sich gegenüber zu erwartenden Gegenstimmen aus der Praxis kaum durchsetzen lassen. Kompensierend muss daher der Datenzugriff zielführend kanalisiert und beschränkt werden. Dazu könnte, angelehnt an die Vorschriften der österreichischen Strafprozessordnung,[86] eine verpflichtende Beschränkung schon der Durchsicht des Datenbestands nach jeweils zu begründenden Datenkategorien, Dateninhalten und vor allem Zeiträumen vorgesehen werden (vgl. § 115f Abs. 3 Hs. 2 öStPO; eine andere Frage ist, ob vorab eine komplette Kopie des Datenträgers anzufertigen ist und inwieweit eine Kopie die Sicherstellung der Hardware entbehrlich machen kann;[87] jedenfalls muss jedem Betroffenen eine Kopie seines Datenträgers zur sachgerechten Interessenwahrnehmung zur Verfügung stehen, bei Datenträgern Dritter muss die Verteidigung des Beschuldigten grundsätzlich den gesamten, für die Durchsicht ausgewählten Datenbestand einsehen können[88]). Diese Hürde könnte mit einer zweiten Anlasstatenschwelle verknüpft werden, die bei schwersten Straftaten die Durchsicht erleichtert. Umgekehrt könnte bei und in den Grenzen einer Zustimmung des Betroffenen auch ein vereinfachtes Verfahren[89] den Zugriff auf konkrete einzelne Informationen ermöglichen.

Aus der Pflicht zur Differenzierung zwischen verschiedenen Kategorien betroffener Personen nach Art. 6 Richtlinie (EU) 2016/680 schließt der EuGH auf ein Adressierungserfordernis dergestalt, dass im Falle des Beschuldigten mindestens „hinreichende objektive Anhaltspunkte" den Verdacht begründen müssen.[90] Das entspricht fast wörtlich dem Anfangsverdacht i.S.v. § 152 Abs. 2 StPO und ergibt daher keine zusätzliche Einschränkung. Jedoch wird eine Adressatenregelung vorzusehen sein, die auch den Zugriff auf Mobiltelefone Nichtbeschuldigter einschließt (unten VI.).[91] Außerdem bedürfen schwerwiegende oder besonders schwerwiegende Eingriffe in Art. 7, 8 GrCh, von begründeten Eilfällen abgesehen, der vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle,[92] so dass ein entsprechender Richtervorbehalt zu normieren ist. Schließlich muss das Verfahrensrecht die in Art. 13 und Art. 54 Richtlinie (EU) 2016/680 i.V.m. Art. 47 GrCh vorgesehenen Anforderungen an die Gewährleistung nachträglichen Rechtsschutzes umsetzen. Ein wirksamer Rechtsbehelf setzt Information voraus, und zwar Information des auf Datenebene Betroffenen (Art. 6) nach Maßgabe des Art. 13 Richtlinie (EU) 2016/680, dessen Abs. 3 eine Zurückstellung erlaubt, wenn die Information das Verfahren beeinträchtigen würde.[93]

Zur Klärung wäre die Sache nach Art. 267 AEUV dem EuGH vorzulegen gewesen. Doch der BGH versucht stattdessen, die erforderliche Rechtsgrundlage in der StPO zu finden.

VI. Zur Reichweite von Befugnisnormen

1. Erkennungsdienstliche Maßnahmen, Identitätsfeststellung, Befugnisgeneralklauseln

Der BGH schließt sich der Auffassung an, die biometrische Entsperrung eines Mobiltelefons durch zwangsweises Auflegen eines Fingers des Beschuldigten auf den Fingerabdrucksensor könne de lege lata auf § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO als Ermächtigungsgrundlage gestützt werden.[94] Teilweise werden von den Vertretern dieser Ansicht verdeckte Eingriffe (Entsperrung, während der Betroffene schläft oder bewusstlos ist) explizit ausgenommen.[95] Kritische Stimmen, die § 81b Abs. 1 StPO nach Wortlaut, Systematik, Entstehungsgeschichte und Ratio enger fassen wollen und für eine voraussetzungsreichere, hinreichend bestimmte Befugnisnorm plädieren,[96] weist der BGH zurück:[97] Als der Aufnahme von

ziter Richtervorbehalt; für Subsidiarität *Hiéramente*, StV 2024, 611 (615); für eine Beschränkung der Anlasstaten kraft Verhältnismäßigkeit schon de lege lata *Neuhaus*, StV 2020, 489 (492).

[84] Vgl. *Rückert*, StV 2025, 350 (352).

[85] *Hiéramente*, StV 2024, 611 (614).

[86] Näher zu deren Neufassung *Zerbes*, GA 2024, 421 (429 ff.) m.w.N.

[87] Näher dazu *El-Ghazi* (Fn. 47), C 23 f., 32 f. m.w.N.

[88] *Zerbes*, GA 2024, 421 (438 f.). Ausnahmen zum Schutz von Persönlichkeitsrechten liegen bei Datenträgern Dritter nahe.

[89] *Zerbes*, GA 2024, 421 (437).

[90] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325).

[91] Vgl. dazu *Eckstein* (Fn. 49), § 100a Rn. 20.

[92] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325 f.).

[93] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (326 f.).

[94] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 35. Für zweistufiges Vorgehen nach § 81b StPO (Entschlüsselung) und §§ 94 ff. StPO (Datenzugriff) OLG Bremen, Beschl. v. 8.1.2025 – 1 ORs 26/24 = NJW 2025, 847; LG Ravensburg, Beschl. v. 14.2.2023 – 2 Qs 9/23 jug. = BeckRS 2023, 3879; AG Baden-Baden, Beschl. v. 13.11.2019 – 9 Gs 982/19 = BeckRS 2019, 66684 (Entsperrung analog § 81b StPO); *Neuhaus*, StV 2020, 489 (490 f.); *Rottmeier/Eckel*, NStZ 2020, 193 (194 ff.), zum Zitiergebot *dies.*, NStZ 2020, 193 (200); *Ruhs*, GSZ 2024, 254 ff.; vgl. auch *Bäumerich*, NJW 2017, 2718 (2721).

[95] *Rottmeier/Eckel*, NStZ 2020, 193 (197).

[96] *Cornelius*, NJW 2025, 2270 (2271); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (118 ff.); *Hecken/Ziegler*, jurisPR-ITR 10/2023 Anm. 5; *F. Horn*, Kriminalistik 2019, 641 (642 ff.); *Horter*, NStZ 2023, 447 (448); *Jahn*, JuS 2025, 791 (792 f.); *Luh/Grosmann*, ZD 2025, 457 (458); *Momsen*, DRiZ 2018, 140 (141 ff.); *Nadeborn/Albrecht*, NZWiSt 2021, 420 (423 f.); *Nicolai*, StV Spezial 2023, 148 (148 f.). Vgl. auch *Bosch* (Fn. 36), § 81b Rn. 7.

[97] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 35 ff.

Fingerabdrücken zumindest ähnliche, das heißt, der Feststellung der körperlichen Beschaffenheit des Beschuldigten dienende Maßnahme soll das Entsperren unter den Wortlaut des § 81b Abs. 1 StPO fallen.[98]

Zur Begründung verweist der BGH auf eine Ununterscheidbarkeit „dem äußeren Anschein nach".[99] Das Aufnehmen von Fingerabdrücken erfolge weitgehend digital durch Pressen des Fingers auf eine Lesevorrichtung. Anschließend finde eine daktyloskopische Vergleichsuntersuchung statt. Das Auflegen des Fingers auf den Fingerabdrucksensor eines Mobiltelefons zur Feststellung der Papillarlinien und zum Abgleich mit zuvor gespeicherten Daten könne davon „dem äußeren Anschein nach" nicht unterschieden werden.[100] Die verkürzende Betrachtung nur des äußeren Anscheins verfehlt allerdings den Wortlaut des Gesetzes. Anderenfalls müsste das Niederschlagen einer Person, die leblos liegen bleibt, in Zukunft als töten i.S.v. § 212 Abs. 1 StGB angesehen werden, auch wenn das Opfer überlebt. Der äußere Anschein kann eben trügen. Und der BGH versucht mit Hilfe des äußeren Anscheins darüber hinwegzutäuschen, dass das Entsperren eines Mobiltelefons nicht der Feststellung der körperlichen Beschaffenheit des Beschuldigten dient, sondern dem Eröffnen des Zugriffs auf Daten. Anders verhielte es sich, wenn die Strafverfolgungsbehörden den Finger eines Beschuldigten auf den Fingerabdrucksensor eines Mobiltelefons auflegten, um ihm dieses Telefon zuzuordnen.[101] Damit soll nicht gesagt sein, dass Befugnisnormen immer direkt zum Ziel führen müssen. Mittelbare Zweckverfolgung genügt, beispielsweise, wenn das Versenden einer stillen SMS auf § 100i StPO gestützt wird, obwohl erst die zusätzliche Verkehrsdatenerhebung nach § 100g StPO den Standort der Zielperson offenbart.[102] Befugnisnormen können aber nicht umgekehrt zur Erreichung überschießender Effekte herangezogen werden, nur weil ein äußerer Anschein den überschießenden Effekt nicht erkennen lässt. Genau genommen wird ohnehin schon der äußere Anschein verkürzt, wenn bei seiner Festlegung das Entsperren des Mobiltelefons ausgeklammert wird. Der Begriff des äußeren Anscheins impliziert eine Unsicherheit, die nicht mit dem Vorbehalt des Gesetzes vereinbar ist.

Der Versuch, die weitergehende Zielrichtung der Entsperrung, also das Eröffnen des Zugriffs auf Daten zu verstecken, prägt auch die Argumentation des BGH zu Entstehungsgeschichte, Systematik und Ratio des § 81b StPO. Es trifft zwar zu, dass – jedenfalls bei objektiver Auslegungsrichtung[103] – Maßnahmen unter § 81b Abs. 1 StPO subsumiert werden können, von denen der Gesetzgeber bei Verabschiedung der Norm nichts wissen konnte.[104] Insbesondere die ausdrückliche Zulassung ähnlicher Maßnahmen ist technikoffen zu verstehen.[105] Ebenso überzeugt es, § 81b Abs. 1 StPO der verkürzenden gesetzlichen Überschrift zum Trotz nicht auf erkennungsdienstliche Maßnahmen im Sinne der Zwecke des Erkennungsdienstes (§ 81b Abs. 1 Alt. 2 StPO) zu beschränken, weil nach Wortlaut, Systematik und Teleologie die im Gesetz ausdrücklich genannte allgemeine Zielrichtung der Zwecke der Durchführung des Strafverfahrens Beachtung verlangt.[106] Das ändert aber nichts daran, dass § 81b Abs. 1 StPO nur zu Maßnahmen ermächtigt, die der Feststellung der körperlichen Beschaffenheit des Beschuldigten dienen.[107] Und zwar einer Feststellung zum Zwecke der Wiedererkennung dieser körperlichen Beschaffenheit. Daran anknüpfend erlaubt § 163b Abs. 1 S. 3 StPO erkennungsdienstliche Maßnahmen zur Identitätsfeststellung, also zum Zwecke der Aufhebung der Anonymität einer Person. Erkennungsdienstliche Maßnahmen nach § 81b Abs. 1 StPO dienen der Erkennung, entweder für Zwecke der Durchführung des Strafverfahrens (Alt. 1) oder für die auf Abwehr künftiger Gefahren zielenden Zwecke des Erkennungsdienstes (Alt. 2). Der BGH hält einen Fingerabdruckvergleich durch das Mobiltelefon für ebenso erlaubt wie andere daktyloskopische Vergleichsuntersuchungen.[108] Die weitergehende Zielrichtung der Entsperrung, also das Eröffnen des Zugriffs auf Daten, sprengt aber die Grenzen der Ermächtigung zur Wiedererkennung i.S.v. § 81b StPO.[109] Dasselbe gilt für § 163b StPO.

Auch wenn der BGH für den anschließenden Zugriff auf die Daten des Mobiltelefons flankierend §§ 94, 110 StPO heranzieht,[110] bleibt es dabei, dass zwischen Fingerabdruckerfassung und Datenzugriff das Eröffnen des Zugriffs auf

[98] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 36 f. Ebenso *Rottmeier/Eckel*, NStZ 2020, 193 (195).
[99] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 38.
[100] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 38.
[101] Ebenso *Horter*, NStZ 2023, 447 (448).
[102] *Eckstein* (Fn. 49), § 100i Rn. 19 ff. m.w.N. zum Streitstand.
[103] Näher dazu *Wank*, Juristische Methodenlehre, 2019, § 6 Rn. 152 ff.
[104] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 39 f. Ebenso *Rottmeier/Eckel*, NStZ 2020, 193 (195). Zur Neufassung der Absätze 2 bis 5 des § 81b StPO LG Ravensburg, Beschl. v. 14.2.2023 – 2 Qs 9/23 jug. = BeckRS 2023, 3879 Rn. 12. Kritisch *Bock/Fülscher*, StraFo 2023, 386 (388: Schweigen des Gesetzgebers bei der Neufassung); *Roggan*, NJW 2015, 1995 (1998).
[105] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 39 f. m.w.N.
[106] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 40 f. m.w.N.
[107] *Bock/Fülscher*, StraFo 2023, 386 (387 f.); *Nadeborn/Albrecht*, NZWiSt 2021, 420 (423 f.); etwas überspitzt *Hecken/Ziegler*, jurisPR-ITR 10/2023 Anm. 5: Maßnahmen an einem technischen Gegenstand sind nicht erfasst; ähnlich *F. Horn*, Kriminalistik 2019, 641 (642).
[108] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 37 f.
[109] Ähnlich *Grzesiek/Zühlke*, StV Spezial 2021, 117 (119); *Hecken/Ziegler*, jurisPR-ITR 10/2023 Anm. 5; *Horter*, NStZ 2023, 447 (448); *Momsen*, DRiZ 2018, 140 (141, 143); *Nadeborn/Albrecht*, NZWiSt 2021, 420 (423 f.); *Nicolai*, StV Spezial 2023, 148 (148 f.); *Ruppert*, StV 2025, 565 (565 f.); *Satzger/Sarfraz*, NStZ 2025, 566.
[110] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 42 ff. Ebenso *Rottmeier/Eckel*, NStZ 2020, 193 (195 f.).

Daten, also die Entsperrung erfolgen muss.[111] Sie kann nicht auf § 81b StPO gestützt werden. Aufschlussreich ist, dass sie vom BGH, beim Wort genommen, auch nicht allein auf § 81b StPO, sondern auf § 81b Abs. 1 StPO i.V.m. §§ 94 ff. StPO als Ermächtigungsgrundlage gestützt wird, und zwar einschränkend nur dann, wenn eine nach §§ 102, 105 Abs. 1 StPO richterlich angeordnete Durchsuchung dem Auffinden von Mobiltelefonen diente und der Datenzugriff verhältnismäßig ist.[112] Genau genommen nimmt der BGH also Zuflucht zu einer Kumulation von Befugnisnormen. Und diese Kumulation soll eine Befugnislücke schließen. Sie ist nicht damit zu erklären, dass ein Entsperren – § 81b Abs. 1 StPO – aus Gründen der Verhältnismäßigkeit nur erfolgen darf, wenn auch der anschließende Datenzugriff – §§ 94 ff. StPO – zulässig ist.[113] Vielmehr korrespondiert die kumulierende Betrachtung des BGH mit der unzulänglichen Reichweite des § 81b StPO und der Entscheidung des EuGH vom 4.10.2024, die schon den Versuch der Strafverfolgungsbehörden, Zugang zu den auf einem Mobiltelefon gespeicherten Daten zu erlangen, als Datenverarbeitung im Anwendungsbereich von Art. 2 Abs. 1 Richtlinie (EU) 2016/680 i.V.m. Art. 1 Abs. 1 und Art. 3 Nr. 2 Richtlinie (EU) 2016/680 einordnet.[114] Der EuGH verlangt gerade dafür insbesondere eine richterliche Anordnungskompetenz, die § 81b StPO nicht vorsieht, die sich aber aus §§ 94 ff., 102, 105 StPO ergeben könnte.

Die Tücken der kumulierenden Flickschusterei offenbaren sich im vorliegenden Fall anschaulich. Denn beim Rückgriff auf die richterliche Zuständigkeit für die Beschlagnahme (§ 98 StPO) konnte der BGH es nicht bewenden lassen, fehlte doch im vorliegenden Fall ein Beschlagnahmebeschluss (oben III.). Durch die zusätzliche Heranziehung der §§ 102, 105 StPO versucht der BGH, die vorherige richterliche Kontrolle zu etablieren, die der EuGH für die Entsperrung eines Mobiltelefons, von Eilfällen abgesehen, verlangt.[115] Deshalb beschränkt der BGH seine Entscheidung über die Zulassung der zwangsweisen Entsperrung von Mobiltelefonen auf Fälle, in denen eine nach §§ 102, 105 Abs. 1 StPO richterlich angeordnete Durchsuchung dem Auffinden von Mobiltelefonen diente und der Datenzugriff verhältnismäßig ist.[116] Ausführlich legt der BGH dar, dass schon der Durchsuchungsbeschluss die datenschutzrechtlich gebotene Begrenzung der Datenerhebung nach Anlass, Umfang und Zweck leisten muss.[117] Diese Konstruktion jedoch bleibt unzulänglich. Zum Beispiel können die Voraussetzungen für ein Vorgehen ohne richterliche Anordnung wegen Gefahr im Verzug bei der Durchsuchung vorliegen, das muss aber keineswegs zugleich für die spätere Entsperrung des bereits sichergestellten Mobiltelefons gelten.[118] Wie soll vorgegangen werden, wenn nicht schon die Durchsuchung auf das Auffinden von Mobiltelefonen gerichtet war oder wenn keine Durchsuchung vorausging? Es zeigt sich: Die Kumulation von Eingriffsvoraussetzungen kann eine gesetzliche Befugnisnorm für die Entsperrung samt Richtervorbehalt nicht ersetzen. Einer solchen bedarf es (oben V.).

Die vom BGH vorgeschlagene Lösung erweist sich als unzulässige Lückenfüllung durch Kumulation der Voraussetzungen unterschiedlicher Eingriffsgrundlagen für eine Maßnahme, die überdies mit dem IT-System-Grundrecht ein anderes Grundrecht betrifft und eine wesentlich gravierendere Eingriffstiefe hat als die anerkannten Fälle des § 81b Abs. 1 StPO.[119] Dass erst recht die Befugnisgeneralklauseln in den §§ 161, 163 StPO nicht hinreichen, ergibt sich aus dem Gewicht des in Rede stehenden Grundrechtseingriffs.[120]

2. Körperliche Untersuchung

Vereinzelt wird ein Rückgriff auf § 81a StPO erwogen.[121] Überwiegend jedoch wird für § 81a StPO davon ausgegangen, dass die Vorschrift auf den Körper als Beweismittel abzielt.[122] Das überzeugt zwar nicht. Denn § 81a StPO dient umfassend der Feststellung von Tatsachen, die für das Verfahren von Bedeutung sind, und zeichnet sich durch spezifische Mittel aus, nämlich körperliche Untersuchungen und Eingriffe.[123] Es bleibt aber dabei, dass § 81a StPO ebenso wenig wie § 81b StPO eine Rechtsgrundlage für die Entsperrung eines Mobiltelefons normiert. Die vom BGH entwickelte Lehre vom äußeren Anschein wird für § 81a StPO glücklicherweise nicht als großer Gleichmacher herangezogen. Die Klarheit, mit der die Unanwendbarkeit des § 81a StPO festgestellt wird, wünschte man sich auch für § 81b StPO:

> „Im Zentrum der Maßnahme steht nicht die Feststellung der biometrischen Merkmale, sondern deren Verwendung. Das zeigt sich auch daran, dass den Strafverfolgungsbehörden die konkrete Beschaffenheit der körperlichen Merkmale vollkommen gleichgültig ist, solange sie nur

[111] Vgl. dazu *Bäumerich*, NJW 2017, 2718 (2721: von § 81b StPO gedeckt). Diese Dreistufigkeit übersehen auch *Rottmeier/Eckel*, NStZ 2020, 193 (195 f.).

[112] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28, 35.

[113] Zu dieser Verknüpfung *Rottmeier/Eckel*, NStZ 2020, 193 (196).

[114] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (322 f.).

[115] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 51 ff.

[116] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 28, 51 ff.

[117] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 53.

[118] *Satzger/Sarfraz*, NStZ 2025, 566.

[119] *Jahn*, JuS 2025, 791 (792 f.), verweist schlagend auf BGHSt 51, 211 (218 Rn. 22: Online-Durchsuchung vor der Neuregelung in § 100b StPO). Grundlegend zu den Grenzen der Rechtsfortbildung bei strafprozessualen Eingriffsbefugnissen *Rückert* (Fn. 6), S. 465 ff., der ebenfalls eine neue Befugnisnorm für das Entsperren von IT-Systemen fordert (a.a.O., S. 489, 507).

[120] *Bock/Fülscher*, StraFo 2023, 386 (389 f.); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (120).

[121] Vgl. dazu AG Ravensburg, Beschl. v. 12.1.2023 – 11 Gs 69/23 = BeckRS 2023, 4139; weiterer Nachweis bei *Momsen*, DRiZ 2018, 140 (141 Fn. 11).

[122] *Bäumerich*, NJW 2017, 2718 (2720); *Bock/Fülscher*, StraFo 2023, 386; *F. Horn*, Kriminalistik 2019, 641 (642); *Momsen*, DRiZ 2018, 140 (141); *Rottmeier/Eckel*, NStZ 2020, 193 (196 f.).

[123] Näher dazu *Eckstein* (Fn. 35), S. 156 f. m.w.N.

zu den im Smartphone hinterlegten Schlüsselmerkmalen passen. § 81a StPO ist damit schon nach seinem Wortsinn nicht einschlägig."[124]

3. Telekommunikationsüberwachung, Online-Durchsuchung, Bestandsdatenauskunft

Für eine Befugnisnorm mit strengeren Voraussetzungen, als § 81b StPO sie vorsieht, streitet das Gewicht des Eingriffs.[125] § 100j StPO betrifft allerdings nur die Auskunft über zugriffsschützende Daten durch den Telekommunikationsdienstleister oder Erbringer digitaler Dienste und scheidet daher aus.[126] Eine Telekommunikationsüberwachung nach § 100a Abs. 1 S. 1 StPO erfasst nur Telekommunikation im Herrschaftsbereich des Telekommunikationsdienstleisters.[127] Die Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 S. 2, 3 StPO) und die Online-Durchsuchung (§ 100b StPO) sind dagegen umfassende Ausforschungserlaubnisse für Endgeräte. Schon die Quellen-Telekommunikationsüberwachung ist ein Schwarzes Loch der Datenerhebung, weil sie potentiell alle ab Anordnung per Telekommunikation übermittelten Daten zum Ausforschungsobjekt macht. Diese Fehlkonstruktion muss de lege ferenda beseitigt und der Eingriff § 100b StPO zugeordnet werden.[128] Das BVerfG hat die Regelung für teilweise verfassungswidrig und nichtig erklärt.[129] Für die Online-Durchsuchung entfällt sogar das Erfordernis eines früheren Telekommunikationsbezugs, so dass alle für die Ermittlung erforderlichen Daten erhoben werden dürfen. Immerhin knüpft § 100b StPO diese Super-Überwachungsbefugnis an strenge Voraussetzungen.[130]

Dass §§ 100a, 100b StPO heimliche Eingriffe erlauben, spricht nicht gegen ihre Anwendung auf offene Maßnahmen wie die Entsperrung eines Mobiltelefons.[131] Das stellt die Formulierung „auch ohne Wissen" im jeweiligen Abs. 1 S. 1 unmissverständlich klar. Aus der Formulierung „mit technischen Mitteln" folgt aber, dass nicht jede Eingriffsform erfasst ist. Zwar könnte neben dem Brute-force-Zugriff wohl auch, gerade noch, eine Passworteingabe darunter subsumiert werden,[132] nicht aber der zusätzliche Zwang, die Verwendung des eigenen Körpers zur Öffnung biometrischer Sicherungen zu dulden.[133] Ein Analogieschluss scheidet im Eingriffsrecht aufgrund des Vorbehalts des Gesetzes richtigerweise aus.[134]

Darf für das Entsperren eines Mobiltelefons wegen einer Nähe der Maßnahme zu §§ 100a, 100b, 100j StPO nicht auf andere Befugnisnormen wie §§ 81b, 94 ff. StPO zurückgegriffen werden?[135] Aus § 100j Abs. 1 S. 2, 3 StPO wird vereinzelt gefolgert, Passwörter und andere zugriffsschützende Daten dürften nur nach dieser Vorschrift erhoben werden.[136] § 100j StPO beschränkt sich freilich nach Wortlaut, Systematik und Ratio auf eine konkrete Datenerhebungssituation, nämlich die Auskunft durch den geschäftsmäßigen Diensteerbringer (siehe § 100j Abs. 5 StPO) über dort gespeicherte Daten auf der Grundlage des Doppeltürmodells. Rückschlüsse auf andere Datenerhebungssituationen – Auskunft vom Beschuldigten und Nemo-tenetur-Grundsatz (oben IV.), Zeugenpflichten bei Kenntnis Dritter – lässt die Regelung nicht zu. Dementsprechend entfaltet sie auch keine Sperrwirkung.[137] Vielmehr betrachtet der Gesetzgeber den offenen Beschlagnahmezugriff als grundsätzlich zulässig. Das stellt § 100g Abs. 5 StPO partiell klar,[138] weil das BVerfG im SIM-Karten-Beschluss[139] für Telekommunikationsverkehrsdaten andere Schlüsse gezogen hatte.[140] Auch §§ 100a, 100b StPO haben insofern keine Sperrwirkung.

4. Durchsuchung und Beschlagnahme

Der Leser fragt sich, warum der BGH den Umweg über § 81b StPO nimmt. Genügen nicht allein §§ 94 ff., 102 ff. StPO als Befugnisnormen, wenn in anderen Fällen den Durchsuchungs- und Beschlagnahmevorschriften als Annexkompetenz die Ermächtigung zu vorbereitenden Eingriffen entnommen wird (z.B. Aufbrechen einer Tür)?[141] Der BGH führt zu den Voraussetzungen der Beschlagnahme aus, dass nicht nur Sachen, sondern auch Daten beschlagnahmefähig sind.[142] Damit ist

[124] *Rottmeier/Eckel*, NStZ 2020, 193 (197).
[125] Nachweise in Fn. 96.
[126] Zutreffend *Rottmeier/Eckel*, NStZ 2020, 193 (198). Anders bei Abfrage der PIN oder PUK vom Telekommunikationsdienstleister zur Überwindung einer SIM-Kartensperre, *Neuhaus*, StV 2020, 489 (490).
[127] *Eckstein* (Fn. 49), § 100a Rn. 67.
[128] *Eckstein* (Fn. 49), § 100a Rn. 23, 58 ff., 97.
[129] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II) = BeckRS 2025, 19413 Rn. 176 ff., 188 ff. (unzulängliche Anlasstatenregelung).
[130] Trotz Verstoßes gegen das Zitiergebot (Art. 19 Abs. 1 S. 2 GG) lässt das BVerfG die Fortgeltung zu, BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II) = BeckRS 2025, 19413 Rn. 240 ff., 275.
[131] A.A. *Bock/Fülscher*, StraFo 2023, 386 (389); *Rottmeier/Eckel*, NStZ 2020, 193 (197).
[132] OLG Stuttgart, Beschl. v. 19.5.2021 – 2 Ws 75/21 = BeckRS 2021, 15469 Rn. 19.
[133] *Eckstein* (Fn. 49), § 100a Rn. 109; *Rottmeier/Eckel*, NStZ 2020, 193 (197).
[134] Vermittelnd *Rückert* (Fn. 6), S. 491 ff. (Analogie nur in den vom Wesentlichkeitsprinzip gezogenen Grenzen) m.w.N. zum Streitstand.
[135] So wohl *Momsen*, DRiZ 2018, 140 (142 f.).
[136] *Graf*, in: Graf (Fn. 31), § 100j Rn. 23; *Hauck*, in: Löwe-Rosenberg (Fn. 33), StPO § 100j Rn. 12.
[137] *Eckstein* (Fn. 49), § 100j Rn. 39 f.; *Rottmeier/Eckel*, NStZ 2020, 193 (198).
[138] Näher dazu *Eckstein* (Fn. 49), § 100g Rn. 124 ff.
[139] BVerfG, Beschl. v. 4.2.2005 – 2 BvR 308/04 = NStZ 2005, 337.
[140] BT-Drs. 16/5846, S. 26.
[141] *Schmitt*, in: Schmitt/Köhler, Strafprozessordnung, Kommentar, 67. Aufl. 2024, § 81b Rn. 8a, stützt die Nutzung der Fingerabdrücke, also die Entsperrung des Mobiltelefons, auf eine Annexkompetenz zu § 94 StPO. Für eine Neuregelung der Beschlagnahme von großen Datenbeständen und in der Folge eine Annexkompetenz *F. Horn*, Kriminalistik 2019, 641 (643 f.). Zur Beschlagnahme eines Zettels, auf dem die PIN notiert ist, *Rottmeier/Eckel*, NStZ 2020, 193 (198).
[142] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 44.

eine Datenkopie gemeint und das entspricht der ganz überwiegenden Ansicht.[143] Eine vorgeschaltete Durchsicht von Datenträgern gestattet § 110 Abs. 3 StPO. §§ 94 ff. StPO und §§ 102 ff. StPO genügen nach Ansicht des BGH verfassungsrechtlichen wie europarechtlichen Vorgaben (oben V.).[144]

Dennoch beschließt der BGH seine Ausführungen zur gesetzlichen Bestimmtheit der Regelung in §§ 94 ff. StPO mit einer Bezugnahme auf § 81b Abs. 1 StPO.[145] Möglicherweise soll die Heranziehung dieser, im Gegensatz zu den uferlos weiten Durchsuchungs- und Beschlagnahmevorschriften, sachnäher und konkreter bestimmt erscheinenden Rechtsgrundlage europarechtlichen Bedenken zuvorkommen (oben V.).[146] Für eine Art Windowdressing spricht, dass der BGH in einer überraschenden Volte das Fehlen einer Anordnung nach § 81b StPO für unerheblich erklärt; zu dieser Lücke im Durchsuchungsbeschluss führt der BGH aus:

> „Ob der Zugriff dann ohne Weiteres oder unter Aufhebung einer numerischen oder einer biometrischen Verschlüsselung erfolgen konnte bzw. auf welche Weise diese vorzunehmen war, war nicht von entscheidender Relevanz."[147]

Und für den Fall, dass eine Entsperrung mangels Ermächtigungsgrundlage doch unzulässig wäre, ergänzt der BGH:

> „Ohnehin ergäbe sich aus der zwangsweisen Entsperrung kein Beweisverwertungsverbot."[148]

Dass schon im Durchsuchungsbeschluss der Richtervorbehalt wirksam werden soll, den der EuGH für die Entsperrung eines Mobiltelefons verlangt,[149] an diesen Baustein seiner Begründung glaubt der BGH offenbar selbst nicht. Dennoch: Wäre der Weg über eine Annexkompetenz gangbar?[150]

5. Lücken im Befugnisnormenkonzept der StPO

Die Strafprozessordnung schweigt weithin zu vorbereitenden und begleitenden Eingriffsmaßnahmen (z.B. Installation des Staatstrojaners für § 100b StPO und der Abhöreinrichtung für § 100c StPO). Dieses Schweigen erinnert an die gemeinrechtliche Vorstellung, was beweisrechtlich erlaubt sei, müsse auch zwangsweise durchgesetzt werden können. Doch diese Sichtweise ist mit dem Vorbehalt des Gesetzes unvereinbar.[151] Dementsprechend muss nach zutreffender Ansicht auch die heutige Lehre von der Annexkompetenz eingehegt und begrenzt werden.

Grundsätzlich zuzulassen sind meines Erachtens vorbereitende und begleitende Eingriffe, die auf eine andere Ermittlungsbefugnis der StPO gestützt werden können. Die mittelbare Zweckverfolgung im Sinne der Vorbereitung einer weiteren Ermittlungsmaßnahme genügt regelmäßig der Zwecksetzung von Ermittlungsmaßnahmen (z.B. Erforschung des Sachverhalts).[152] Darin liegt der wahre Kern des missglückten Rückgriffs auf § 81b StPO durch den BGH – missglückt, weil § 81b StPO die Entsperrung eines Mobiltelefons nicht gestattet. Eine solche Sukzession von Befugnissen ist keine unzulässige, dem Vorbehalt des Gesetzes widersprechende Kumulation von Eingriffsvoraussetzungen bzw. Addition zwecks Schaffung neuer Befugnisse.[153]

Diskutiert wird vor diesem Hintergrund beispielsweise, ob das Aufspielen einer Überwachungssoftware nach § 100a Abs. 1 S. 2, 3 StPO oder § 100b Abs. 1 StPO[154] im Anschluss an eine Entsperrung nach § 81b StPO erfolgen darf.[155] Abgesehen davon, dass schon die Entsperrung nicht auf § 81b StPO gestützt werden kann, würde dadurch jedoch die Beschränkung von § 100a Abs. 1 S. 2, S. 3, § 100b Abs. 1 StPO auf technische Mittel umgangen. Deshalb ist eine Sperrwirkung anzunehmen. Die Beschränkung sperrt auch die Sukzession von Befugnissen.[156] In vergleichbarer Weise wird teilweise vorgeschlagen, die Benutzung des menschlichen Körpers aus den Annexkompetenzen auszuscheiden, weil diese abschließend in den §§ 81a ff. StPO geregelt sei.[157]

Grundsätzlich werden Annexkompetenzen, vermittelnd und mit Unterschieden im Einzelnen, dann zugelassen, wenn es sich um typische, unerlässliche und verhältnismäßige Begleitmaßnahmen handelt,[158] wenn diese nicht intensiver in

[143] BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02 = NJW 2005, 1917 (1919 f.); zusammenfassend und kritisch *Stam*, JZ 2023, 1070 (1073 f.) m.w.N. (fehlende Befugnis zur Kopie).
[144] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 45 ff.
[145] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 50.
[146] *Rottmeier/Eckel*, NStZ 2020, 193 (196), erklären § 81b StPO für spezieller, so dass es keines Rückgriffs auf §§ 94, 110 StPO bedürfe.
[147] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 56.
[148] BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 59. A.A. *Bock/Fülscher*, StraFo 2023, 386 (390).
[149] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325 f.); BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 51 ff.
[150] Dafür *Stam*, JZ 2023, 1070 (1079).
[151] Näher dazu *Eckstein* (Fn. 35), S. 161 f. m.w.N.; *Ziemann*, ZStW 2018 (130), 762 (772 ff.).
[152] *Eckstein* (Fn. 49), § 100a Rn. 139 ff. m.w.N. Einschränkend *Horter*, NStZ 2023, 447 (448: Bezugnahme nötig).
[153] Vgl. dazu *Eckstein* (Fn. 49), § 100b Rn. 11 ff. m.w.N.; *Rüscher*, NStZ 2018, 687 (692). Abweichend *Nadeborn/Albrecht*, NZWiSt 2021, 420 (422 ff.): Aus Intensität und Qualität des Grundrechtseingriffs kann sich die Zulässigkeit einer Kumulation wie die Unzulässigkeit einer Sukzession ergeben; ähnlich *Schrott*, NSW 2024, 286 (293).
[154] Zur Verfassungswidrigkeit dieser Vorschriften siehe Fn. 129 f.
[155] Dafür *Rottmeier/Eckel*, NStZ 2020, 193 (198).
[156] *Eckstein* (Fn. 49), § 100a Rn. 201 m.w.N. A.A. *Rottmeier/Eckel*, NStZ 2020, 193 (198): Sperrung nur der Annexkompetenz.
[157] *Bock/Fülscher*, StraFo 2023, 386 (389); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (119 f.); *Horter*, NStZ 2023, 447 (448); *Nicolai*, StV Spezial 2023, 148 (149).
[158] BGH, Beschl. v. 11.10.2018 – 5 BGs 48/18 = BeckRS 2018, 47025 insbesondere zu Exzessen, Grenzen und § 164 StPO; *Ziemann*, ZStW 2018 (130), 762 (802 f.).

Grundrechte eingreifen als die Primärmaßnahme[159] oder wenn sie nicht in andere Grundrechte als die Primärmaßnahme eingreifen und erheblich weniger eingriffsintensiv sind.[160] Diese Gesichtspunkte entfalten aber richtigerweise nur in den Grenzen einer möglichen Auslegung der jeweiligen Befugnisnorm Relevanz.[161] Sie ersetzen nicht das Erfordernis einer Befugnisnorm. Daher lassen sich auf diese Weise zwar einzelne, notwendige Begleitmaßnahmen wie der freiheitsbeschränkende Zwang zur Durchführung körperlicher Untersuchungen und Eingriffe als mitgeregelte Bestandteile eingeräumter Befugnisse verstehen. Im Übrigen jedoch erscheint es konsequent und vorzugswürdig, vom Gesetzgeber ausdrückliche Befugnisnormen zu fordern, insbesondere für Substanzeingriffe, um deren Grenzen zu bestimmen (Aufbrechen der Wohnungstür etc.)[162] – auch wenn der gegenwärtige Rechtszustand für eine Übergangszeit hinzunehmen sein wird. Bei geringfügigen Eingriffen kommen die Befugnisgeneralklauseln in den §§ 161, 163 StPO als Rechtsgrundlage für Annex-Maßnahmen in Betracht.

Die Entsperrung eines Mobiltelefons kann, wie dargestellt, weder auf eine vorhandene spezielle Befugnisnorm noch auf die Befugnisgeneralklauseln gestützt werden. Von Durchsuchung und Beschlagnahme ist die Entsperrung, nach den geläufigen Auslegungsregeln, nicht als Annexkompetenz mitumfasst. Des Eingriffsgewichts wegen ist der Gesetzgeber vielmehr zur Neuregelung aufgerufen. Die Neuregelung sollte sich nicht auf die zwangsweise biometrische Entsperrung beschränken (oben V.). Sie sollte die Verwendung einer beschlagnahmten Notiz mit PIN oder Passwort einschließen, ebenso die Verwendung von Zugangsdaten, wenn ein verdeckter Ermittler von ihnen Kenntnis erlangt oder ein Zeuge über sie Auskunft gegeben hat, die offene wie die verdeckte Entsperrung. Denn bei allen Methoden zur Entsperrung muss die erhöhte Schutzbedürftigkeit von Zugangsdaten[163] berücksichtigt werden. Anderweitige Offenbarung der Zugangsdaten führt dabei nicht, im Sinne mangelnden Selbstschutzes, zu einer Absenkung der Anforderungen, schon weil biometrische Merkmale wie das Gesicht grundsätzlich öffentlich zugänglich sind. Anders wäre es nur, wenn der Berechtigte den Schutz eigenverantwortlich willentlich vollständig preisgibt. Einbezogen werden sollten über Mobiltelefone hinaus auch sonstige zugriffsgeschützte Datenträger. Denn in allen diesen Fällen liegt ein Eingriffsschwerpunkt auf der vorbereitenden Maßnahme der Entsperrung, die selbstschützende Vorkehrungen der Betroffenen untergräbt. Die Schutzbedürftigkeit von Zugangsdaten besteht in allen Fällen einheitlich. Wie bei § 100j StPO kommt als zusätzliche Voraussetzung hinzu, dass auch die anschließende Datenerhebung zulässig ist. Die Spezialregelung in den §§ 100a, 100b StPO bleibt unberührt.

Mit dieser Neuregelung wäre ein erster Schritt getan, um im System der Eingriffsbefugnisse den Technikbezug zu variieren und maßnahmenübergreifend stärker auf die Schutzbedürftigkeit und Schutzwürdigkeit von Informationen in konkreten Datenerhebungssituationen abzustellen.[164] Für dieses Regelungsmodell stehen beispielsweise § 160a StPO[165] und § 500 StPO i.V.m. §§ 48, 46 Nr. 14 BDSG. Eingewandt werden könnte, dass erhöhter Schutz für elektronische Systeme formuliert wird (oben V.), während Öffnung und Durchsuchung einer Wohnung den Ermittlungsbehörden ohne weitere Anlassschwelle Einblick in die gesamte Lebensführung einer Person eröffnen. Dieser Einwand übersieht aber, dass elektronische Systeme auch autonom Daten generieren, dass die Beherrschbarkeit für den Durchschnittsnutzer beschränkt ist und dass Art, Menge und Zeitraum der verfügbaren Daten eine qualifizierte Informationsdichte ergeben, die überdies maschinell verarbeitet werden kann. All das beeinflusst das Eingriffsgewicht.[166]

Die Neuregelung muss Nichtbeschuldigte einschließen. Das ermöglicht den Zugriff auf Mobiltelefone Toter. Es stellt sicher, dass Nichtbeschuldigte nicht allein qua Aussage- oder Herausgabepflicht (§§ 48 ff., 95 StPO) um den gebotenen Zugangsdatenschutz gebracht werden und andererseits nicht unter Berufung auf § 163b Abs. 2 S. 2 Hs. 2 StPO[167] verschont bleiben. Außerdem streitet die Unschuldsvermutung gegen das verbreitete Konzept, Eingriffsbefugnisse vorrangig gegen den Beschuldigten zu richten. In-Verdacht-Geraten ist kein zurechnungsbegründendes Verhalten, das eine verschärfte Inanspruchnahme rechtfertigen würde. Vielmehr obliegt es im Ausgangspunkt der Rechtsgemeinschaft, dem Beschuldigten eine Straftat nachzuweisen. Die konkrete Lastenverteilung richtet sich im Rahmen der Verhältnismäßigkeit nach den Ermittlungserfolgsaussichten. Höhere Ermittlungserfolgsaussichten können eine vorrangige Inanspruchnahme des Beschuldigten rechtfertigen. Doch Geräte nichtbeschuldigter Informationsträger (insbesondere Zeugen) müssen gleichermaßen herangezogen werden können, ebenso Geräte, die der Beschuldigte oder ein Informationsträger benutzt. Nach § 72 BDSG muss zwar zwischen Kategorien betroffener Personen, insbesondere Verdächtigen und Zeugen, unterschieden werden. Das gilt aber nur „so weit wie möglich", so dass die unschuldsvermutungskonforme Adressierung von Eingriffsbefugnissen Vorrang hat. Der EuGH betont zwar das Erfordernis, zwischen Kategorien betroffener Personen zu unterscheiden, versteht diese Unterscheidung aber letztlich als formale Notwendigkeit, die jeweils nötigen Voraussetzungen klar festzulegen.[168] Abhilfemöglichkeiten (Herausgabe der

[159] *F. Horn*, Kriminalistik 2019, 641 (643) m.w.N.
[160] *Rückert* (Fn. 6), S. 496, 770.
[161] *Ziemann*, ZStW 2018 (130), 762 (802).
[162] *Beling*, Die Beweisverbote als Grenzen der Wahrheitserforschung im Strafprozess, Nachdruck, 2. Aufl. 1968, S. 22 f., 294; *Eckstein* (Fn. 35), S. 162; *Eckstein* (Fn. 49), Vor §§ 100a–101 Rn. 31.
[163] Dazu z.B. *Grzesiek/Zühlke*, StV Spezial 2021, 117 (121 f.); *Nadeborn/Albrecht*, NZWiSt 2021, 420 (424); *Neuhaus*, StV 2020, 489 (491).
[164] *Eckstein* (Fn. 49), § 100a Rn. 34.
[165] Zur Kritik an dieser Vorschrift *Eckstein* (Fn. 49), § 100a Rn. 75 f. und § 100d Rn. 74 ff. m.w.N.
[166] *Eckstein* (Fn. 49), § 100a Rn. 34 m.w.N.
[167] Dafür *Wegner* (Fn. 44), S. 857 ff., 861.
[168] EuGH (Große Kammer), Urt. v. 4.10.2024 – C-548/21 = NVwZ 2025, 321 (325).

verfahrensrelevanten Daten durch den Betroffenen) haben aus Gründen der Verhältnismäßigkeit bei Beschuldigten wie Nichtbeschuldigten Vorrang.[169] Besondere schützende Vorkehrungen kommen zum Beispiel bei der Weiterverarbeitung von Daten in Betracht. Hinzugefügt werden sollte überdies eine Regelung zur unvermeidbaren Mitbetroffenheit Dritter. Rechtspolitisch soll dieses Plädoyer für weitergehende Inanspruchnahme Nichtbeschuldigter die Diskussion über generelle statt personellen Grenzen der Überwachung fördern.[170]

VII. Fazit

Der BGH lässt eine zwangsweise Entsperrung von Mobiltelefonen des Beschuldigten im Ausgangsfall zu. Doch die Befugnisnormen kumulierende Argumentation des BGH legt nolens volens offen, dass eine tragfähige Rechtsgrundlage fehlt. Die Entscheidung ist geprägt vom Bemühen, dem zu entscheidenden Fall gerecht zu werden.[171] Doch das Gesetz hält die gesuchte Lösung nicht bereit. Für eine Neuregelung sprechen sich, zur Klarstellung, auch einige Befürworter der Lösung des BGH aus.[172] Dieser Beitrag unterbreitet einen Regelungsvorschlag (oben V., VI.). Nach europarechtlichen Maßstäben ist die Neuregelung zwingend erforderlich. Das Europarecht wird so zum Motor für die Modernisierung der StPO. Solange es nicht gelingt, das Befugnisnormenkonzept der Strafprozessordnung sachgerecht zu modernisieren, bleibt es ein Spielfeld rabulistischer Gesetzesanwendung unter dem Druck praktischer Bedürfnisse. Der Wissenschaft muss das ein Ansporn sein, noch stärker zu versuchen, dem Gesetzgeber breit konsentierte Reformvorschläge zu unterbreiten.

[169] A.A. *Brodowski*, JZ 2024, 750 (752): Schonung Nichtbeschuldigter.
[170] Näher dazu *Eckstein* (Fn. 35), S. 307 ff., 359 ff.; *ders.* (Fn. 49), § 100a Rn. 20 m.w.N.
[171] Kritisch *Ferner*, beck-aktuell v. 23.5.2025, becklink 2034373: „Hard cases make bad law“.
[172] *Neuhaus*, StV 2020, 489 (492); *Rottmeier/Eckel*, NStZ 2020, 193 (200).