

Entscheidungsbesprechung

BGH, Beschl. v. 13.3.2025 – 2 StR 232/24 (LG Köln)¹

Zwangsentsperrung des Smartphones mittels Fingerabdrucks

Der Versuch der Ermittlungsbehörden, Zugang zu den auf einem Mobiltelefon eines Beschuldigten gespeicherten Daten durch zwangsweises Auflegen von dessen Finger auf den Fingerabdrucksensor zu erlangen, ist von § 81b Abs. 1 in Verbindung mit §§ 94 ff. StPO als Ermächtigungsgrundlage jedenfalls dann gedeckt, wenn eine zuvor nach §§ 102, 105 Abs. 1 StPO richterlich angeordnete Durchsuchung gerade auch dem Auffinden von Mobiltelefonen dient und der beabsichtigte Datenzugriff trotz seiner Eingriffsintensität verhältnismäßig ist.

(Amtlicher Leitsatz)

StPO §§ 81b, 94 ff.

Anton Jansen, Tübingen*

I. Einführung

Der Fall wirft die Frage auf, ob Strafverfolgungsbehörden berechtigt sind, ein sichergestelltes Mobiltelefon eines Beschuldigten gegen dessen Willen mittels eines Fingerabdrucks zu entsperren und die auf dem Gerät gespeicherten Daten auszuwerten.

Dabei stehen sich das staatliche Interesse an effektiver Strafverfolgung und der Schutz zentraler Beschuldigtenrechte gegenüber. Problematisch ist vor allem, dass die Strafprozessordnung keine ausdrücklich auf das Entsperren digitaler Endgeräte zugeschnittene Ermächtigungsgrundlage enthält. Es stellt sich daher die Frage, ob und in welchem Umfang bestehende Normen, insbesondere § 81b StPO sowie §§ 94 ff. StPO, auf moderne biometrische Entsperrmethoden übertragen werden können.

II. Sachverhalt

Der Angeklagte stand im Verdacht, gegen ein Berufsverbot verstoßen zu haben, das gegen ihn in einem anderen Verfahren verhängt worden war, weil er als Erzieher Nacktaufnahmen von ihm betreuten Kindern angefertigt hatte.

Im Zuge des Ermittlungsverfahrens wegen Verdachts einer Tat nach § 145c StGB, Verstoß gegen ein Berufsverbot, ordnete der Ermittlungsrichter auf Antrag der Staatsanwaltschaft gem. §§ 102, 105 Abs. 1 StPO die Durchsuchung der Wohnräume des Beschuldigten an. Diese sollte u.a. dem Auffinden von Mobiltelefonen dienen, da zu erwarten war, dass der Beschuldigte über diese weitere Betreuungsverhältnisse u.a. als Babysitter angebahnt hatte.

* Der Verf. ist Student der Rechtswissenschaft im siebten Semester an der Eberhard Karls Universität Tübingen. Der Beitrag entstand im Kurs „Publizieren in der Rechtswissenschaft“ unter Betreuung von Jun.-Prof. Dr. Jennifer Grafe, LL.M.

¹ Die Entscheidung ist veröffentlicht u.a. in BeckRS 2025, 9876.

Da der Beschuldigte sich weigerte, seine Mobiltelefone zu entsperren, ordnete ein Beamter bei der Durchsuchung an, den rechten Zeigefinger des Beschuldigten auf den Fingerabdrucksensor der zwei aufgefundenen Mobiltelefone zu legen.

Bei der anschließenden Auswertung der sichergestellten Geräte wurde kinderpornographisches Material gefunden, das zur späteren Verurteilung führte.

In der Hauptverhandlung widersprach der Verteidiger daher sowohl der Erhebung als auch der Verwertung dieser Beweise. Er machte geltend, dass für die Entsperrung der Mobiltelefone eine Rechtsgrundlage fehle und der Angeklagte dadurch in seiner Selbstbelastungsfreiheit sowie seinem Recht auf ein faires Verfahren und auf informationelle Selbstbestimmung verletzt worden sei.

III. Entscheidungsgründe

Der BGH entschied, dass die zwangsweise Entsperrung eines sichergestellten Smartphones mittels Fingerabdrucks des Beschuldigten zulässig ist und die Verfahrensrüge damit ohne Erfolg bleibt. Das Auflegen des Fingers stelle eine bloße Duldung körperlichen Zwangs dar und verletze weder die Selbstbelastungsfreiheit noch das Recht auf ein faires Verfahren.²

Als Rechtsgrundlage für die Entsperrung zog der *Senat* § 81b Abs. 1 StPO heran.³ Die Norm erfasse auch solche Maßnahmen, bei denen körperliche Merkmale zur Durchführung des Strafverfahrens genutzt würden.⁴ Der Fingerabdruck unterscheide sich dabei funktional nicht von klassischen erkennungsdienstlichen Maßnahmen, sodass die Maßnahme als „ähnliche Maßnahme“ i.S.d. § 81b Abs. 1 StPO anzusehen sei.⁵

Den Zugriff auf die nach der Entsperrung zugänglichen Daten ordnete der BGH §§ 94 ff., 110 StPO zu.⁶ Entsperrung und Datenauswertung seien rechtlich getrennte Maßnahmen.⁷ Verfassungsrechtliche Bedenken, insbesondere im Hinblick auf das Recht auf informationelle Selbstbestimmung, wies der *Senat* zurück.⁸

IV. Kritische Einordnung

1. Einordnung in die bisherige Rechtsprechung

Die Entscheidung des BGH steht nicht isoliert, sondern knüpft an eine bereits zuvor entwickelte Rechtsprechung an, die § 81b Abs. 1 StPO als Ermächtigungsgrundlage für das zwangsweise Entsperren mobiler Endgeräte heranzog.⁹ Uneinheitlich blieb jedoch die Beantwortung der Frage, ob und in welchem Umfang die Norm auch den Zugriff auf die auf dem Gerät gespeicherten Daten legitimieren kann.¹⁰

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

³ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 35.

⁴ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 40.

⁵ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 37.

⁶ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 44.

⁷ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 43.

⁸ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 46.

⁹ So AG Baden-Baden, Beschl. v. 13.11.2019 – 9 Gs 982/19; LG Baden-Baden, Beschl. v. 26.11.2019 – 2 Qs 147/19; LG Ravensburg, Beschl. v. 14.2.2023 – Qs 9/23 jug; OLG Bremen, Beschl. v. 8.1.2025 – 1 ORs 26/24.

¹⁰ AG Baden-Baden, Beschl. v. 13.11.2019 – 9 Gs 982/19 sieht § 81b StPO als „jedenfalls analog“ anwendbar, während OLG Bremen, Beschl. v. 8.1.2025 – 1 ORs 26/24 den Zugriff auf die gespeicherten Daten ausdrücklich auf §§ 94, 110 StPO stützt.

Neu ist daher nicht die grundsätzliche Zulässigkeit der Entsperrung, sondern die dogmatische Präzisierung des weiteren Vorgehens. In diesem Punkt stellt die Entscheidung eine Fortentwicklung der bisherigen Rechtsprechung dar, ohne deren Grundlinie zu verlassen.

2. Grundsätzliche Zulässigkeit der Datenerhebung von Endgeräten

Die Entsperrung mittels Fingerabdrucks als bloße Duldung körperlichen Zwangs einzuordnen, begegnet im Grundsatz keinen durchgreifenden Bedenken.¹¹ Gleichzeitig ist darauf hingewiesen, dass sich in der praktischen Anwendung einzelner Ermittlungsmaßnahmen zur Entsperrung mobiler Endgeräte Grenzbereiche ergeben können, in denen die Trennlinie zwischen zulässiger Mitwirkung und unzulässiger Selbstbelastung nicht stets eindeutig verläuft.¹²

Trotz der Möglichkeit praktischer Abgrenzungsschwierigkeiten ist dem BGH bis hierhin zuzustimmen.

3. Ermächtigungsgrundlage des § 81b StPO für die Entsperrung

a) Wortlaut

Die Literatur weist zurecht daraufhin, dass der Wortlaut nicht isoliert¹³, sondern stets im Zusammenhang mit dem Zweck der Norm zu verstehen ist.¹⁴ Zwar wird anerkannt, dass Ziel der Norm die Erfassung dauerhafter Persönlichkeitsgegebenheiten auch gegen den Willen des Beschuldigten sei, um diese mit vorhandenen Informationen abzugleichen und Rückschlüsse auf eine mögliche Täterschaft zu ziehen.¹⁵ Entscheidend präzisiert wird jedoch, dass sobald der Fingerabdruck nicht mehr zur Identifizierung, sondern allein zur Entsperrung genutzt wird, dies die Norm entfremde.¹⁶ Eine Betrachtung, die allein auf das äußerliche Erscheinungsbild des Fingerauflegens abstellt, bliebe damit an der Oberfläche stehen und verkennte, dass für die Einordnung als „ähnliche Maßnahme“ nicht die äußere Form, sondern der zugrunde liegende Zweck maßgeblich ist.¹⁷

Hier hat die Kritik an der Wortlautauslegung des BGH anzusetzen. Zwar ist richtig, dass das Auflegen des Fingers auf den Entsperrungssensor eine erkennungsdienstliche Maßnahme darstellen kann, die Entscheidung verfehlt jedoch, das Kriterium der „Ähnlichkeit“ nicht lediglich auf das äußere Erscheinungsbild zu beschränken. Es wird nicht berücksichtigt, ob auch der Zweck der Maßnahme dem erkennungsdienstlichen Charakter entspricht. Die Norm ist jedoch so auszulegen, dass „ähnlich“ sowohl die äußere Form als auch den funktionalen Zweck erfassen muss.

¹¹ Rottmeier/Eckel, NStZ 2020, 193 (199); Nadelborn/Irscheid, StraFo 2019, 274 (275).

¹² Zweifel an der Übertragbarkeit der Maßnahme auf die Face-ID und dem damit verbundenen gewaltsamen Aufsperrern der Augen Ziegler, jurisPR-ITR 17/2025 Anm. 3; weitergehende Zweifel Satzger/Sarfratz, NStZ 2025, 560 (566).

¹³ Wobei selbst bei einer isolierten Betrachtung nach Satzbau und Wortstellung der Begriff „ähnliche Maßnahme“ sich auf den Begriff der Messung bezieht, so Rogall, in: SK-StPO, Bd. 1, 5. Aufl. 2018, § 81b Rn. 44.

¹⁴ Satzger/Sarfratz, NStZ 2025, 560 (566); a.A. Krause, in: Löwe/Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 2, 28. Aufl. 2025, § 81b Rn. 16.

¹⁵ Nadelborn/Albrecht, NZWiSt 2021, 420 (423).

¹⁶ Bosch, in: SSW-StPO, 6. Aufl. 2025, § 81b Rn. 7.

¹⁷ Horter, NStZ 2023, 447 (448); a.A. Güntge, JR 2025, 504 (517).

b) Sinn und Zweck

Auch hinsichtlich der teleologischen Auslegung des § 81b StPO gibt es Kritik¹⁸ an der Auffassung des BGH. Es wird richtigerweise darauf hingewiesen, dass § 81b StPO unter der amtlichen Überschrift „Erkennungsdienstliche Maßnahmen bei dem Beschuldigten“ geführt wird und damit lediglich eine Identitätsfeststellungsfunktion hat.¹⁹ Zusätzlich wird insbesondere der Rückgriff auf den „Zweck der Durchführung des Strafverfahrens“ kritisiert, da dieser § 81b StPO zu einer undenkbar weitreichenden Ermittlungsgeneralklausel hochstilisiere.²⁰ Dem ist zuzustimmen: § 81b StPO ist nicht allgemein auf die Förderung des Strafverfahrens gerichtet, sondern funktional auf erkennungsdienstliche Zwecke begrenzt. Diese Zweckbindung verliert der *Senat* aus dem Blick, wenn er den Normzweck im Wesentlichen auf effektive Strafverfolgung überträgt.

Dadurch wird das Merkmal der Erkennungsdienstlichkeit inhaltlich entleert, da § 81b StPO zwar nicht selbst den Datenzugriff legitimiert, jedoch funktional als Brücke zu §§ 94 ff. StPO eingesetzt wird. Eine Norm, die ihrem Zweck nach auf Identitätsfeststellung zugeschnitten ist, wird damit mittelbar zur Voraussetzung für inhaltsbezogene Ermittlungsmaßnahmen.

Diese Entleerung zeigt sich besonders darin, dass der BGH seine eigene Rechtsprechung aus dem Jahr 1986, wonach § 81b StPO auf identifizierende Maßnahmen zur Feststellung der körperlichen Beschaffenheit begrenzt ist,²¹ nicht aufgreift und den daraus resultierenden Wertungswiderspruch nicht einmal thematisiert. Gerade dieser Bruch mit der eigenen Linie hätte einer ausdrücklichen Auseinandersetzung bedurft.

c) Technologieoffenheit

Die vom BGH postulierte Technologieoffenheit des § 81b StPO ist differenziert zu betrachten. Häufig wird argumentiert, dass die Norm auch bei Erlass noch nicht absehbare Ermittlungsformen erfassen müsse und dass die vorliegende Maßnahme darunter falle.²² Dabei übersieht man jedoch, dass die Überzeugungskraft dieses Arguments bei der konkreten Maßnahme deutlich schwindet.²³ Für die Identifikation des Beschuldigten macht es keinen Unterschied, ob ein Fingerabdruck analog (z.B. auf Papier) oder digital (z.B. über einen Scanner) erhoben wird, der Zweck bleibt stets die Feststellung der körperlichen Beschaffenheit.²⁴ Wird der Fingerabdruck hingegen genutzt, um Zugriff auf ein Smartphone zu erlangen, verlässt die Maßnahme diesen erkennungsdienstlichen Rahmen und betritt grundrechtlich besonders sensibles Terrain.²⁵

Somit ist der BGH auch in diesem Punkt zu ungenau. Er nutzt die Technologieoffenheit lediglich, um seine Argumentation zu stützen. Er übersieht dabei jedoch, dass sie keineswegs uneingeschränkt gilt, sondern stets im Rahmen des erkennungsdienstlichen Charakters der Norm zu beachten ist, wodurch eine dogmatische Verwendung als unbegrenztes Argument nicht haltbar ist.

¹⁸ Mosbach, JuS 2025, 742 (743); Horter, NSTZ 2023, 447 (448); Ruppert, StV 2025, 565 (566).

¹⁹ El-Ghazi/Imsameh, NSW 2025, 333 (342).

²⁰ Ruppert, StV 2025, 565 (566); a.A. Rottmeier/Eckel, NSTZ 2020, 193 (195); Goers, in: BeckOK StPO, Stand: 1.10.2025, § 81b Rn. 4.1.

²¹ BGH, Beschl. v. 9.4.1986 – 3 StR 551/85.

²² Trück, JZ 2025, 971 (973).

²³ Luh/Grosmann, ZD 2025, 453 (458).

²⁴ Satzger/Sarfraz, NSTZ 2025, 560 (566).

²⁵ Satzger/Sarfraz, NSTZ 2025, 560 (566).

4. Auswertung der Daten nach §§ 94 ff. StPO

Das Zwei-Stufen-Modell²⁶, das der BGH wählt, um die Rechtmäßigkeit der Maßnahme zu bejahen, wird dahingehend kritisiert, dass darin eine unnatürliche Aufspaltung eines tatsächlich einheitlichen Vorgangs liege.²⁷ Zur Begründung wird angeführt, dass durch die Kombination ein Eingriff in das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ermöglicht werde.²⁸ Dieser Eingriff reiche jedoch weiter als die Summe der dafür benutzten Bausteine (=die verwendeten Ermächtigungsgrundlagen).²⁹ Zudem komme damit der körperlichen Beschaffenheit des Beschuldigten in dieser Konstellation keine eigenständige Beweisbedeutung zu, sondern lediglich den auf dem Endgerät befindlichen Daten.³⁰

Diese Kritik überzeugt. Zwar ist die Trennung zwischen dem grundsätzlichen Zugriff auf ein technisches System und der anschließenden Auslese bzw. Auswertung der erlangten Daten dem Strafprozessrecht nicht fremd und findet sich etwa im Bereich der Telekommunikationsüberwachung wieder. Im Kontext der zwangsweisen physischen Smartphone-Entsperrung vermag diese dogmatische Konstruktion jedoch nicht zu überzeugen.

Das Zwei-Stufen-Modell löst sich zu stark vom tatsächlichen Lebenssachverhalt. In der Praxis bilden beide Schritte einen einheitlichen und untrennbaren Grundrechtseingriff, der unabhängig von einer zeitlichen oder räumlichen Trennung bereits mit der Entsperrung wirksam wird. Die normative Trennung verschleiert daher, dass erst die Kombination beider Schritte den schwerwiegenden Eingriff in die digitale Privatsphäre des Beschuldigten ermöglicht. Gerade diese kumulative Eingriffsintensität lässt die Konstruktion als formalistisch und realitätsfern erscheinen und verdeutlicht die Diskrepanz zwischen dogmatischer Logik und tatsächlicher Lebenswirklichkeit.

5. Die verfassungsrechtliche Situation

a) Grundrechte

Der BGH konzentriert sich bei seinen grundrechtlichen Ausführungen lediglich auf das Recht auf informationelle Selbstbestimmung.³¹ Das vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitete IT-System-Grundrecht³² findet dabei keine Erwähnung.

Vereinzelte wird es damit gerechtfertigt, dass dieses das Recht auf informationelle Selbstbestimmung nicht verdränge, da es bei der Entschlüsselung und Auswertung eines Endgeräts nicht um die Integrität des informationstechnischen Systems, sondern um die Sichtung und Erhebung der darauf befindlichen Daten gehe.³³ Diese Ansicht greift zu kurz, da sie bereits eine Schutzbereichseröffnung des IT-System-Grundrechts ablehnt.

Das Bundesverfassungsgericht stellt bei der Schutzbereichsbestimmung ausdrücklich darauf ab, dass das IT-System-Grundrecht „insbesondere vor einem heimlichen Zugriff“ schützt.³⁴ Der Begriff

²⁶ Krause, in: Löwe/Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 2, 28. Aufl. 2025, § 81b Rn. 16.

²⁷ Pschorr, jurisPR-StrafR 13/2025 Anm. 1; Ziegler, jurisPR-ITR 17/2025 Anm. 3.

²⁸ Nadeborn/Oberholz, HRRS 2025, 297 (299).

²⁹ Nadeborn/Albrecht, NZWiSt 2021, 420 (421 ff.).

³⁰ Ruppert, StV 2025, 565.

³¹ BGH, Beschl. v. 13.3.2025 – 2 StR 232/24, Rn. 46; so auch Neuhaus, StV 2020, 489 (491).

³² BVerfG, Beschl. v. 27.2.2008 – 1 BvR 370/07, Rn. 302 ff.

³³ Brodowski, JZ 2024, 750 (753); a.A. El-Ghazi/Imsameh, NSW 2025, 333 (344 ff.).

³⁴ BVerfG, Beschl. v. 27.2.2008 – 1 BvR 370/07, Rn. 205.

„insbesondere“ ist so zu verstehen, dass auch offene Zugriffe auf informationstechnische Systeme vom Schutzbereich erfasst sind.³⁵

Daraus folgt, dass die zwangsweise Entsperrung und anschließende Auswertung eines Smartphones, unabhängig davon, ob der Zugriff heimlich oder offen erfolgt, einen Eingriff in das IT-System-Grundrecht darstellen kann. Ob dieser Eingriff im konkreten Einzelfall gerechtfertigt ist, muss fallbezogen geprüft werden. Den Schutzbereich des Grundrechts jedoch überhaupt nicht zu thematisieren, wie es der BGH getan hat, lässt sich nicht rechtfertigen.

b) Einzelfallprüfung

Daran anschließend zeigt sich die problematischste Schwäche des Urteils in der Einzelfallbewertung des BGH und den damit eröffneten Konsequenzen.

Bereits bei einem bloßen Verdacht nach § 145c StGB, einem Delikt mit einer Höchststrafe von einem Jahr, erlaubte die Auslegung des BGH die zwangsweise Entsperrung des Smartphones und die vollständige Auslese der darauf befindlichen Daten. Dass zufällig kinderpornographisches Material entdeckt wurde, mag auf den ersten Blick ein zufriedenstellendes Ergebnis sein, offenbart jedoch auf den zweiten Blick das Risiko einer erheblichen Ausweitung der Ermittlungsbefugnisse. Auch bei geringfügigen Delikten würde so der Zugriff auf die gesamte digitale Lebenssphäre eröffnet.

Dies wirft rechtsstaatliche Bedenken auf, insbesondere im Hinblick auf intime Bilddaten, private Kommunikation oder medizinische Informationen, die typischerweise auf Smartphones gespeichert sind. Dass solche Daten ohne spezifische gesetzliche Grundlage allein über eine weit ausgelegte erkennungsdienstliche Maßnahme zugänglich werden, überzeugt nicht. Selbst eine Verhältnismäßigkeitsprüfung bietet hier keinen hinreichenden Schutz, wie der vorliegende, entschiedene Fall zeigt.

V. Fazit

Der BGH hat sich erkennbar um einen Ausgleich zwischen Ermittlungsinteressen und Grundrechtsschutz bemüht, diesen aber nur teilweise erreicht. Die Entscheidung ist funktional nachvollziehbar und reagiert auf praktische Herausforderungen digitaler Beweismittel, führt allerdings zu einer bedenklichen Ausweitung des § 81b Abs. 1 StPO über die Grenzen seines Wortlauts und seines Zwecks hinaus. Die Zwangsentperrung von Mobiltelefonen erfordert eine klar konturierte gesetzliche Grundlage³⁶, die (moderne) Grundrechte, das Unionsrecht³⁷ und die Besonderheiten biometrischer Verfahren wie Fingerabdruck, Face-ID oder Iris-Scan berücksichtigt. Die Gesetzgebung sollte daher eine technologieoffene, grund- und unionsrechtskonforme Lösung schaffen, die Eingriffsintensität und Verhältnismäßigkeit angemessen balanciert, ohne einen starren Katalog³⁸ zu etablieren.

³⁵ Jahn, JuS 2025, 791 (792).

³⁶ So auch die Literatur, auf die sich der BGH stützt Bäumerich, NJW 2017, 2718 (2722); Rottmeier/Eckel, NSTZ 2020, 193 (200).

³⁷ Dazu Hamed, StraFo 2025, 275 (279); Güntge, JR 2025, 504 (514 f.).

³⁸ Ein überzeugendes Argument zugunsten der BGH-Entscheidung, das bemerkenswerterweise nur Trück, JZ 2025, 971 (979), anführt, ist, dass sie eine an §§ 100a ff. StPO orientierte Kataloggesetzgebung vermeide. Zwar ist die Katalogtechnik verfassungsrechtlich anerkannt, sie erfasst jedoch nicht immer die für digitale Zugriffe relevanten Rechtsgüter und die Eingriffsintensität hängt hier primär vom Umfang des Datenzugriffs ab, nicht allein vom Deliktstyp. Vgl. hierzu Trück, JZ 2025, 971 (977 ff.).