# Look into the camera! Strafprozessuale, verfassungsrechtliche und methodisch-strukturelle Probleme im Zusammenhang mit biometrisch gesicherten Beweismitteln, insbesondere Smartphones

Nina Schrott, München*

**ABSTRACT**

Ob biometrisch gesicherte Smartphones ermittlungsbehördlich entschlüsselt und ausgelesen werden dürfen, ist nach wie vor heftig umstritten. Der Beitrag diskutiert, ob derartige Eingriffe gegen den Grundsatz der Selbstbelastungsfreiheit verstoßen, und unterzieht die in Rechtsprechung und Literatur aufgerufenen Ermächtigungsgrundlagen einer kritischen Prüfung. Dabei wird deutlich, dass v.a. die zugrunde gelegten methodisch-strukturellen Zugänge nicht selten auf dogmatisch tönernen Füßen stehen.

## A. Der Zugriff auf das Smartphone als das, „was dem *Zugriff auf die menschliche Seele* am nächsten kommt“[1]

Mobile Endgeräte wie Laptops, Smartphones, Tablets und Wearables sind inzwischen allgegenwärtig und bestimmen unseren beruflichen wie privaten Alltag. Sie fungieren u.a. als Telekommunikations- und Nachrichteninstrument, Kamera und Fotoalbum, als Kalender, Notizbuch, Arbeitsmittel, Spielkonsole, Datingtool, Fitnesstracker und Navigationsgerät – und sind aufgrund ihrer handlichen Größe (fast) immer mit dabei.

* Die Verfasserin ist Akademische Rätin a.Z. am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtssoziologie von Prof. Dr. *Armin Engländer* an der Ludwig-Maximilians-Universität München.

[1] *Greco* StV 2024, 276, 279, Hervorheb. im Original.



https://doi.org/10.61039/29427509-2024-22

Das gilt insbesondere für Smartphones, aus deren gespeicherten Datensätzen sich ganze Persönlichkeitsprofile erstellen lassen.[2] Um dieses „ultimative[ ] Beweismittel“[3] vor dem Zugriff Dritter zu schützen, sind inzwischen die allermeisten mobilen Endgeräte mit biometrischen Sicherungsmechanismen wie Fingerabdruckscan, Gesichts- und Iriserkennung versehen.[4] Diese Verschlüsselungsmaßnahmen treten dabei neben die klassische PIN-Eingabe und sollen einen gleichermaßen bequemen wie sicheren Zugriff auf das Gerät ermöglichen. Die technischen Hintergründe sind einigermaßen komplex und hängen von den jeweils verwendeten biometrischen Verschlüsselungstechniken ab. Sie eint, dass sie auf individuelle körperliche Merkmale wie Fingerabdruck, Gesicht, Iris oder Venenbild des Nutzers abstellen und bei Übereinstimmung mit den gespeicherten Merkmalen das Gerät freigeben.[5]

Ob Ermittlungsbehörden biometrisch gesicherte Mobilfunkendgeräte entschlüsseln und anschließend auf die gespeicherten Daten zugreifen dürfen, darüber wird in Rechtsprechung und Literatur nach wie vor heftig gestritten. Bemerkenswert ist dabei nicht nur die Vielzahl und Unterschiedlichkeit der beigezogenen Befugnisnormen – jedenfalls thematisiert werden u.a. (ggf. in analoger Anwendung) §§ 81a, 81b, 94, 100a, 100b, 102, 110 III StPO sowie die §§ 160, 161 StPO –, sondern auch die verschiedenen methodischen Zugänge, die die Autorinnen und Autoren wählen, um Entschlüsselung und Datenzugriff zu (de-)legitimieren. Eine lediglich untergeordnete Rolle in der Diskussion spielt hingegen der Nemo-tenetur-Grundsatz.

Der vorliegende Beitrag möchte daher zunächst einen vertieften Blick auf etwaige Friktionen hinsichtlich des Grundsatzes der Selbstbelastungsfreiheit bei zwangsweiser Smartphone-Entschlüsselung werfen (unter B.), bevor er sowohl die diskutierten Ermächtigungsgrundlagen als auch insbesondere die – oftmals weitgehend begründungslos – gewählten methodisch-strukturellen Herangehensweisen einer kritischen Prüfung unterzieht (unter C.). Der Text endet mit einem kurzen Fazit sowie einem Appell an den Gesetzgeber (unter D.).

---

[2] Zum Ganzen *Ludewig* KriPoZ 2019, 293; *Greco* StV 2024, 276, 276; *Stam* JZ 2023, 1070, 1071; vgl. auch BVerfGE 115, 166, 190, 192 ff. Daneben kann über das Smartphone i.d.R. auch auf Online- bzw. Clouddienste zugegriffen werden.

[3] *Grzesiek/Zühlke* StV-S 2021, 117, 122.

[4] Vgl. https://de.statista.com/infografik/11117/weltweiter-absatz-anteil-von-geraeten-mit-biometrischen-technologien/ [5.7.2024].

[5] Zu den technischen Hintergründen *Bäumerich* NJW 2017, 2718, 2718 f.; *Horn*, Biometrische Sicherungen, 2020, 6 ff.

## B. Zwangsweise Entschlüsselung bei Freiheit zur Selbstbelastung?

### I. Zwischen aktiver Duldung und passiver Mitwirkung

Da die Selbstbelastungsfreiheit grundsätzlich vor jeder Form aktiver Mitwirkung schützt, darf ein Beschuldigter unstreitig nicht dazu gezwungen bzw. durch Täuschung oder List dazu gebracht werden, seinen PIN-Code an die Ermittlungsbehörden herauszugeben.[6] Soll dennoch auf das Beweismittel „(verschlüsseltes) Smartphone" zurückgegriffen werden, bleibt entweder ein zeit- und kostenintensiver Brute-Force-Einsatz[7] oder bei einem biometrisch gesicherten Smartphone die zwangsweise Entschlüsselung u.a. mittels Fingerauflegens bzw. Kopf- und Liderfixierung beim Beschuldigten.[8] Verträgt sich ein solcher Einsatz von Zwang(smitteln) aber mit der verfassungsrechtlich garantierten Freiheit zur Selbstbelastung?

Literatur und Rechtsprechung belassen es in diesem Zusammenhang zumeist bei der knappen, einigermaßen lapidaren Feststellung, der Nemo-tenetur-Grundsatz sei hier mangels des Erfordernisses aktiver Mitwirkung bzw. Willensbildung – der Finger könne auch ohne Beschuldigtenbeteiligung auf dem Scanner platziert, Kopf und Lider auch ohne dessen Mitwirkung fixiert werden – nicht betroffen.[9] Tatsächlich wird die Grenze des Zulässigen ganz überwiegend entlang der dichotomen Demarkationslinie von erlaubtem Zwang zu *passiver* Duldung – dann kein Verstoß gegen die Selbstbelastungsfreiheit – und dem wegen eines Verstoßes gegen den Nemo-tenetur-Grundsatz verbotenen Zwang zur *aktiven* Mitwirkung gezogen.[10]

Doch selbst bei Anwendung dieses (vermeintlich) klaren Unterscheidungskriteriums – zur Kritik hieran sogleich – unterfällt die Entschlüsselung biometrisch gesicherter Smartphones nur zum Teil von vornherein *nicht* dem geschützten Anwendungsbereich der Selbst-

---

[6] H.M., im hiesigen Kontext *Momsen* DRiZ 2018, 140, 141; *Nadeborn/Irscheid* StraFo 2019, 274, 275.

[7] Brute-Force-Methode („rohe Gewalt") = Erraten von Anmeldeinformationen / Verschlüsselungscodes durch reines Ausprobieren; dazu *Horn*, Biometrische Sicherungen, 2020, 14 f.

[8] Sofern jedenfalls die max. Anzahl biometrischer Entsperrungen vor PIN-Eingabe noch nicht überschritten wurde.

[9] So z.B. *Momsen* DRiZ 2018, 140, 141: Nemo-tenetur-Grundsatz „strukturell nicht betroffen"; ähnlich knapp *Bäumerich* NJW 2017, 2718, 2721; *Nadeborn/Irscheid* StraFo 2019, 274, 275; etwas ausführlicher *Braun/Hummels* PSP 2018, 3, 4; *Rottmeier/Eckel* NStZ 2020, 193, 195; s. auch *Nicolai* StV-S 2023, 148; *Rückert*, in Münchener Kommentar StPO, Bd. 1, 2. Aufl. 2023, § 100b Rn. 42; i.T. anders *Neuhaus* StV 2020, 489, 491.

[10] H.M. und st.Rspr., BVerfGE 56, 42; BGHSt 24, 125, 129; 34, 39, 45 f.; 42, 139, 152; *Schuhr*, in Münchener Kommentar StPO, Bd. 1, 2. Aufl. 2023, Vor § 133 Rn. 91 f. m.w.N.

belastungsfreiheit: So mag zwar das erzwungene Strecken bzw. Auflegen des Fingers auf den Fingerabdrucksensor durch die Ermittlungspersonen für den Betroffenen tatsächlich lediglich eine passive Duldungshandlung darstellen und folglich nicht vom Verbot aktiver Selbstbelastung erfasst sein.[11] Anders kann sich die Sachlage hingegen bei einem mittels Gesichts- bzw. Iriserkennung gesicherten mobilen Endgerät darstellen: Denn insbesondere bei neueren Smartphones funktioniert die Freischaltung oftmals nur dann, wenn die (berechtigte) Person direkten Blickkontakt mit der Kamera aufnimmt, mithin darf sie den Blick jedenfalls nicht aktiv (weit) nach links, rechts, oben oder unten abwenden („aktiv wegschauen").[12] Da es insofern auf die Ausrichtung der Iris ankommt, kann eine Fixierung von Kopf und Lidern eine solche aktive Abkehr- bzw. Abwehrhaltung kaum verhindern.

Damit ist aber jedenfalls in diesen Fällen dahingehend eine aktive, nicht durch äußerlichen Zwang zu erwirkende Mitwirkungshandlung erforderlich, als dass der eigene Blick bewusst auf die Kamera des Smartphones gerichtet werden muss. Zöge man sich nun auf eine streng formalistisch-dichotome Position zurück, ließe sich in dieser Notwendigkeit durchaus ein Element erforderlicher aktiver Mitwirkung erkennen mit der Folge, dass über die fehlende Pflicht zum In-die-Kamera-Schauen vorab belehrt werden müsste und Beweisergebnisse, die unter Verstoß gegen diese Pflicht bzw. durch Täuschung oder List – z.B. durch plötzliches „Einfangen" des Blicks – erlangt worden wären, nicht verwertet werden dürften.

## II. Zum Schutzbereich der Selbstbelastungsfreiheit

Das vorstehende Beispiel macht damit zugleich deutlich, dass eine derart strenge Entgegensetzung von aktiver Mitwirkung und passiver Duldung bisweilen zu einigermaßen zufälligen, wenig sachgerechten Ergebnissen führt:[13] Nicht nur hinge die Zulässigkeit der Maßnahme maßgeblich von der spezifischen technischen Ausgestaltung der einzelnen biometrischen Sicherung ab. Vielmehr würde auch der bloße Umstand, dass sich gewisse – wenige – körperliche Mitwirkungshandlungen im Gegensatz zu den allermeisten anderen weder durch aktiven Zwang noch durch

[11] S. hierzu bereits Fn. 9.

[12] Exemplarisch bzgl. Face-ID von Apple https://de.wikipedia.org/wiki/Face_ID [5.7.2024]. Gedruckte oder digitale zweidimensionale Fotos sind ebenfalls nicht geeignet, die Sicherung zu überwinden, ausführlich https://support.apple.com/de-de/102381 [5.7.2024].

[13] Ähnlich *Kasiske* JuS 2014, 15, 18; *Verrel* NStZ 1997, 415, 417.

bloßes Zuwarten „erzwingen“ lassen,[14] zum maßgeblichen Unterscheidungsfaktor, obwohl sich die einzelnen Handlungen angesichts ihres lediglich „körperlichen“ Persönlichkeitsbezugs in qualitativer Hinsicht kaum voneinander unterscheiden.

Auch wegen derartiger Unstimmigkeiten wird vielfach eine Einschränkung des Anwendungsbereichs des Nemo-tenetur-Grundsatzes gefordert: So plädieren Teile der Literatur für eine strenge Begrenzung der Selbstbelastungsfreiheit auf den kommunikativen Bereich, mithin auf verbale, gestische oder auch verschriftlichte *Aussagen*.[15] Der EGMR wiederum unterscheidet primär danach, ob ein Beweismittel unabhängig vom Willen des Beschuldigten existiert (dann grundsätzlich kein Verstoß gegen Nemo-tenetur, auch wenn das Beweismittel nur unter dessen aktiver Mitwirkung erlangt werden kann) oder aber in seiner Existenz willensabhängig ausgestaltet ist.[16] Der aktive Blick als non-kommunikativer „Beweismittel-Schlüssel“ unterfiele damit ebenso wenig wie die grundsätzlich willensunabhängig existierenden Smartphonedaten dem Schutzbereich der Selbstbelastungsfreiheit.

Möchte man soweit nicht gehen, so streitet jedenfalls die verfassungsrechtliche Verankerung des Nemo-tenetur-Grundsatzes u.a. in der Menschenwürdegarantie des Art. 1 I GG, im Recht auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG) sowie als Element eines fairen Verfahrens (vgl. Art. 6 EMRK)[17] für eine gewisse (Selbst-)Beschränkung: Danach sollte der Schutz der Selbstbelastungsfreiheit neben dem Schweigerecht zumindest nicht jede beliebige aktive Mitwirkungshandlung erfassen, sondern lediglich solche, die einen unmittelbaren Bezug zur Persönlichkeit des Beschuldigten aufweisen, sodass sich seine Mitwirkung nach außen „als eine Unterwerfung der Person unter das Verfahren darstellt“[18]. Andernfalls drohte eine weitgehend „grundrechtsimmunisierte“, in ihrer spezifischen Ausprägung bisweilen zufällige – und damit im Ergebnis kaum überzeugend begründbare – Ausweitung des Schutzbereichs der Selbstbelastungsfreiheit.

---

[14] So z.B. beim Ausscheiden verschluckter Beweismittel.

[15] *Verrel* NStZ 1997, 415, 417 ff.; *Böse*, GA 2002, 98, 128; *Ransiek/Winsel* GA 2015, 620, 635; nur auf Aussagen i.R. förmlicher Vernehmungen beschränkend *Lesch* ZStW 111 (1999), 624, 638.

[16] EGMR NJW 2006, 3117, 3124 – Brechmitteleinsatz.

[17] Daneben wird z.T. auch auf das Rechtsstaatsprinzip abgestellt. Zur i.E. umstr. verfassungsrechtlichen Herleitung *Kasiske* JuS 2014, 15, 15 ff.; *Ransiek/Winsel* GA 2015, 620, 621 f.; diesbzgl. kritisch *Verrel* NStZ 1997, 361, 364; zu den verschiedenen Begründungsmodellen s. auch *Teixeira* ZStW 135 (2023), 253, 260 ff.

[18] *Kasiske* JuS 2014, 15, 18 u.V.a. *Böse*, GA 2002, 98, 128; für eine prozessuale Fundierung des Nemo-tenetur-Grundsatzes *C. Dannecker* 127 (2015), 991, 992.

Der Nemo-tenetur-Grundsatz ist daher auf seinen persönlichkeitsbezogenen Kernbereich zu beschränken. Derart begrenzt unterfällt das aktive In-die-Kamera-Schauen dann aber bereits nicht dem Anwendungsbereich der Selbstbelastungsfreiheit, da der bloße Blick in die Kamera als körperliche „Normalfunktion" weder einen unmittelbaren Persönlichkeitsbezug aufweist noch eine Verfahrensunterwerfung des Beschuldigten bedeutet. Nemo-tenetur ist insofern nicht betroffen. Anders müssten dies freilich Teile der Literatur und die Rechtsprechung beurteilen – jedenfalls sofern sie schutzbereichsbezogen schlichtweg auf die klassische Unterscheidung zwischen passiver Duldung und aktiver Mitwirkung verweisen.

## C. Methodisches Potpourri und eine Vielzahl von Ermächtigungsgrundlagen

### I. Erfordernis einer Befugnisnorm und strukturelle Ausgangsüberlegungen

Dass der Grundsatz der Selbstbelastungsfreiheit einer Entschlüsselung biometrisch gesicherter Smartphones grundsätzlich nicht entgegensteht, sagt selbstredend noch nichts über die Zulässigkeit dieser Maßnahme aus. Da mit Beschlagnahme, Entsperrung und anschließendem Datenzugriff sowohl Art. 10 GG[19], Art. 14 GG sowie bei Fixierungen ggf. Art. 2 II 1 GG als auch insbesondere das aus dem Allgemeinen Persönlichkeitsrecht abgeleitete Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (sog. „IT-Grundrecht")[20] sowie das Recht auf informationelle Selbstbestimmung betroffen sein können,[21] bedarf der Eingriff einer gesetzlich normierten Ermächtigungsgrundlage. Das gebietet bereits der verfassungsrechtliche Grundsatz des Vorbehalts des Gesetzes (vgl. Art. 20 III GG).[22]

Eine ausdrückliche Befugnisnorm enthält die StPO lediglich in Bezug auf den in aller Regel vorgelagerten Schritt der Beschlagnahme des mobilen

[19] Sofern der Kommunikationsvorgang noch nicht abgeschlossen ist, vgl. BVerfGE 115, 166, 183, 187; 124, 43; *Neuhaus* StV 2020, 489, 489; anders *Horn*, Biometrische Sicherungen, 2020, 23 f.

[20] *Momsen* DRiZ 2018, 140, 143; *Bäumerich* NJW 2017, 2718, 2722; *Stam* JZ 2023, 1070, 1071 f. m.w.N.; a.A. *Horn*, Biometrische Sicherungen, 2020, 24 ff.

[21] Ausführlich zu den betroffenen Rechtspositionen des Beschuldigten *Stam* JZ 2023, 1070, 1071 f.; *Horn*, Biometrische Sicherungen, 2020, 23 ff.; s. auch *Greco* StV 2024, 276, 279.

[22] H.M., s. nur BVerfGE 40, 237; 49, 89; ausführlich *Ziemann* ZStW 130 (2018), 762, 765 f. mit umf. N. in Fn. 16.

Endgeräts „Smartphone“ als Gegenstand i.S.d. § 94 I StPO.[23] Dagegen finden sich hinsichtlich der Entschlüsselung und / oder des sich anschließenden Zugriffs auf die auf dem Smartphone gespeicherten Daten keine strafprozessualen Regelungen, die *spezifisch* auf das beschriebene Maßnahmenbündel „zugeschnitten“ sind.

Die zunächst lediglich chronologische Zweistufigkeit des Eingriffsvorgangs aus Entschlüsselung (1. Stufe) und Zugriff auf die entschlüsselten Daten (2. Stufe) wird in Rechtsprechung und Schrifttum auch in methodischer Hinsicht vielfach aufgegriffen und unterschiedlich verarbeitet. Grob haben sich hierbei drei (bzw. vier) Herangehensweisen herausgebildet, die im Folgenden sowohl auf ihre dogmatische Tragfähigkeit wie auch ihre Einschlägigkeit im konkreten Einzelfall hin untersucht werden sollen.

Zu unterscheiden sind: 1. Sukzessiv-additive Lösungen (unter II.), 2. Inzidentlösungen (unter III.), 3. Annexlösungen (unter IV.) sowie 4. Kombinationen aus den vorstehenden Ansätzen (unter V.).

## II. Sukzessiv-additive Lösungen („Baukastenprinzip“)

Im Rahmen von sukzessiv-additiven Lösungen – von *Nadeborn/Albrecht* anschaulich als „Baukastenprinzip“[24] bezeichnet – werden die benannten Stufen aus Entschlüsselung und Datenzugriff weitgehend isoliert voneinander betrachtet und grundsätzlich eigenständig auf (eine) jeweils taugliche Rechtsgrundlage(n) hin untersucht. Dabei sollen durch die Kombination verschiedener bestehender Befugnisnormen die sukzessiv abfolgenden Einzelmaßnahmen zunächst für sich genommen legitimiert werden – mit dem Ergebnis einer Rechtfertigung des Gesamteingriffs.[25]

So gehen beispielsweise *Rottmeier/Eckel* ausdrücklich von einer „zweistufige[n] Struktur“ des Geschehens aus, bestehend aus 1. der Datenentsperrung und – als „eigentliche[s] Ziel der Maßnahme“ – 2. dem Zugriff auf die so entschlüsselten Daten.[26] Dabei seien „beide Stufen prinzipiell zu trennen und die mit ihnen jeweils verbundenen Grundrechtseingriffe einer Rechtfertigung durch gesonderte Rechtsgrundlagen zugänglich“[27].

---

[23] I.E. ebenso *Momsen* DRiZ 2018, 140, 142.

[24] *Nadeborn/Albrecht* NZWiSt 2021, 420.

[25] Vgl. *Nadeborn/Albrecht* NZWiSt 2021, 420.

[26] *Rottmeier/Eckel* NStZ 2020, 193, 195.

[27] *Rottmeier/Eckel* NStZ 2020, 193, 195. Gleichwohl soll i.R.d. Verhältnismäßigkeitsprüfung der 1. Stufe zwingend zu berücksichtigen sein, ob die Voraussetzungen des Datenzugriffs auf 2. Stufe

Ähnlich argumentiert das LG Ravensburg, wenn es die Entnahme von Fingerabdrücken beim Beschuldigten zum Zwecke der Entschlüsselung auf § 81b I StPO stützt, jedoch ausdrücklich klarstellt, dass es sich beim anschließenden Auslesen der Smartphonedaten um einen „eigenständigen Eingriff" handle, der sich nicht über die Regelungen zu den erkennungsdienstlichen Maßnahmen beim Beschuldigten legitimieren lasse, sondern über einen selbstständigen Rückgriff auf die Durchsichtsnorm des § 110 I, III StPO.[28]

Unabhängig davon, ob sich hier tatsächlich taugliche Ermächtigungsgrundlagen finden lassen, stellt sich zunächst die Frage nach der grundsätzlichen Zulässigkeit eines solchen methodisch-strukturellen Vorgehens. So hat etwa der BGH in Bezug auf die damals noch unnormierte verdeckte „Online-Durchsuchung" ausgeführt, es sei mit Blick auf den Grundsatz des Gesetzesvorbehalts sowie den Grundsatz der Normenklarheit und Tatbestandsbestimmtheit von strafprozessualen Eingriffsnormen „unzulässig, einzelne Elemente von Eingriffsermächtigungen zu kombinieren, um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen"[29]. Wenngleich vorliegend ein strukturell geringfügig anders gelagertes methodisches Vorgehen in Rede steht – dort: Kumulation von Ermächtigungsgrundlagen zu einer Gesamtrechtsgrundlage, hier: sukzessiv-additive Methode[30] –, so lassen sich die maßgeblichen Überlegungen des Gerichts dennoch auf den hiesigen Kontext übertragen: Denn insbesondere der Vorbehalt des Gesetzes bleibt nur dann hinreichend gewahrt, wenn sich der fragliche Vorgang einerseits tatsächlich, d.h. bei natürlicher Betrachtung, als ein Bündel isolierter Einzelmaßnahmen mit grundsätzlich unterschiedlicher Zielrichtung präsentiert und nicht als ein letztlich einheitliches, zusammengehöriges Geschehen. Andererseits darf die Maßnahmenkombination insgesamt, d.h. gerade in ihrer stufenweisen Verknüpfung, nicht schwerer wiegen als die Summe der Einzelmaßnahmen oder sich gar als gänzliches *aliud* gegenüber dem gesetzlich (Einzel-)Normierten erweisen.[31]

Beide Voraussetzungen sind hier indes nicht erfüllt: Das Auslesen eines (biometrisch) verschlüsselten Smartphones stellt sich einerseits als eine

---

vorliegen. Legt man hierauf den Schwerpunkt, ließe sich der Ansatz auch als Inzidentlösung (unter C.III.) und / oder Kombinationslösung (unter C.V.) begreifen.

[28] LG Ravensburg NStZ 2023, 446 m.Anm. *Horter*, StV-S 2023, 146 m.Anm. *Nicolai* unter zahlr. Hinweisen auf *Rottmeier/Eckel* NStZ 2020, 193.

[29] BGH NJW 2007, 930 Rn. 22 = BGHSt 51, 211.

[30] Zu dieser Unterscheidung *Nadeborn/Albrecht* NZWiSt 2021, 420, 421 ff.

[31] Ähnlich *Nadeborn/Albrecht* NZWiSt 2021, 420, 424.

grundsätzlich einheitliche Maßnahme dar: Der Entschlüsselung als solcher kommt nur eine vorgelagerte, letztlich „unselbstständige“ Rolle gegenüber dem eigentlich intendierten, nachfolgenden Schritt des Datenzugriffs zu.[32] Zwar lassen sich beide Maßnahmen begrifflich voneinander trennen, gleichwohl eint sie sowohl die vereinheitlichte Zielrichtung „Datenauslese“ wie auch der Umstand, dass Schritt 2 ohne Schritt 1 unmöglich, Schritt 1 ohne Schritt 2 – zumindest beweisrechtlich – einigermaßen sinnlos ist. Eine isolierte Betrachtung birgt damit unweigerlich die Gefahr einer unnatürlichen „Aufsplittung“ einer eigentlich einheitlichen Ermittlungsmaßnahme. Daneben weist der Zugriff auf verschlüsselte Daten angesichts des gesteigerten Nutzervertrauens in die Integrität des verschlüsselten Systems ein deutlich höheres Eingriffsgewicht auf als eine „ungesicherte Auslese“: Das Auslesen *ent*schlüsselter Daten ist eben nicht gleichzusetzen mit dem Auslesen *un*verschlüsselter Daten, denen *von vornherein* geringeres Vertrauen entgegengebracht wird und die sich damit normativ als weniger schutzwürdig erweisen.[33] Das legitimatorische „Abschichten“ durch das Abstellen auf verschiedene Befugnisnormen mag daher zwar verführerisch sein, dogmatisch tragfähig ist es mit Blick auf den Grundsatz des Vorbehalts des Gesetzes insbesondere angesichts der *aliud*-Stellung des Zugriffs auf (biometrisch) gesicherte Smartphones aber nicht.

Darüber hinaus fehlt es ohnehin bereits an einer tatsächlich einschlägigen, spezifischen Befugnisnorm auf 1. Stufe (Daten-Entschlüsselung):[34]

Ein Abstellen auf § 81a StPO, wie beispielsweise vom AG Verden und AG Wuppertal praktiziert,[35] scheidet angesichts gänzlich unterschiedlicher Zielrichtungen aus: So darf hiernach zwar der Körper des Beschuldigten zum Augenscheinsobjekt – und damit zum Beweismittel gegen sich selbst – gemacht werden.[36] Bei der biometrischen Smartphone-Entschlüsselung geht es jedoch nicht darum, Erkenntnisse hinsichtlich der Beschaffenheit des Körpers des Beschuldigten zu gewinnen, sondern der

[32] So letztlich auch *Rottmeier/Eckel* NStZ 2020, 193, 195 selbst: Datenzugriff der 2. Stufe als „eigentliche[s] Ziel der Maßnahme“.

[33] Ebenso *Grzesiek/Zühlke* StV-S 2021, 117, 124: verschlüsselte Daten als „Daten *eigener Qualität*“; vgl. auch *Gerhards*, (Grund-)Recht auf Verschlüsselung, 2010, 43 ff.; BVerfGE 120, 274, 324 sowie § 202a StGB, der u.a. auf *besonders gesicherte* Daten abstellt; a.A. *Rottmeier/Eckel* NStZ 2020, 193, 195 f.; kritisch auch *Stam* JZ 2023, 1070, 1079.

[34] Zu möglichen Befugnisnormen der 2. Stufe s. unter C.IV.

[35] AG Verden, Beschl. v. 27.6.2017 – 9a Gs 800 Js 15636/17 (2373/17) (unveröffentlicht); AG Wuppertal BeckRS 2017, 166377.

[36] *Goers*, in BeckOK-StPO, 52. Ed. 1.7.2024, § 81a; *Hadamitzky*, in Karlsruher Kommentar StPO, 9. Aufl. 2023, § 81a Rn. 1.

Beschuldigtenkörper soll lediglich als „Daten-Schlüssel“ Verwendung finden.[37]

Aus ähnlichen Gründen taugt auch der vielfach genannte § 81b StPO nicht als Ermächtigungsgrundlage. Denn dieser dient nach ganz h.M. dazu, notwendige Maßnahmen zur *Identifizierung* des Beschuldigten zu ermöglichen.[38] Im klassischen Fall der Entschlüsselung eines Smartphones geht es jedoch – auch und gerade bei isolierter Stufenbetrachtung – nicht darum, dass das Gerät den Beschuldigten als seinen Nutzer erkennt, mithin identifiziert, sondern um die Entsperrung der Verschlüsselung.[39]

## III. Inzidentlösungen

Einen methodisch anders gelagerten Weg beschreiten Autorinnen und Autoren, die – ähnlich dem in § 100j I 2 StPO beschriebenen „Stufen-Zusammenhang“ – im Rahmen der Verhältnismäßigkeitsprüfung einer Maßnahme der 1. Stufe (Entschlüsselung) das Vorliegen der Voraussetzungen des Datenzugriffs der 2. Stufe mithineinlesen, mithin die Voraussetzungen der Auslese „bereits auf dieser [1., *Anm. d. Verf.*] Ebene inzident [...] prüfen“[40]. Insofern müsse, so *Neuhaus*, der in § 100j I 2 StPO vom Gesetzgeber niedergelegte „Stufen-Grundsatz“ „als eine generelle Ausprägung des Verhältnismäßigkeitsgrundsatzes [...] auch in den hiesigen Fällen gelten“[41] – mit der Folge einer inzidenten Zulässigkeitsprüfung der Datenauslese i.R.d. Entschlüsselungsprüfung auf Ebene 1.

Abgesehen davon, dass eine Prüfung der Legitimationsvoraussetzungen der 1. Stufe nach dem oben Gesagten – unabhängig vom Ergebnis einer Inzidentprüfung der 2. Stufe – mangels einschlägiger Ermächtigungsgrundlage ohnehin negativ ausfallen müsste, fragt sich auch hier, inwieweit sich ein solches methodisches Vorgehen ins Regelungsgefüge der StPO einfügt. Hierbei ist insbesondere zu beachten, dass derartige inzidente Prüfzusammenhänge, sollen sie denn tatsächlich stattfinden,

---

[37] *Momsen* DRiZ 2018, 140, 141; *Stam* JZ 2023, 1070, 1078; i.E. ebenso *Bäumerich* NJW 2017, 2718, 2720; *Grzesiek/Zühlke* StV-S 2021, 117, 118; *Rottmeier/Eckel* NStZ 2020, 193, 196 f.; *Horn* Kriminalistik 2019, 641, 642; *Trück*, in Münchener Kommentar StPO, Bd. 1, 2. Aufl. 2023, § 81a Rn. 9.

[38] BeckOK-StPO/*Goers*, § 81b; KK-StPO/*Hadamitzky*, § 81b Rn. 1.

[39] Ausführlich zur Argumentation *Grzesiek/Zühlke* StV-S 2021, 117, 118 f.; *Stam* JZ 2023, 1070, 1078; i.E. ebenso *Momsen* DRiZ 2018, 140, 141; *Nadeborn/Irscheid* StraFo 2019, 274, 275; *Horter* NStZ 2023, 447, 448; a.A *Rottmeier/Eckel* NStZ 2020, 193, 194 ff.; *Bäumerich* NJW 2017, 2718, 2720 f.; MüKo-StPO/*Trück*, § 81b Rn. 8.

[40] *Neuhaus* StV 2020, 489, 491; vgl. auch *Rottmeier/Eckel* NStZ 2020, 193, 196 mit Fn. 27.

[41] *Neuhaus* StV 2020, 489, 491; in diese Richtung auch *Hecken/Ziegler* jurisPR-ITR 10/2023 Anm. 5.

grundsätzlich entweder ausdrücklich – wie eben in § 100j I 2 StPO – benannt oder aber jedenfalls im Wortlaut der Norm angelegt sind, so z.B. in § 110 StPO, der auf die Durchsuchung verweist. „Inzidentlösungen" werden also normalerweise in der Befugnisnorm (der 1. Stufe) irgendwie „thematisiert". Einen allgemeinen, keine spezifische Formulierung erforderlich machenden Grundsatz beschreiben sie demzufolge gerade nicht.

Weder § 81a StPO noch § 81b StPO als etwaige Befugnisnormen der 1. Stufe beinhalten jedoch inzidente Prüfzusammenhänge hinsichtlich des nachgelagerten Datenzugriffs; es fehlt den vorgeschlagenen Inzidentlösungen daher bereits an ihren methodischen Anwendungsvoraussetzungen. Im Übrigen vermag auch die generelle Zugriffs*richtung* des Ansatzes, wonach die wesentlich schwerwiegendere (Haupt-)Eingriffsmaßnahme (Datenzugriff) inzident im deutlich weniger gewichtigen Eingriff (Entschlüsselung) implizit mitenthalten sein soll, unter Wertungsgesichtspunkten kaum zu überzeugen.[42]

## IV. Annexlösungen

Eine dritte Ansicht greift auf die „prozessuale Übung"[43] sog. Annexkompetenzen zurück, betrachtet also die Entschlüsselung des Smartphones auf 1. Stufe als konkludent mitermächtigte Maßnahme der 2. Stufe „Datenzugriff bzw. -auslese". So enthält beispielsweise nach *Stam* „§ 94 StPO als Annex auch die Befugnis [...], rechtmäßig sichergestellte Smartphones biometrisch zu entschlüsseln"[44]. *Braun/Hummels* wiederum bewerten die „(zwangsweise durchgesetzte) Anordnung, das Smartphone mittels Fingerprint zu entsperren, [...] als notwendige Begleitmaßnahme (‚Annex-Kompetenz') zur nachfolgenden Durchsuchung des Geräts"[45]. Und auch *Momsen* geht grundsätzlich davon aus, dass bei Rechtmäßigkeit der „eigentlich intendierten Datengewinnung" – gemeint ist letztlich wiederum die 2. Stufe des Datenzugriffs – „auch die Entsperrung als Mittel zum Zweck legitimiert [wäre]"[46].

Ungeachtet nicht unerheblicher Probleme, die sich bei der Anerkennung von Annexkompetenzen u.a. mit Blick auf die besondere Eingriffsqualität und -intensität bestimmter Annexmaßnahmen ergeben können, hält die

[42] Für diesen Hinweis danke ich herzlich Prof. Dr. *Armin Engländer*.

[43] *Ziemann* ZStW 130 (2018), 762, 766.

[44] *Stam* JZ 2023, 1070, 1079; vgl. auch *Rottmeier/Eckel* NStZ 2020, 193, 196.

[45] *Braun/Hummels* PSP 2018, 3, 5 f.; in diese Richtung auch *Horn*, Biometrische Sicherungen, 2020, 43 ff.; *ders*. Kriminalistik 2019, 641, 642 f., 645.

[46] *Momsen* DRiZ 2018, 140, 142.

überwiegende Ansicht in Rechtsprechung und Literatur diese für zulässig, sofern sie typischerweise mit der Durchführung der Hauptmaßnahme verbunden und verhältnismäßig sind.[47] Beides wäre hinsichtlich der Entschlüsselung biometrisch gesicherter Smartphones wohl zu bejahen, da die Auslese von Smartphonedaten (als Hauptmaßnahme) inzwischen in der Mehrzahl der Fälle eine Überwindung irgendwie gearteter Zugangssicherungen – und damit eben auch biometrischer Verschlüsselungstechniken[48] – erfordert. Zugleich dürften Fingerabdruckscan bzw. Gesicht- oder Iriserkennung auch geeignet, erforderlich und angesichts ihrer bei isolierter Betrachtung geringen Eingriffstiefe – es wird „nur" ein Finger aufgelegt bzw. ein Smartphone vorgehalten – grundsätzlich auch angemessen sein. Die gilt insbesondere angesichts der Alternative zeit- und kostenintensiver Brut-Force-Angriffe, deren Erfolg zudem ungewiss ist.[49]

Gleichwohl verbliebe als selbstverständliche (weitere) Zulässigkeitsvoraussetzung, dass sich der Datenzugriff als (Haupt-)Ermittlungsmaßnahme auf eine *explizite* gesetzliche Befugnisnorm stützen ließe:[50]

Nicht wenige wollen in diesem Zusammenhang Zugriff, Auslese und Auswertung auf dem Smartphone befindlicher Daten über § 94 StPO bzw. § 102 StPO legitimieren.[51] Hier hat jüngst u.a. *Greco* überzeugend dargelegt, dass dieses traditionelle „Aktenordner-Modell" der Intensität und Tiefe des Grundrechtseingriffs „Smartphone-Auslese" nicht gerecht wird.[52] Denn das Smartphone ist, ob verschlüsselt oder nicht, eben keine schlichte „Dokumenten-Sammelmappe" (oder auch ein einfacher USB-Stick), sondern gewährt einen nahezu allumfassenden Einblick in die Nutzerpersönlichkeit.[53] Als „Abbild der Person" lässt es sich daher nicht einfach „als Gegenstand, der für die Untersuchung von Bedeutung sein kann" bzw. als „Sache" bagatellisieren, wird ihm doch angesichts seines sämtliche Lebensbereiche durchdringenden (Beweis-)Charakters sowie seiner (höchst-)persönlichen Inhalte bereits eine Einstufung als

[47] Zum Ganzen ausführlich *Ziemann* ZStW 130 (2018), 762, 769 ff. m.w.N. Zur weitgehend anerkannten Annexkompetenz bzgl. der Beschlagnahme „analoger" Schlüssel *Rottmeier/Eckel* NStZ 2020, 193, 196 m.w.N.; zu notwendigen Begleitmaßnahmen beim Einsatz von GPS s. BGHSt 46, 266.

[48] S. hierzu bereits Fn. 4.

[49] I.E. ebenso *Horn*, Biometrische Sicherungen, 2020, 45.

[50] So ausdrücklich *Ziemann* ZStW 130 (2018), 762, 766.

[51] So die wohl (noch) h.M., im hiesigen Zusammenhang *Stam* JZ 2023, 1070, 1080; *Neuhaus* StV 2020, 489, 489; *Braun/Hummels* PSP 2018, 3, 5 f.; s. auch *Zerbes/El-Ghazi* NStZ 2015, 425, 427 f.; vgl. auch BVerfGE 113, 29; 115, 166; 124, 43. Siehe hierzu auch Fn. 55.

[52] *Greco* StV 2024, 276 bzgl. unverschlüsselter Smartphones; i.E. ebenso *Momsen* DRiZ 2018, 140, 142.

[53] Ausführlich zum Ganzen *Greco* StV 2024, 276, 278 ff.; ähnlich *Momsen* DRiZ 2018, 140, 142.

„informationstechnisches System“ nur bedingt gerecht.[54] Das mobile Endgerät kann danach zwar z.B. im Rahmen einer Durchsuchung nach § 94 I StPO sichergestellt bzw. beschlagnahmt, nicht jedoch in seinem digitalen „Inhalt“ ausgelesen bzw. „durchsucht“ werden.[55]

Der Zugriff auf die auf dem Smartphone gespeicherten Daten lässt sich auch nicht, wie zum Teil vorgeschlagen,[56] auf § 110 I, III StPO stützen:[57] Zwar ermöglicht Absatz 3 explizit die Durchsicht elektronischer Speichermedien – worunter sich grundsätzlich auch Smartphones subsumieren ließen –, jedoch bezieht sich die Norm ausdrücklich auf Speichermedien „bei dem von der Durchsuchung Betroffenen“. Damit aber schafft § 110 III StPO keine eigenständige Eingriffsgrundlage, sondern nimmt als Teil der Durchsuchung unmittelbaren Bezug auf die Regelungen der §§ 102 f. StPO, die sie materiell entsprechend begrenzen.[58] Die durchsuchungslegitimierenden Normen der §§ 102 f. StPO greifen nach hiesiger Ansicht jedoch lediglich hinsichtlich des „analogen“ Mobilfunkendgeräts selbst, nicht jedoch hinsichtlich seines digitalen „Dateninhalts“ (s.o.). § 110 StPO vermag insofern zwar die Modalitäten der Durchsuchung zu regeln.[59] An deren spezifisches Bezugsobjekt – hier: nur Mobilfunkendgerät, nicht: Dateninhalt – bleibt die Norm in ihrem Anwendungsbereich aber gebunden.

Ein Abstellen auf § 100a StPO scheitert jedenfalls daran, dass die Norm einerseits lediglich den Zugriff auf Telekommunikationsdaten erfasst,[60] andererseits die in Absatz 1 Satz 2 und 3 geregelte Quellen-TKÜ, die die größte sachliche Nähe zum hier in Rede stehenden Smartphone-Datenzugriff aufweist, ausdrücklich einen Eingriff in das vom Betroffenen genutzte informationstechnische System „mit technischen Mitteln“ verlangt. Dies umfasst klassischerweise v.a. den Einsatz von Späh- und

---

[54] Hierzu im Einzelnen *Greco* StV 2024, 276, 280.

[55] A.A. aber wohl die (noch) h.M., vgl. BVerfGE 113, 29; 115, 166, 192 ff.; BGH NStZ 2021, 623; BGH BeckRS 2023, 10043; BGH StV-S 2021, 146; *Hauschild*, in Münchener Kommentar StPO, Bd. 1, 2. Aufl. 2023, § 94 Rn. 13, § 102 Rn. 25 f.; KK-StPO/*Greven*, § 94 Rn. 4; KK-StPO/*Henrichs/Weingast*, § 102 Rn. 11, jeweils m.w.N.; vgl. hierzu auch bereits Fn. 51.

[56] Vgl. hierzu bereits Fn. 28 mit diesbzgl. zust. Anm. *Horter*; zumindest grundsätzlich auch *Ludewig* KriPoZ 2019, 293, 298.

[57] Jedenfalls i.E. ebenso *Stam* JZ 2023, 1070, 1074, allerdings mit z.T. anderer Begründung; anders MüKo-StPO/*Hauschild*, § 110 Rn. 6; KK-StPO/*Henrichs/Weingast*, § 120 Rn. 2 m.w.N.; vgl. auch BVerfGE 115, 166; LG Ravensburg NStZ 2023, 446.

[58] *Hiéramente* NStZ 2021, 390, 394 f.; *Hegmann*, in BeckOK-StPO, 52. Ed. 1.7.2024, § 110 Rn. 14; MüKo-StPO/*Hauschild*, § 110 Rn. 1: Durchsicht als Bestandteil der Durchsuchung; vgl. auch BVerfGK 15, 225; i.T. anders *Peters* NZWiSt 2017, 465, 469.

[59] So ausdrücklich *Hiéramente* NStZ 2021, 390, 394 u.V.a. *Wicker* MMR 2013, 765, 767.

[60] Und damit z.B. keine Fotos o.Ä. erfasst; zur Zuordnung *Rückert*, in Münchener Kommentar StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 69 ff.

Überwachungssoftware („Staatstrojaner"), beinhaltet aber selbst bei weiter Auslegung[61] jedenfalls nicht den Einsatz rein *körperlicher* Zugriffsmittel wie Fingerabdruck oder Gesichtserkennung.[62] Hingegen dürfte die Offenheit des Smartphonedaten-Zugriffs einer Anwendbarkeit nicht entgegenstehen, da die erlaubte Heimlichkeit der Quellen-TKÜ *a maiore ad minus* auch nicht verdeckte Maßnahmen mitumfasst.[63] Auf die Regelung zur Online-Durchsuchung nach § 100b StPO kann ebenfalls nicht zurückgegriffen werden, da der Datenzugriff schon nicht „online", d.h. remote als Fernzugriff, erfolgt und es zudem wiederum am erforderlichen Einsatz *technischer* Mittel fehlt (s.o.).[64]

Sofern hinsichtlich §§ 100a, 100b StPO eine analoge Anwendung angedacht wird,[65] dürfte dies jedenfalls nicht für die Annahme einer Annexkompetenz zur Entschlüsselung genügen, da insofern eine *explizit* gesetzlich normierte (Haupt-)Ermittlungsmaßnahme erforderlich ist.[66] Andernfalls stützte man etwas bloß konkludent Miterklärtes (Annexkompetenz) auf etwas bloß gesetzlich Mitgemeintes (Analogie).

Nach § 100i StPO dürfen wiederum lediglich Geräte- und Kartennummer sowie der Standort des Mobilfunkendgeräts ermittelt werden, während §§ 100j und 100k StPO einen Auskunftsanspruch gegenüber den Telekommunikations- bzw. Telemediendienstleistern normieren bzw. zur Erhebung von sog. Nutzungsdaten von Telemediendienstanbietern berechtigen. Die Normen taugen daher ebenfalls nicht als Eingriffsgrundlage für die Auslese gespeicherter Smartphonedaten.

Ein Rückgriff auf die Ermittlungsgeneralklausel der §§ 160, 161 StPO verbietet sich schließlich angesichts der erheblichen Eingriffstiefe, die mit dem Zugriff auf das Smartphone als „ultimatives Beweismittel"[67] verbunden ist.[68]

---

[61] Vgl. MüKo-StPO/*Rückert*, § 100a Rn. 203: „alle denkbaren technischen Mittel".

[62] I.E. ebenso MüKo-StPO/*Rückert*, § 100b Rn. 42.

[63] Bzgl. § 110b StPO: *Stam* JZ 2023, 1070, 1077; MüKo-StPO/*Rückert*, § 100b Rn. 42; ebenfalls kritisch bzgl. der Gegenüberstellung „offen vs. heimlich" *Greco* StV 2024, 276, 278; anders *Rottmeier/Eckel* NStZ 2020, 193, 197.

[64] *Grzesiek/Zühlke* StV-S 2021, 117, 120; *Stam* JZ 2023, 1070, 1077; MüKo-StPO/*Rückert*, § 100b Rn. 42.

[65] Dahingehend zunächst *Momsen* DRiZ 2018, 140, 142 f., der i.E. eine Analogie dann aber doch ablehnt. Vgl. in diesem Zusammenhang auch *Greco* StV 2024, 276, 280. Insgesamt kritisch bzgl. einer analogen Anwendung *Grzesiek/Zühlke* StV-S 2021, 117, 120; MüKo-StPO/*Rückert*, § 100b Rn. 42.

[66] Vgl. hierzu bereits Fn. 63.

[67] S. hierzu bereits unter A.

[68] *Grzesiek/Zühlke* StV-S 2021, 117, 120; *Stam* JZ 2023, 1070, 1077; vgl. auch *Kölbel/Ibold*, in: Münchener Kommentar StPO, Bd. 2, 2. Aufl. 2024, § 161 Rn. 7: Beschränkung auf Ermittlungsmaßnahmen, die eine „minder intensive Eingriffswirkung entwickeln".

Nach hiesiger Ansicht fehlt es daher – zumindest aktuell – bereits an einer explizit gesetzlich normierten Hauptermittlungsmaßnahme „Smartphonedaten-Zugriff"; für eine etwaige Annexkompetenz zur biometrischen Entschlüsselung verbleibt insofern kein Anknüpfungspunkt.

## V. Kombinationslösungen

Bisweilen finden sich auch Kombinationen der drei oben genannten Lösungsansätze. So nimmt beispielsweise *Stam* eine Annexkompetenz über § 94 StPO für die Entschlüsselung an (s.o.), empfiehlt dann aber i.R.d. Verhältnismäßigkeit eine „Orientierung am Katalog des § 100b Abs. 2 StPO"; zugleich sollte der Zugriff „nur subsidiär zulässig sein (vgl. § 100b Abs. 1 Nr. 3 StPO)"[69].

Wenngleich an dieser Stelle angesichts des beschränkten Umfangs nicht auf sämtliche Kombinationsvarianten eingegangen werden kann, so liegt doch der Gedanke nahe, dass sich diese in weiten Teilen wenigstens die beschriebenen methodisch-strukturellen Mängel der Lösungsansätze (mit-)einkaufen, auf die sie jeweils (mit-)abstellen. Bezogen auf den kombinierten Ansatz von *Stam* lässt sich jedenfalls – abgesehen von der fehlenden Ermächtigungsgrundlage auf 2. Stufe (s.o.) – mit dem BGH entgegnen, dass der Grundsatz der Verhältnismäßigkeit zwar im Einzelfall gesetzliche Befugnisse begrenzen, nicht jedoch eine fehlende Ermächtigungsgrundlage ersetzen kann.[70] Andernfalls erschöpfte sich der verfassungsrechtlich verbürgte Grundsatz des Vorbehalts des Gesetzes in der schlichten – und unter Bestimmtheitsgesichtspunkten kaum tragbaren – „Bastelei", auf eine jedenfalls nicht völlig geeignet erscheinende gesetzliche Befugnisnorm abzustellen, diese dann jedoch mittels einer besonders strikten, anderweitige gesetzliche Bestimmungen – welche nun genau? – in Bezug nehmenden Verhältnismäßigkeitsprüfung passend zu *machen*.

## VI. Zwischenergebnis

Wenngleich damit Annexlösungen im Vergleich zu sukzessiv-additiven, Inzident- und Kombinationslösungen wohl noch mit den wenigsten methodisch-strukturellen Fallstricken behaftet zu sein scheinen, vermögen sie mangels einer ausdrücklich gesetzlich normierten (Haupt-)

[69] *Stam* JZ 2023, 1070, 1080.
[70] BGH NJW 2007, 930 Rn. 22 = BGHSt 51, 211.

Ermittlungsmaßnahme als Anknüpfungspunkt etwaiger Annexkompetenzen die Entschlüsselung und Datenauslese bei mobilen Endgeräten aktuell nicht zu legitimieren. Hinsichtlich der übrigen methodischen Zugänge bestehen bereits massive Bedenken hinsichtlich ihrer dogmatischen Tragfähigkeit im Allgemeinen (bzgl. „Baukastenprinzip" bzw. Kombinationslösungen) bzw. im Besonderen (Inzident- bzw. Kombinationslösungen).

## D. Fazit und Ausblick

Die Entschlüsselung und Auslese biometrisch gesicherter Mobilfunkendgeräte verstößt selbst bei erzwungenem Fingerabdruck bzw. ertäuschtem Gesichtsvorhalt nicht gegen den Grundsatz der Selbstbelastungsfreiheit, da die Maßnahmen jedenfalls keinen unmittelbaren Persönlichkeitsbezug aufweisen und keine Unterordnung des Beschuldigten unter das Verfahren bedeuten. Der Schutzbereich von Nemo-tenetur ist dahingehend nicht betroffen.

Gleichwohl sind die zwangsweise Entschlüsselung und Datenauslese biometrisch gesicherter Smartphones durch die Ermittlungsbehörden *de lege lata* unzulässig:[71] Die in Literatur und Rechtsprechung hierzu vertretenen anderslautenden Ansätze sind zwar bisweilen durchaus kreativ,[72] stehen jedoch entweder bereits aufgrund ihres methodisch-strukturellen Vorgehens auf dogmatisch tönernen Füßen (sukzessiv-additive, Inzident- und Kombinationslösungen) oder können die Maßnahme(n) jedenfalls aufgrund des Fehlens einer einschlägigen expliziten Ermächtigungsgrundlage für den Datenzugriff als nachgelagertes Ziel nicht legitimieren (Annexlösungen).

*De lege ferenda* sollte angesichts des erheblichen und durchaus nachvollziehbaren Bedürfnisses der Strafverfolgungsbehörden, Smartphonedaten auslesen zu können, dringend eine eigenständige Ermächtigungsgrundlage geschaffen werden, die sowohl den Zugriff auf verschlüsselte wie auch auf unverschlüsselte mobile Endgeräte ausdrücklich regelt.[73] Andernfalls drohen wichtige Ermittlungsansätze aufgrund des Fehlens einer einschlägigen Befugnisnorm ungenutzt zu bleiben.

[71] I.E. ebenso *Momsen* DRiZ 2018, 140, 143.

[72] Ähnlich *Nicolai* StV-S 2023, 148.

[73] Ebenfalls für eine ausdrückliche gesetzliche Regelung u.a. *Greco* StV 2024, 276, 280; *Momsen* DRiZ 2018, 140, 143; *Stam* JZ 2023, 1070, 1080; *Neuhaus* StV 2020, 489, 491; *Ludewig* KriPoZ 2019, 293, 300. Eine solche würde schließlich auch von vornherein von den benannten Schwierigkeiten der Annexlösungen entbinden.

Herausforderung bei der Schaffung einer Neuregelung wird sein, sowohl den Anforderungen der täglichen Ermittlungspraxis als auch den grundrechtlichen Positionen des Beschuldigten (u.a. durch einen expliziten Kernbereichsschutz) in hinreichendem Maße Rechnung zu tragen.