Kapitel 5 – Verfassungsrechtliche Rechtfertigung

Wie in Kap. 4 herausgearbeitet, liegt sowohl durch die Anwendung der dargestellten Auswertungsmethoden als auch durch die Verknüpfung der Ergebnisse der Auswertungsmethoden miteinander jeweils ein Eingriff in das RiS vor. Zur rechtmäßigen Anwendung der Auswertungsmethoden ist daher eine verfassungsrechtliche Rechtfertigung erforderlich. Eine solche kann insbesondere eine gesetzliche Grundlage sein, auf der die Anwendung der Auswertungsmethoden beruht. Eine derartige gesetzliche Grundlage muss dabei insbesondere bestimmten, verfassungsrechtlichen Anforderungen genügen, um einen Grundrechtseingriff rechtfertigen zu können.

Um zu untersuchen, ob es zum Zweck der Strafverfolgung eine ausreichende gesetzliche Ermächtigungsgrundlage in der StPO gibt, wird nachfolgend zunächst nochmals ausführlicher darauf eingegangen, wie die Auswertungsmethoden konkret in der Ermittlungspraxis eingesetzt werden könnten (hierzu unter A.). Anschließend wird darauf eingegangen, ob die StPO grundsätzlich eine den Anforderungen an die Einschränkung des RiS genügende Ermächtigungsgrundlage enthält, die für die hier gegenständlichen Auswertungsmethoden einschlägig sein kann (hierzu unter B.).

Die so ermittelte, einschlägige Ermächtigungsgrundlage wird dann auf ihre grundsätzliche Verfassungsmäßigkeit hin überprüft (hierzu unter C.), um anschließend darauf einzugehen, ob die Auswertungsmethoden zulässigerweise auf die einschlägige Ermächtigungsgrundlage der StPO gestützt werden können (hierzu unter D.).

Nachdem in einer kurzen Zusammenfassung das Ergebnis formuliert wird, dass die hier gegenständlichen Auswertungsmethoden nur teilweise eine ausreichende verfassungsrechtliche Rechtfertigung in den Ermittlungsgeneralklauseln der §§ 161, 163 StPO finden (hierzu unter E.), wird schließlich eine Lösung vorgeschlagen, wie durch eine gesetzliche Änderung des § 98a StPO die Auswertungsmethoden auf eine ausreichende verfassungsrechtliche Rechtfertigung gestützt werden können (hierzu unter F.).

A. Auswertungsmethoden in der Ermittlungspraxis

Um bewerten zu können, ob die StPO eine ausreichende gesetzliche Grundlage für die Auswertungsmethoden enthält, stellt sich zunächst die Frage, wie diese Auswertungsmethoden wohl in der Praxis eingesetzt werden. Denn einerseits sind die in der Blockchain enthaltenen Daten grundsätzlich pseudonym[1029], sodass hierdurch die Intensität des Grundrechtseingriffs möglicherweise verringert ist[1030]. Andererseits muss auch berücksichtigt werden, dass wohl jedenfalls ein Ziel des Einsatzes der Auswertungsmethoden darin liegt, einen Personenbezug herzustellen. Dementsprechend muss auch berücksichtigt werden, wie die Auswertungsmethoden in der Ermittlungspraxis konkret eingesetzt werden könnten.

Dabei dürften sich insbesondere zwei Fragen stellen:

- In welchem Stadium der Strafverfolgung werden die Auswertungsmethoden eingesetzt?
- Welche Informationen ergeben sich aus den einzelnen Auswertungsmethoden und welche Informationen können sich aus deren Verknüpfung ergeben?

Für die Stadien der Strafverfolgung kommen insbesondere drei Varianten in Betracht, die danach differenziert werden können, ob bereits ein Anfangsverdacht besteht:

1029 Siehe zur begrifflichen Unterscheidung zwischen Anonymität und Pseudonymität *Bechtolf/Vogt,* ZD 2018, 66 (68f.).

1030 *Rückert,* ZStW 129 (2017), 302 (324). Das BVerfG nimmt außerdem an, dass die Grundrechtsintensität verringert ist, wenn der Personenbezug erst durch Zusatzwissen hergestellt werden kann, vgl. BVerfGE 128, 1 (53). Allerdings nimmt das BVerfG an, dass es sich insoweit um anonyme Daten handele. Der Begriff der anonymen Daten dürfte insoweit vom Begriff der anonymen Daten im Datenschutzrecht abweichen, vgl. Erwägungsgrund Nr. 26 DSGVO. Außerdem nimmt das BVerfG auch eine verringerte Grundrechtsintensität bei anonymen Daten an, vgl. BVerfGE 65, 1 (45); BVerfGE 100, 313 (376); BVerfGE 115, 320 (347), wobei allerdings unklar ist, inwieweit bei anonymen Daten überhaupt ein Grundrechtseingriff vorliegen soll (vgl. hierzu ausführlich oben unter Kap. 4, B.I.b)). Grund hierfür könnte etwa sein, dass das BVerfG für die Bewertung der Grundrechtsintensität wechselseitig auf die jeweiligen Maßstäbe der Bewertung der Grundrechtsintensität bei Eingriffen in Art. 10, Art. 13 GG und das RiS nimmt, vgl. *Buermeyer,* Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug, S. 165f. Hieraus lässt sich aber der Rückschluss ziehen, dass die Grundrechtsintensität jedenfalls verringert ist, wenn kein unmittelbarer Personenbezug besteht.

1. Die Auswertungsmethoden können eingesetzt werden, um Anhaltspunkte zu ermitteln, die auf das Vorliegen einer Straftat hindeuten (verdachtsbegründend). Die Auswertungsmethoden würden also proaktiv eingesetzt werden, bevor der Verdacht einer Straftat besteht (ein Beispiel hierzu sogleich unter I.).
2. Die Auswertungsmethoden können eingesetzt werden, um, nachdem der Verdacht einer Straftat besteht, diesen zu erhärten und nach Möglichkeit eine natürliche Person als Verdächtige zu ermitteln (ein Beispiel hierzu sogleich unter II.).
3. Die Auswertungsmethoden können in einem Zwischenstadium zwischen der Begründung eines Anfangsverdachts (siehe 1.) und dem Bestehen eines Anfangsverdachts (siehe 2.) eingesetzt werden – etwa, um die Blockchain-Daten unmittelbar nach zuvor genau bezeichneten Transaktionsmustern zu durchsuchen, die auf eine bestimmte Straftat hindeuten (ein Beispiel hierzu sogleich unter III.). Insoweit bestünden bereits verdachtsbegründende Anhaltspunkte (das bestimmte Transaktionsmuster), die aber noch keine konkrete, einzelne Straftat betreffen.

I. Einsatz zur Verdachtsbegründung

Um einen Verdacht zu begründen, könnte etwa zunächst eines der oben[1031] beschriebenen *Clustering* Verfahren eingesetzt werden, um einzelne Bitcoin-Adressen zunächst zu *Entitäten* zu gruppieren. Das Transaktionsverhalten dieser Entitäten könnte dann ausgewertet werden, um den Zahlungsströmen zu folgen und sie anschließend graphisch darzustellen. Die so ermittelten *Entitätsdaten* könnten dann beispielsweise von einem Algorithmus ausgewertet werden, wie ihn *Hirshman/ Huang/ Macke*[1032] entwickelt haben, um auffälliges Transaktionsverhalten zu ermitteln. Bereits hieraus könnten sich etwa Anhaltspunkte ergeben, die auf Geldwäsche hindeuten.[1033]

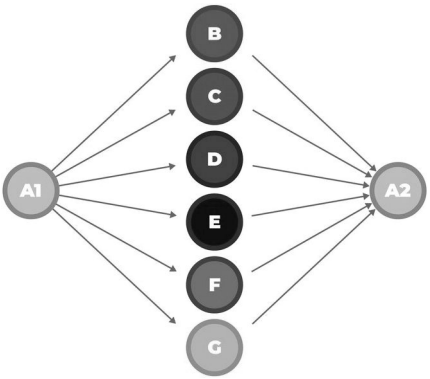
So haben *Hirshman/ Huang/ Macke* beispielsweise Transaktionen ermittelt, bei denen von einer *Bitcoin-Adresse* (A1) Bitcoin an mehrere, verschie-

1031 Siehe hierzu unter Kap. 3 A.I.

1032 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network 1 (1ff.); siehe hierzu oben unter Kap. 3 A.II.

1033 Siehe hierzu etwa *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (5), die bereits Anhaltspunkte für Geldwäsche lediglich anhand der Zahlungsströme von Bitcoin-

dene andere *Bitcoin-Adressen* (B-G) transferiert wurden und anschließend über Umwege wieder zu einer einzelnen *Bitcoin-Adresse* (A2) zusammengeführt wurden.



Diese Abbildung bildet nicht die Transaktionsströme ab, die von *Hirshman/Huang/Macke* ermittelt wurden, sondern veranschaulichen vereinfacht deren Ergebnisse.

Weitere Ergebnisse derartiger Ermittlungen können sich daraus ergeben, wenn die Blockchain-Daten mit Zusatzinformationen angereichert werden.

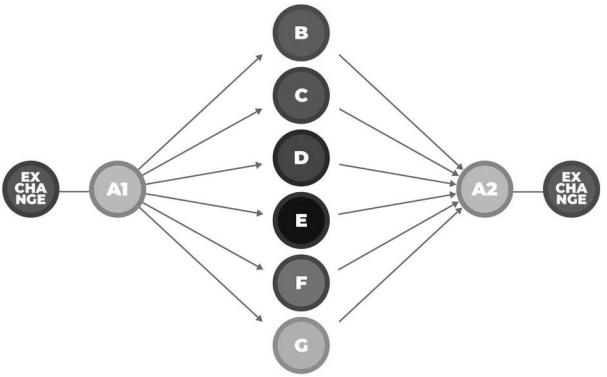
So können etwa einzelnen Bitcoin-*Adressen/-Entitäten* bestimmte Attribute zugeordnet werden, wie etwa, dass sie wahrscheinlich zu einem *Exchange-Service* gehören. Diese Attribute können etwa durch den Vergleich mit bekanntem Transaktionsverhalten[1034] oder durch *Web-Crawler*, die das Internet nach veröffentlichten *Bitcoin-Adressen* durchsuchen, zu *Bitcoin-Adressen/-Entitäten* zugeordnet werden.[1035]

So könnte in dem oben angeführten Beispiel ermittelt werden, dass die von A1 empfangene Transaktion von einem *Exchange-Service* stammt und A2 die von ihm empfangenen Transkationen wieder an einen *Exchange-Service* weiterleiten. So würde sich das oben dargestellte Beispiel wie folgt graphisch darstellen lassen:

Adressen ermittelt haben, also ohne ein *Clustering* Verfahren zusätzlich einzusetzen.

1034 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.); siehe hierzu oben unter Kap. 3 A.III.3.

1035 Siehe hierzu oben unter Kap. 3 C.I.



Die bereits bestehenden Anhaltspunkte für Geldwäsche (siehe das vorangegangene Beispiel) könnten so erhärtet werden und einen Verdacht begründen.

Ein Ermittlungstool, das die *Bitcoin-Adressen* automatisch zu *Entitäten clustert* und diese automatisch mit verfügbaren Daten zu den Hintergründen der *Entitäten* und *Adressen* verknüpft, wurde bereits vom Austrian Institute of Technology entwickelt, ist bisher aber nur zu Forschungszwecken im Einsatz.[1036]

Insoweit können die Ermittlungsmöglichkeiten zur Begründung eines Verdachts eingesetzt werden.

II. Einsatz zur Ermittlung nach bestehendem Verdacht

Allerdings kann sich ein Verdacht auch aus anderen Umständen ergeben, wie etwa, dass auf einem *Darknet-Handelsplatz* der Verkäufer von illegalen Waren seine Bitcoin-Empfangsadresse veröffentlicht oder der Erpresser, der vorgibt, einen Computer gehackt zu haben, fordert das Opfer zur Zahlung an eine bestimmte *Bitcoin-Adresse* auf.

Wenn nun der Verdacht einer Straftat besteht, ist regelmäßig das Ziel weiterer Ermittlungen, herauszufinden, welche natürlichen Personen hinter den jeweiligen *Bitcoin-Adressen* stehen.

1036 Das Tool nennt sich *GraphSense,* siehe hierzu: https://graphsense.info (letzter Abruf: 20. Dezember 2021).

Hierzu könnten einerseits die Ermittlungsmethoden, durch die IP-Adressen ermittelt werden können[1037], eingesetzt werden, um anschließend bei dem jeweiligen Internet-Access-Provider die Kundendaten des Anschlussinhabers abzufragen.

Andererseits können die Ermittlungsbehörden an der Schnittstelle zwischen virtueller und realer Welt ansetzen. Wenn etwa in dem oben beschriebenen Beispiel die *Bitcoin-Adresse* A2 sich ihre erhaltenen Bitcoin bei einem bestimmten *Exchange-Service* auszahlen lässt, könnten die Strafverfolgungsbehörden an den jeweiligen *Exchange-Service* herantreten und Auskunft über die Identität von A2 oder über das Bankkonto, über das der Umtausch abgewickelt wurde, verlangen.[1038]

III. Einsatz von Ermittlungsmethoden, durch die unmittelbar ein Anfangsverdacht begründet werden kann

Außerdem ist es, wie oben[1039] dargestellt, möglich in einem zweischrittigen Verfahren zunächst Transaktionsverhalten, von dem die Hintergründe bekannt sind, nach deren typischen Transaktionsmustern hin zu analysieren, und anschließend die Blockchain-Daten nach ähnlichen Transaktionsmustern zu durchsuchen.[1040]

Wenn also von mehreren Transaktionen bekannt ist, dass sie im Zusammenhang mit Betrug, Erpressung oder Geldwäsche standen, ist es möglich, deren typisches Transaktionsverhalten von anderem Transaktionsverhalten abzugrenzen und so zu definieren, bei welchen bestimmten Anhaltspunkten wohl ein Transaktionsmuster vorliegt, das ebenfalls auf eine dieser Straftaten hindeutet. So ließen sich dann die Blockchain-Daten nach diesen zuvor ermittelten Anhaltspunkten durchsuchen, um so weitere Transaktionen aufzudecken, die wahrscheinlich auch im Zusammenhang mit Betrug, Erpressung oder Geldwäsche stehen.[1041]

1037 Siehe hierzu unter Kap. 3 B.

1038 Dies setzt wohl voraus, dass der jeweilige *Exchange-Service* in Deutschland bzw. in der EU ansässig ist. Siehe zu den rechtlichen Voraussetzungen bereits oben unter Kap. 4 B.II.c)(1).

1039 Siehe hierzu unter Kap. 3 A.III.

1040 Siehe hierzu unter Kap. 3 A.III.

1041 Siehe hierzu oben ausführlich unter Kap. 3 A.III.1ff. und insbesondere *Monamo/Marivate/Twala*, ISSA 2016, 129 (129); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

Anhaltspunkte für das Vorliegen einer konkreten Straftat bestehen also unmittelbar, wenn das Durchsuchen der Blockchain-Daten weitere Transaktionen ermittelt hat, die auf Grund des Transaktionsmusters ebenfalls auf ein strafbares Verhalten hindeuten. Unklar ist jedoch, ob bereits verdachtsbegründende Anhaltspunkte vorliegen, wenn lediglich abstrakt das Transaktionsmuster ermittelt wurde, dessen Vorliegen auf ein strafbares Verhalten hindeutet.

IV. Zwischenergebnis

Die oben dargestellten Auswertungsmethoden können nicht getrennt voneinander betrachtet werden, sondern sie werden zu Strafverfolgungszwecken in der Praxis wohl regelmäßig miteinander kombiniert werden, um einerseits die Hintergründe einzelner Transaktionen zu ermitteln und andererseits die natürlichen Personen zu ermitteln, die hinter den Transaktionen stehen. Insoweit muss für die Frage nach einer ausreichenden gesetzlichen Grundlage nicht nur auf die jeweils einzelne Maßnahme abgestellt werden, sondern die Maßnahmen müssen insoweit auch dahingehend betrachtet werden, welche weiteren Auswertungen sie ermöglichen oder vereinfachen. Betrachtet man etwa eines der *Clustering*-Verfahren – etwa das in der Praxis gängigste, das *Multi-Input-Clusutering* – ließe sich argumentieren, dass die hierdurch nur ein Eingriff mit geringer Grundrechtsintensität vorliegt, für den keine besondere gesetzliche Grundlage erforderlich ist. Denn die ausgewerteten Daten sind öffentlich verfügbar, lassen zunächst keine Rückschlüsse auf die hinter ihnen stehenden Personen zu und ermöglichen selbst auch kein Erstellen von Persönlichkeitsprofilen oder Ähnlichem.[1042] Dabei ist jedoch zu berücksichtigen, dass ein derartiges *Clustering*-Verfahren gerade ein Ansatzpunkt sein kann, um diese intensitätsverringernden Aspekte zu beseitigen. Denn wie unter II. dargestellt, können sich hieraus weitere Ansatzpunkte ergeben, um die Identität einer *Entität* zu ermitteln, wenn für mehrere *Bitcoin-Adressen* die Auswertungsmethoden angewendet werden können. Außerdem ermöglichen bzw. vereinfachen sie darüber hinaus die in Kap. 3, A.III. dargestellten *Labelling*-Verfahren, um *Entitäten* und den darin enthaltenen *Bitcoin-Adressen* bestimmte Attribute auf Grund ihres Transaktionsverhaltens zuzuschreiben.

1042 Siehe zu den Kriterien für die Bewertung der Grundrechtsintensität nachfolgend ausführlich unter Kap. 5, D.II.

Dies muss insoweit bei der Frage, ob die StPO eine ausreichende gesetzliche Grundlage enthält, entsprechend berücksichtigt werden.

B. Einschlägige Ermächtigungsgrundlage in der StPO

Eine gesetzliche Grundlage, die zu einem Eingriff in das RiS ermächtigt, muss nach vorherrschender Auffassung zunächst der sog. Schrankentrias des Art. 2 Abs. 1 Hs. 2 GG genügen.[1043] Nach der Schrankentrias des Art. 2 Abs. 1 Hs. 2 GG können die Grundrechte des Art. 2 Abs. 1 GG auf Grund einer Verletzung der Rechte anderer, der verfassungsmäßigen Ordnung und dem Sittengesetz eingeschränkt werden.[1044] Besondere Bedeutung kommt dabei der verfassungsmäßigen Ordnung zu, die nach dem sog. Elfes-Urteil des BVerfG[1045] die „Gesamtheit der verfassungsgemäßen Rechtsordnung"[1046] und damit jede formell und materiell mit der Verfassung im Einklang stehende Norm umfasst.[1047] Nach einhelliger Auffassung liegt in der verfassungsmäßigen Ordnung daher ein einfacher Gesetzesvorbehalt bzw. ein allgemeiner Rechtsvorbehalt[1048] vor, sodass ein Eingriff durch eine formell und materiell verfassungsgemäße gesetzliche Grundlage gerechtfertigt werden kann.[1049] Insoweit ist für die Anwendung der Auswertungsmethoden eine formell und materiell verfassungsgemäße gesetzliche Grundlage erforderlich.

Gegenstand dieser Untersuchung ist der Einsatz der Auswertungsmethoden, um die Strafverfolgung zu unterstützen. Dementsprechend beschränkt sich die nachfolgende Prüfung auf die Ermittlungsbefugnisse der StPO.

Problematisch ist in diesem Zusammenhang vor allem, dass die Ermächtigungsgrundlagen der StPO die Strafverfolgungsbehörden vorwiegend dazu ermächtigen, entweder bestimmte Daten oder Daten in einer bestimm-

1043 BVerfGE 65, 1 (44); BVerfGE 78, 77 (85); BVerfGE 97, 228 (269); *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 40; *Bauer*, Soziale Netzwerke, S. 67; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 87 jeweils m.w.N.

1044 *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 87.

1045 BVerfGE 6, 32ff.

1046 BVerfG NJW 1957, 297 Ls. c); Stern-Becker-GG/*Horn,* Art. 2 Rn. 96.

1047 BVerfG NJW 1957, 297 Ls. c); Stern-Becker-GG/*Horn,* Art. 2 Rn. 96; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 87.

1048 So Stern-Becker-GG/*Horn,* Art. 2 Rn. 96; *Bauer*, Soziale Netzwerke, S. 67; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 87f.

1049 Stern-Becker-GG/*Horn,* Art. 2 Rn. 96. Zu den Anforderungen der formellen und materiellen Verfassungsmäßigkeit sogleich im Einzelnen.

ten Art und Weise zu erheben[1050] – etwa Telekommunikationsdaten (§ 100a StPO), Daten von informationstechnischen Systemen (§ 100b StPO) oder das gesprochene Wort in Wohnungen (§ 100c StPO).

Der hier gegenständliche Eingriff in das RiS durch die Auswertungsmethoden liegt zwar auch teilweise durch die Erhebung in Form einer umfassenden und zielgerichteten Speicherung der Daten vor[1051], maßgeblich ist hier jedoch insbesondere die systematische Analyse der so erhobenen Daten.[1052] Insoweit stellt sich die Frage, ob die StPO für derartige Eingriffe in das RiS eine entsprechende Rechtsgrundlage enthält.

Um diese Frage zu untersuchen, wird nachfolgend zunächst geprüft, ob eine der speziellen Ermittlungsbefugnisse der StPO hier einschlägig sein kann (hierzu unter I.-VI.) oder lediglich die Ermittlungsgeneralklauseln der §§ 161, 163 StPO Anwendung finden können (hierzu unter VIII.), die ohnehin nur subsidiär herangezogen werden können[1053].

I. §§ 94, 110 StPO – Sicherstellung, Beschlagnahme, Durchsuchung und Durchsicht

In Betracht kommen daher grundsätzlich die bereits für andere Ermittlungen im Zusammenhang mit Telekommunikation(sdaten) herangezogenen Ermächtigungsgrundlagen der §§ 94, 110 StPO.[1054] Diese Vorschriften stehen in einem engen Zusammenhang zueinander[1055] und ermächtigen die Strafverfolgungsbehörden einerseits zur Sicherstellung bzw. Beschlagnahme[1056] von Beweismitteln (§ 94 StPO) und andererseits zur Durchsicht von

1050 Vgl. *Körffer,* DANA 2014, 146 (147).

1051 Siehe hierzu insbesondere die Datenerhebung der in Kap. 3, B. dargestellten Auswertungsmethoden, durch die bereits ein Eingriff in das RiS vorliegt, vgl. Kap. 4, B.II.2.c)(1).

1052 Vgl. hierzu bereits Kap. 4, B.II.2.c)(1), wonach ein Eingriff in das RiS durch die Auswertung der unmittelbaren Blockchain-Daten vorliegt.

1053 Die Subsidiarität ergibt sich bereits unmittelbar aus § 161 Abs. 1 S. 1 Hs. 2 StPO. So auch *Rückert*, ZStW 129 (2017), 302 (315); Meyer-Goßner/Schmitt/*Köhler,* § 161 Rn. 1.

1054 Siehe zur Beschlagnahme von E-Mails, die auf dem Server des Providers zwischen- und endgespeichert werden, insbesondere BVerfGE 124, 43ff.

1055 Vgl. *Park,* Durchsuchung und Beschlagnahme, § 1 Rn. 14.

1056 Zur begrifflichen Differenzierung, dass die Beschlagnahme eine Sicherstellung gegen den Willen des Betroffenen ist, sogleich.

Papieren und elektronischen Speichermedien (§ 110 StPO), die bei einer Durchsuchung aufgefunden werden.[1057]

I. § 94 StPO – Sicherstellung bzw. Beschlagnahme

Nach § 94 Abs. 1 StPO können „Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können" in Verwahrung genommen werden oder auf andere Weise sichergestellt werden. Darüber hinaus ermächtigt § 94 Abs. 2 StPO zur Beschlagnahme derartiger Gegenstände gegen den Willen des Betroffenen. Der Begriff der „Gegenstände" ist dabei weit auszulegen[1058], sodass er sich auf „alles, was einen Beweiswert haben und für die Untersuchung von Bedeutung sein kann"[1059] erstreckt und sowohl Datenträger als auch digital gespeicherte Informationen erfasst.[1060]

Insbesondere bei der Beschlagnahme von Datenträgern und digital gespeicherten Informationen ermächtigt er daher unter anderem auch zu einem Eingriff in das RiS.[1061]

So kann § 94 StPO nach der Rechtsprechung des BVerfG auch eine ausreichende Ermächtigungsgrundlage darstellen, um E-Mails zu beschlagnahmen, die auf dem Server eines E-Mail-Dienstes zwischengespeichert sind.[1062]

Insoweit stellt sich die Frage, ob § 94 StPO auch für die hier gegenständlichen Auswertungsmethoden einschlägig sein kann, durch die ebenfalls in das RiS eingegriffen wird.[1063]

a) Keine unmittelbare Einschlägigkeit von § 94 StPO

Gegen die Einschlägigkeit von § 94 StPO spricht zunächst, dass die Beschlagnahme – soweit etwa Daten beschlagnahmt werden – vorrangig zur

1057 Vgl. Meyer-Goßner/Schmitt/*Köhler,* Vor § 94 Rn. 3f.; Hdb-StA/*Andrä/Tischer,* I. Teil, 1. Kapitel, Rn. 30.
1058 BeckOK-StPO/*Gerhold,* § 94 Rn. 3.
1059 BeckOK-StPO/ *Gerhold,* § 94 Rn. 3 mit Verweis auf BVerfG NJW 2005, 1917 (1920).
1060 Meyer-Goßner/Schmitt/*Köhler,* § 94 Rn. 4 mit Verweis auf BVerfGE 124, 43.
1061 BVerfG NJW 2005, 1917 (1919f.). Vgl. *Michl*, NVwZ 2019, 1631 (1635).
1062 BVerfGE 124, 43ff. In diesem Fall liegt allerdings ein Eingriff in das Telekommunikationsgeheimnis vor.
1063 Vgl. hierzu bereits Kap. 4, B.II.2.c.)

Datenerhebung ermächtigt und nicht zu der bei den Auswertungsmethoden maßgeblichen Datenverarbeitung.[1064]

Dem lässt sich zwar entgegenhalten, dass von der Ermächtigung zur Beschlagnahme auch die Datenauswertung erfasst sein muss, da es widersprüchlich wäre, wenn etwa (besonders sensible)[1065] Daten zwar erhoben werden dürften, aber anschließend nicht ausgewertet werden dürften.[1066] Da außerdem typische Vorbereitungs- und Begleitmaßnahmen von den jeweiligen Ermächtigungsgrundlagen erfasst sind[1067], ließe sich möglicherweise argumentieren, dass § 94 StPO auch eine taugliche Ermächtigungsgrundlage für einen Eingriff in das RiS in Form der Datenverarbeitung darstellt.

Allerdings muss berücksichtigt werden, dass bei der Beschlagnahme nach § 94 StPO der maßgebliche Anknüpfungspunkt das „Verfügbarmachen" bzw. die Sicherung von Beweismitteln ist und ein staatliches Gewahrsamsverhältnis begründet werden kann.[1068] Die darüberhinausgehende Ermächtigung zur Auswertung der als Beweismittel erhobenen Daten stellt insoweit nur eine typische Begleiterscheinung der spezifischen Ermächtigungsgrundlage der Beschlagnahme dar.[1069]

Insoweit stellt die Auswertung der beschlagnahmten Beweismittel nur eine untergeordnete Rolle dar und der Schwerpunkt der Beschlagnahme liegt in der Begründung eines staatlichen Gewahrsamsverhältnisses – für elektronisch gespeicherte Daten also in deren Erhebung.[1070]

Dem entgegen stellt die Erhebung der jeweiligen Daten bei den hier gegenständlichen Auswertungsmethoden wohl nur einen untergeordneten Eingriff in das RiS dar. Maßgeblich ist erst die sich daran anschließende Auswertung.[1071] Der Schwerpunkt der Auswertungsmethoden liegt insoweit

1064 Vgl. SSW-StPO/*Eschelbach,* § 94 Rn. 1; Gercke/Julius/Temming/Zöller/*Gercke,* § 94 Rn. 24.
1065 Siehe hierzu etwa BVerfG NJW 2005, 1917 (1918f.).
1066 Vgl. insoweit BVerfG NJW 2005, 1917 (1918f.), das den Eingriff in das RiS insbesondere auch mit dem Zugriff auf die beschlagnahmten Daten begründet.
1067 Gercke/Julius/Temming/Zöller/*Gercke,* Vor. §§ 94 Rn. 5, der hierfür den Begriff der Annexkompetenz verwendet. Siehe zum Begriff der Annexkompetenz bei strafprozessualen Maßnahmen ausführlich *Ziemann,* ZStW 130 (2018), 762 (766f.), der insbesondere auf BGHSt 46,266; OLG Karlsruhe, StV 2009, 516 (517); LG Hamburg, wistra 2011, 155 (156) verweist.
1068 Meyer-Goßner/Schmitt/*Köhler,* § 94 Rn. 11ff.
1069 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* §§ 94 Rn. 24.
1070 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* §§ 94 Rn. 24.
1071 Siehe hierzu oben unter Kap 4, B.II.2.c).

in der Datenverarbeitung und nicht in deren Erhebung. Dementsprechend kann die gegenständliche Datenverarbeitung der Auswertungsmethode auch nicht als typische Begleiterscheinung der Datenerhebung angesehen werden.

Anders könnte dies allenfalls für das in Kap 3, C.I. dargestellte Durchsuchen des Internets nach der Zeichenstruktur von *Bitcoin-Adressen* mittels *Web-Crawler* gesehen werden.[1072] Denn hierbei liegt das Ziel der Auswertungsmethode eben auch in einer Datenerhebung. Allerdings ist in diesem Zusammenhang zu berücksichtigen, dass diese Datenerhebung erst durch eine automatisierte Datenverarbeitung ermöglicht wird. Denn die gesuchten Daten können nur dadurch erhoben werden, dass die im Internet verfügbaren Daten, automatisiert nach der besonderen Zeichenstruktur von *Bitcoin-Adressen* durchsucht werden. Insoweit liegt auch hierfür der Schwerpunkt der Ermittlungsmaßnahme auf der Datenverarbeitung und nicht in deren Erhebung.

b) Keine Minus-Maßnahme der Beschlagnahme

Ferner ließe sich zwar zunächst anführen, dass die Auswertungsmethoden insoweit nur eine sog. *Minus*-Maßnahme zur Beschlagnahme darstellen könnten, da sie die nur einen Teil der gesetzlichen Ermächtigungsgrundlage (Datenverarbeitung) betreffen und insoweit die Ermächtigungsgrundlage nicht voll ausgeschöpft sei.[1073] Dem lässt sich allerdings entgegenhalten, dass der Schwerpunkt beider Ermittlungsmaßnahmen, wie soeben dargestellt, weit auseinandergeht. Denn die Auswertungsmethoden betreffen die Gewinnung von Ermittlungsansätzen und Beweisen durch die Auswertung von öffentlich verfügbaren Daten, die Beschlagnahme soll dagegen Beweismittel in Form von Sachen und Daten zur Strafverfolgung verfügbar machen. Daher stellen die Auswertungsmethoden ein *Aliud* und kein *Minus* im Vergleich zur Beschlagnahme dar.

Darüber hinaus liegt ein wesentlicher Unterschied der gegenständlichen Auswertungsmethoden zu der Beschlagnahme darin, dass die Beschlagnah-

1072 Siehe zur Funktionsweise ausführlich oben unter Kap. 3, C.I.

1073 Siehe zur Zulässigkeit solcher Minus-Maßnahmen Gercke/Julius/Temming/Zöller/*Gercke,* Vor. §§ 94 ff. Rn. 5.

me eine sog. *offene* Ermittlungsmaßnahme ist, da sie den Betroffenen und Verfahrensbeteiligten bekannt zu machen ist.[1074]

Offene und verdeckte bzw. heimliche Ermittlungsmaßnahmen lassen sich grundsätzlich wie folgt voneinander abgrenzen, wobei in der Literatur die Begriffe der heimlichen und verdeckten Ermittlungsmaßnahmen teilweise synonym verwendet werden[1075]:

Offene und *heimliche* bzw. *verdeckte* Ermittlungsmaßnahmen unterscheiden sich jedenfalls darin, dass *heimliche* bzw. *verdeckte* Ermittlungsmaßnahmen dem Betroffenen nicht bekannt gegeben werden.[1076] Der Betroffene ist sich einer Ermittlungsmaßnahme daher nicht bewusst. Teilweise werden *heimliche* und *verdeckte* Ermittlungsmaßnahmen darüber hinaus noch dahingehend differenziert, dass *heimliche* Ermittlungsmaßnahmen solche sind, die für den Betroffenen nicht erkennbar sind und sonst der Ermittlungszweck auch nicht erfüllt werden könnte.[1077] Dagegen sind *verdeckte* Ermittlungsmaßnahmen solche, bei denen sich der Betroffene „bewusst ist, dass er Informationen von sich preisgibt, die möglicherweise Relevanz als Beweismaterial in potenziellen Strafverfahren gegen ihn besitzen"[1078], er sie aber im Vertrauen darauf preisgibt, dass sein Gegenüber nicht für staatliche Strafverfolgungsbehörden tätig ist.[1079]

Die hier gegenständlichen Auswertungsmethoden sind verdeckte Ermittlungsmaßnahmen, da dem Betroffenen hier nicht bewusst sein kann, dass er Gegenstand einer staatlichen Ermittlungsmaßnahme wird. Für die Annahme von *offenen* Ermittlungsmaßnahmen ließe sich argumentieren, dass ein Betroffener, der an einem Blockchain-Netzwerk teilnimmt, sich bewusst sein muss, dass die so verarbeiteten Daten von einem unbestimmten Personenkreis zur Kenntnis genommen werden können[1080] und daher auch von Strafverfolgungsbehörden zur Kenntnis genommen werden könnten. Dem steht jedoch entgegen, dass das bloße abstrakte Bewusstsein, dass eine unbestimmte Personenanzahl Daten zur Kenntnis nehmen kann, noch nicht zur Folge hat, dass sich jeder Betroffene konkret darüber bewusst ist, dass er Gegenstand einer staatlichen Ermittlungsmaßnahme ist. Insbesondere ließe sich so allenfalls nur argumentieren, dass möglicherweise

1074 LR-StPO/*Menges*, Vor § 94 Rn. 1, § 94 Rn. 14.
1075 *Zöller*, ZStW 124 (2012), 411 (419f.).
1076 *Zöller*, ZStW 124 (2012), 411 (419f.).
1077 *Zöller*, ZStW 124 (2012), 411 (419).
1078 *Zöller*, ZStW 124 (2012), 411 (419f.).
1079 *Zöller*, ZStW 124 (2012), 411 (419f.).
1080 Siehe hierzu bereits ausführlich oben unter Kap. 2, A.IV.

die Erhebung bzw. Kenntnisnahme der ausgewerteten Daten für den Betroffenen erkennbar sein kann. Maßgeblich ist hier jedoch wiederum nicht die Erhebung bzw. Kenntnisnahme der Daten, sondern die sich daran anschließende systematische Auswertung. Diese ist für den Betroffenen nicht erkennbar, sodass hier eine *verdeckte* Ermittlungsmaßnahme vorliegt.

Insoweit kann für die gegenständlichen Auswertungsmethoden auch keine Minus-Maßnahme zur Beschlagnahme angenommen werden.

c) Zwischenergebnis

Auf Grund der vorstehenden Unterschiede ist § 94 StPO nicht für die hier gegenständlichen Auswertungsmethoden einschlägig.

2. § 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien

In einem engen Zusammenhang zur Beschlagnahme nach § 94 StPO steht die Befugnis des § 110 StPO zur Durchsicht.[1081] § 110 StPO ermächtigt die Staatsanwaltschaft und ihre Ermittlungspersonen zunächst zur Durchsicht von Papieren einer Person, die von einer Durchsuchung betroffen ist. Gegenstand der Durchsicht können dabei aber nicht nur Papiere sein, sondern auch elektronisch gespeicherte Daten[1082], selbst, wenn diese auf einem räumlich getrennten Speichermedium gespeichert sind (§ 110 Abs. 3 StPO). Durchsicht bedeutet in diesem Zusammenhang, die Papiere „inhaltlich darauf zu prüfen, ob eine richterliche Beschlagnahme beantragt werden muss oder ggf. die Rückgabe […] zu veranlassen ist“[1083]. Dies gilt insoweit grundsätzlich auch für elektronisch gespeicherte Daten.[1084] Auf Grund der Größe von Datenbeständen, die eine vollständige vor Ort Sichtung ausschließen, wird nach § 110 StPO auch eine vollständige Mitnahme bzw. Spiegelung von möglicherweise beweiserheblichen Datenträgern als zulässig erachtet.[1085]

1081 Vgl. BeckOK-StPO/*Hegmann,* § 110 Rn. 6; Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 2 jeweils m.w.N.
1082 Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 1.
1083 BeckOK-StPO/*Hegmann,* § 110 Rn. 6; Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 2 mit Verweis auf OLG Frankfurt NStZ 1997, 74ff.; OLG Jena NJW 2001, 1290ff.; BVerfG WM 2009, 963ff.
1084 Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 2a.
1085 BVerfG NJW 2014, 3085 (3088); Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 2a.

Insoweit ist die Durchsicht eine Maßnahme vor der förmlichen Beschlagnahme bzw. ein „minus" zu ihr, um tiefere Grundrechtseingriffe zu vermeiden.[1086] Insoweit ermächtigt § 110 StPO grundsätzlich zu einem Eingriff in das RiS.[1087]

Fraglich ist jedoch wiederum, ob hiervon eine systematische Datenverarbeitung, wie sie bei den Auswertungsmethoden stattfindet, erfasst sein kann. Dem steht maßgeblich entgegen, dass die Durchsicht mit dem Ziel erfolgt, zu entscheiden, ob Daten förmlich beschlagnahmt werden sollen oder nicht. Insoweit erfolgt nur eine inhaltlich oberflächliche Prüfung. Ziel ist es lediglich, den Inhalt von Daten grob zu erfassen und auf seine Beweistauglichkeit zu prüfen.[1088] Dagegen liegt das Ziel der hier gegenständlichen Auswertungsmethoden nicht darin, aus vielen Daten bzw. Informationen die maßgeblichen herauszufiltern – wie bei der Durchsicht – sondern Ziel ist es, durch Verknüpfung von Daten Informationen zu erhalten, die über den Gehalt der jeweils einzelnen Information hinausgehen.[1089]

Außerdem setzt § 110 StPO dem Wortlaut nach voraus, dass Daten bei einer Durchsuchung gesichtet werden. Da die Auswertungsmethoden aber ohne einen räumlichen Zugriff auf die Wohnung eines Betroffenen erfolgen, ist § 110 StPO hier nicht anwendbar.

II. § 98a StPO – Rasterfahndung

Anwendbar könnte jedoch die Ermittlungsbefugnis des § 98a StPO zur sog. Rasterfahndung sein. § 98a StPO ermächtigt insbesondere zu einem Eingriff in das RiS in Form einer Datenverarbeitung – dem maschinellen Abgleich von personenbezogenen Daten mit anderen Daten.[1090]

Allerdings stellt sich die Frage, ob die Rasterfahndung, die im Kern darauf abzielt, einen sog. Verdächtigenkreis zu ermitteln, auch auf die hier gegenständlichen Auswertungsmethoden angewendet werden kann. Denn bei der Rasterfahndung wird der Verdächtigenkreis dadurch ermittelt, dass

1086 BeckOK-StPO/*Hegmann,* § 110; Löwe-Rosenberg/*Tsambikakis,* § 110 Rn. 1.
1087 Löwe-Rosenberg/*Tsambikakis,* § 110 Rn. 1.
1088 Vgl. BeckOK-StPO/*Hegmann,* § 110 Rn. 6; Meyer-Goßner/Schmitt/*Köhler,* § 110 Rn. 2 mit Verweis auf OLG Frankfurt NStZ 1997, 74ff.; OLG Jena NJW 2001, 1290ff.; BVerfG WM 2009, 963ff.
1089 Siehe hierzu bereits ausführlich Kap. 4, B.II.2.c).
1090 SSW-StPO/*Eschelbach/Jäger,* Vor. 98a ff. Rn. 2; SK-StPO/*Wohlers/Greco,* § 98a Rn. 4.

personenbezogene Daten mit anderen Daten maschinell abgeglichen werden, um bestimmte, möglichst wenige Personen als Schnittmenge von zuvor definierten Prüfungsmerkmalen zu ermitteln.[1091]

Bei den hier gegenständlichen Auswertungsmethoden werden dagegen einzelne oder mehrere Datensätze systematisch analysiert, um entweder die Anonymität der in der Blockchain enthaltenen Daten (teilweise) zu beseitigen bzw. um weitere Anhaltspunkte für die Identitätsermittlung zu erhalten oder um Transaktionen aufzudecken, die auf bestimmte Straftaten – wie etwa Geldwäsche – hindeuten. Andererseits könnte man annehmen, dass auch bei dieser systematischen Auswertung von Datensätzen ein maschineller Datenabgleich zur Feststellung eines Verdächtigenkreises vorliegt. Denn etwa bei der Ermittlung von bestimmten, strafrechtlich möglicherweise relevanten Transaktionsmustern werden insoweit *Entitäten* ermittelt, auf die die entsprechenden, zuvor definierten Prüfmerkmale zutreffen. Ebenso ließe sich etwa annehmen, dass durch die identitätsermittelnden Maßnahmen ebenfalls Personen ermittelt werden, auf die „bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale"[1092] zutreffen, da etwa das Merkmal „Absender einer bestimmten Bitcoin-Transaktion" durch die Auswertung ermittelt werden könnte.[1093]

Insoweit ist zwar möglicherweise der technische Hintergrund – der maschinelle Datenabgleich personenbezogener Daten mit anderen Daten – vergleichbar, es stellt sich aber die Frage, ob die Rasterfahndung des § 98a StPO auch auf die hier gegenständlichen Auswertungsmethoden anwendbar sein kann.

Dabei stellen sich für den Anwendungsbereich des § 98a StPO insbesondere folgende Einzelprobleme: so soll etwa der Anwendungsbereich auf den Abgleich von Daten mehrerer Speicherstellen begrenzt sein.[1094] Dies könnte insbesondere für die Auswertungsmethoden problematisch sein, deren Datengrundlage nur die Blockchain-Daten sind[1095]. Außerdem soll § 98a StPO nur für Daten anwendbar sein, die für die Strafverfolgungsbehörden fremd sind und entweder von einer Speicherstelle nach § 98a Abs. 2 StPO

1091 Hierzu im Einzelnen sogleich.
1092 So der Wortlaut des § 98a Abs. 1 Hs. 2 StPO.
1093 Vgl. KK-StPO/*Greven,* § 98a Rn. 32.
1094 SK-StPO/*Wohlers/Greco,* § 98a Rn. 4; BeckOK-StPO/*Gerhold,* § 98a Rn. 14 mit Verweis auf BVerfG NJW 2009, 1405 (1406).
1095 Siehe zu diesen Auswertungsmethoden ausführlich oben unter Kap. 3, A.

übermittelt werden oder freiwillig herausgegeben werden.[1096] Insoweit stellt sich die Frage, wie die hier gegenständlichen Daten, die öffentlich verfügbar sind und deren Erhebung nur teilweise überhaupt einen Eingriff in das RiS darstellt[1097], einzuordnen sind.

Um diese Abgrenzungsfragen zu beantworten, wird die Anwendbarkeit des § 98a StPO für die hier gegenständlichen Auswertungsmethoden wie folgt untersucht:

Zunächst werden die Historie und der praktische Einsatz des Ermittlungsinstruments der Rasterfahndung dargestellt (hierzu unter 1.). Anschließend wird auf das wesentliche Merkmal der Rasterfahndung – den maschinellen Datenabgleich – eingegangen (hierzu unter 2.). Daraufhin wird auf die problematische Rechtsprechung eingegangen, nach der keine Rasterfahndung vorliegen soll, wenn lediglich die Abfrage von nur einer Speicherstelle stattfindet – selbst, wenn diese hierzu einen maschinellen Abgleich ihrer Daten vornehmen muss (hierzu unter 3.). Ferner wird auf die Frage eingegangen, auf welcher Datengrundlage ein derartig maschineller Abgleich stattfinden muss (hierzu unter 4.).

1. „Herkömmliche" Rasterfahndung – Historie und Praxis

Die Ermächtigungsgrundlage des § 98a StPO ist historisch insbesondere im Zusammenhang mit den Terroristen der RAF und den Anschlägen des 11. September 2001 bekannt.[1098] Eingesetzt wurde das neuartige Ermittlungsinstrument der Rasterfahndung erstmalig im Rahmen der Suche nach den Terroristen der RAF.[1099] Gestützt wurde sie in diesem Zusammenhang noch auf die Ermittlungsgeneralklauseln der §§ 161, 163 StPO.[1100]

Bei der Suche nach den Terroristen der RAF vermutete man etwa, dass die Terroristen wohl möglichst wenig in Erscheinung treten wollten und

1096 KK-StPO/*Greven,* § 98a Rn. 26 mit Verweis auf BT-Drs. 12/989, S. 37, der ausdrücklich klarstellt, dass § 98a auch für freiwillig herausgegebene Daten anzuwenden sei; SK-StPO/*Wohlers/Greco,* § 98a Rn. 3; KMR-StPO/*Jäger,* § 98a Rn. 3; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 7; SSW-StPO/*Jäger,* § 98a Rn. 3.

1097 Siehe zur Frage, welche Maßnahmen der Auswertungsmethoden einen Eingriff in das RiS darstellen ausführlich oben unter Kap. 4, B.II.2.c).

1098 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 96.

1099 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 96.

1100 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 96, 115 m.w.N.; *Simon/Taeger*, JZ 1982, 140 (142).

daher entweder ihren Strom bar unter falschem Namen bezahlen würden oder die Bezahlung über ihren Vermieter abwickeln ließen.[1101]

Um Personen bzw. Wohnungen zu ermitteln, bei denen die Bezahlung über den Vermieter abgewickelt wurden, fragten die Strafverfolgungsbehörden einerseits bei Stromanbietern Kundendaten ab, bei denen die Rechnungs- und Verbrauchsanschrift voneinander abwichen.[1102] Die so erhobenen Daten, glich die Polizei mit weiteren personenbezogenen Daten ab[1103], die sie auf Grund ähnlicher Fahndungshypothesen erhalten hatte, und ermittelte so einen kleinen Verdächtigenkreis für weitere Ermittlungen.[1104]

Um Personen zu ermitteln, die ihre Stromrechnung bar unter falschem Namen bezahlten, wurden von den Stromanbietern Daten der barzahlenden Kunden abgefragt. Diese wurden dann mit den ebenfalls abgefragten Daten der Einwohnermeldeämter und der Sozialversicherungen abgeglichen, um Personen zu ermitteln, die wahrscheinlich unter falschem Namen auftraten.[1105]

Lediglich die Fahndungshypothese der bar zahlenden Stromkunden führte im Ergebnis zur Ergreifung des RAF-Terroristen Heißler.[1106] Die Fahndungshypothese der Zahlungsabwicklung über den Vermieter blieb erfolglos.[1107]

Diese Ermittlungsmethode fand im Anschluss Eingang in den Kanon der Ermittlungsinstrumente der Strafverfolgungsbehörden und wurde später zum 22.09.1992 in § 98a StPO durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (nachfolgend als „OrgKG“ bezeichnet) in die StPO aufgenommen.[1108]

1101 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 109f..
1102 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110; Löwe-Rosenberg/*Menges,* § 98a Rn. 9.
1103 Etwa mit den so ermittelten Rechnungsanschriften, sodass Sozialämter oder Pflegeheime aus den Datensätzen gestrichen wurden. Außerdem fand ein Abgleich mit den Daten der Einwohnermeldeämter statt. *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.
1104 Siehe hierzu im Einzelnen: *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.
1105 BeckOK-StPO/*Gerhold,* § 98a Rn. 12.
1106 BeckOK-StPO/G*erhold,* § 98a Rn. 12.
1107 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.
1108 BeckOK-StPO/*Gerhold,* § 98a Rn. 1.

Aus diesen Beispielen ergibt sich bereits der typische, dreischrittige[1109] Verfahrensablauf einer Rasterfahndung:

In einem ersten Schritt wird zunächst eine Fahndungshypothese aufgestellt.[1110] Bestimmt werden typische Faktoren, die vermutlich auf den Tatverdächtigen zutreffen.[1111] Damit wird das gesuchte Raster, nach dem die Daten überprüft werden sollen, festgelegt.[1112] Im Fall der Suche nach Terroristen der RAF etwa die Annahme, dass diese vermutlich die Bezahlung der Strombelieferung über ihren Vermieter abwickeln ließen oder bar bezahlten, um möglichst unauffällig zu bleiben.[1113]

In einem zweiten Schritt werden dann die für die Rasterung erforderlichen Daten erhoben – so etwa die Abfrage bei den Stromanbietern, bei welchen Kunden Rechnungs- und Lieferanschrift voneinander abweichen bzw. welche Kunden bar bezahlten.[1114] Hierbei muss die abgefragte Stelle zunächst die abgefragten Daten herausfiltern und in einer gesonderten Datei, dem sog. Report, ablegen.[1115] Je nach Umfang des jeweiligen Rasters und der darin enthaltenen Prüfungsmerkmale, können hier unterschiedlich viele Speicherstellen abgefragt werden.

In einem dritten Schritt, der den Kern der Rasterfahndung darstellt[1116], werden die so erhobenen Daten miteinander abgeglichen, um so eine gemeinsame Schnittmenge zu erhalten und so diejenigen Personen herauszufiltern, auf die alle zuvor festgelegten Merkmale zutreffen[1117] und die dann Gegenstand weiterer Ermittlungen werden können.[1118] Hierzu gibt es zwei Methoden: die positive und die negative Rasterfahndung.[1119] Bei der negativen Rasterfahndung werden die sog. „Nichttreffer" herausgefil-

1109 Der dreischrittige Verfahrensablauf ist vereinfacht, vgl. hierzu ausführlich *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 101ff.
1110 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 101f.
1111 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 101f.
1112 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 102.
1113 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.
1114 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 96, 102.
1115 BeckOK-StPO/*Gerhold,* § 98a Rn. 11.
1116 Siehe *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 103; BVerfG NJW 2009, 1405 (1406); OLG Stuttgart NStZ 2001, 158 (159).
1117 Bzw. nicht zutreffen, siehe sogleich.
1118 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 119.
1119 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 119; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 4; Löwe-Rosenberg/*Menges,* § 98a Rn. 8.

tert, also diejenigen Personen, auf die keine der Merkmale zutreffen.[1120] Dagegen werden bei der positiven Rasterfahndung diejenigen Personen ermittelt, auf die bestimmte Merkmale zutreffen.[1121] Insoweit werden auch die Suchkriterien bei den beiden Methoden unterschiedlich formuliert.[1122] Einerseits wird ein Personenkreis ermittelt, indem Personen ausgeschlossen werden, auf die bestimmte Kriterien zutreffen, wohingegen andererseits der Personenkreis ermittelt wird, indem nach Personen gesucht wird, auf die alle Kriterien zutreffen.[1123]

In diesen typischen Verfahrensablauf lassen sich die hier gegenständlichen Auswertungsmethoden grundsätzlich ebenfalls einordnen.

Denn auch bei den Auswertungsmethoden wird in einem ersten Schritt eine Auswertungshypothese aufgestellt. Bei den *Entitäts-Clustering*-Verfahren ist dies etwa die Hypothese, dass bei Transaktionen, bei denen mehrere *Inputs* von unterschiedlichen *Bitcoin-Adressen* stammen, diese *Bitcoin-Adressen* zu der gleichen *Entität* gehören.[1124] Bei den Auswertungen der Netzwerkverbindungen ist dies etwa die Hypothese, dass der Inhaber einer *Bitcoin-Adresse* bei einer neuen Transaktionsnachricht dieser *Bitcoin-Adresse* die IP-Adresse zuzuordnen ist, die diese Transaktionsnachricht als erste im Netzwerk versandt hat.[1125]

In einem zweiten Schritt werden die Daten erhoben, die zum Abgleich der im ersten Schritt festgelegten Prüfungsmerkmale erforderlich sind. Bei den *Entitäts-Clustering*-Verfahren sind dies etwa die in der Blockchain enthaltenen Transaktionsdaten und teilweise weitere verfügbare Daten.[1126] Bei den Auswertungen des Netzwerkverhaltens sind dies etwa die Daten über die Verbreitung von Transaktionsnachrichten im jeweiligen Blockchain-Netzwerk.[1127]

Die so erhobenen Daten werden dann in einem dritten Schritt auf die zuvor definierten Prüfmerkmale – wie etwa, dass mehrere *Inputs* einer

1120 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 120; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 4; Löwe-Rosenberg/*Menges,* § 98a Rn. 8.
1121 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 121; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 4; Löwe-Rosenberg/*Menges,* § 98a Rn. 9.
1122 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 121.
1123 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 121.
1124 Siehe hierzu und zu weiteren *Clustering* Verfahren im Einzelnen oben unter Kap. 3, A.
1125 Siehe hierzu im Einzelnen oben unter Kap. 3, B.
1126 Siehe hierzu im Einzelnen oben unter Kap. 3, A.
1127 Siehe hierzu im Einzelnen oben unter Kap. 3, B.

Transaktion von mehreren *Bitcoin-Adressen* stammen – abgeglichen, um so diejenigen Daten herauszufiltern, auf die die Prüfungsmerkmale zutreffen.[1128]

2. Maschineller Datenabgleich im Sinne des § 98a Abs. 1 StPO

Aus diesen Beispielen ergibt sich bereits, dass die Ermächtigungsgrundlage des § 98a typischerweise zu einem Eingriff in das RiS ermächtigt, der darin liegt, dass personenbezogene Daten technikgestützt bzw. maschinell mit anderen Daten abgeglichen werden, um so eine Schnittmenge von Personen zu erhalten, auf die bestimmte zuvor festgelegte Prüfungsmerkmale zutreffen. Maßgebliches Kriterium der Rasterfahndung ist dabei der maschinelle Datenabgleich, da auch jede herkömmliche Ermittlungsmethode zum Auffinden einer unbekannten, verdächtigen Person grundsätzlich auf der Suche nach Auffälligkeiten des Gesuchten beruht[1129], ein händischer Abgleich allerdings nicht die gleiche Menge an Daten verarbeiten kann.[1130]

Der wesentliche Unterschied der Rasterfahndung zu anderen Ermittlungsmethoden, um unbekannte Personen zu ermitteln, liegt damit im Umfang der abgleichbaren Daten auf Grund der technischen Möglichkeiten.[1131]

Daraus ergibt sich, dass ein maschineller Datenabgleich vorliegt, wenn Daten technikgestützt miteinander dahingehend abgeglichen werden, ob bzw. bei welchen Daten einzelne, mehrere oder keine der vorher zu bestimmenden Prüfungsmerkmale vorliegen und so eine gemeinsame Schnittmenge ermittelt werden kann.[1132]

Ob bei den hier gegenständlichen Auswertungsmethoden ein derartiger maschineller Datenabgleich vorliegt, hängt insoweit davon ab, ob eine Auswertung der Daten technikgestützt in der Weise stattfindet, dass Datenmengen nach Prüfmerkmalen abgeglichen werden, die händisch nicht abgeglichen werden können.

1128 Siehe hierzu im Einzelnen oben unter Kap. 3.

1129 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 111f.

1130 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 112.

1131 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 111f; vgl. KK-StPO/*Greven,* § 98a Rn. 22. So auch BT-Drs. 12/989 S. 37: dort wird von einer „Massendatenverarbeitung" gesprochen.

1132 Vgl. *Siebrecht*, Rasterfahndung, S. 125; BeckOK-StPO/*Gerhold,* § 98a Rn. 14; KK-StPO/*Greven,* § 98a Rn. 22ff.

Typischerweise ist das bei den hier gegenständlichen Auswertungsmethoden der Fall. Denn, soweit die unmittelbaren Blockchain-Daten etwa nach *Entitäts-Clustern* ausgewertet werden oder deren Transaktionsverhalten nach bestimmten Mustern abgeglichen werden, waren hiervon etwa insgesamt 380.000.000 Transaktionen und insgesamt 1.000.000.000 *Bitcoin-Adressen* betroffen.[1133]

Für die Auswertung der Netzwerkverbindung ist darüber hinaus eine Verbindung mit allen *nodes* erforderlich, um so zunächst zu erheben, wann welche Transaktionsnachricht von welcher IP-Adresse versendet wird. Zwischen September 2019 und September 2020 sind zur Bitcoin Blockchain etwa 113.050.000 Transaktionen hinzugekommen. Hierzu müssten zusätzlich noch die Daten zu den Zeitpunkten der Einzelverbindungen hinzugefügt werden. Ein händischer Abgleich dieser Datenmengen erscheint tatsächlich nicht möglich. Daher finden die bereits beschriebenen Auswertungsmethoden gerade durch die Anwendung bestimmter Algorithmen statt.

Vorstellbar ist allenfalls, dass eine händische Auswertung dahingehend vorgenommen wird, dass etwa bei einer einzelnen, verdächtigen *Bitcoin-Adresse* deren weitere Transaktionen durch händisches Anklicken durchsucht werden, um so weitere *Bitcoin-Adressen* dieser *Entität* zuordnen zu können. Allerdings erscheint selbst diese händische Auswertung teilweise unwahrscheinlich, wenn man davon ausgeht, dass bereits bei Entwicklung von Bitcoin die Empfehlung bestand, für jede neue Transaktion auch eine neue *Bitcoin-Adresse* verwendet werden sollte.[1134]

Ein technikgestützter Datenabgleich ist darüber hinaus auch für die sog. *Bloom-Filter-Attacks*[1135] erforderlich. Denn hierbei müssen alle bereits verwendeten *Bitcoin-Adressen* und deren *public keys* bei dem jeweiligen *SPV-Client* abgefragt werden, um ermitteln zu können, welche *Bitcoin-Adressen* zu einer IP-Adresse gehören. Bei der Menge der bisher verwendeten *Bitcoin-Adressen* ist dies händisch wohl nicht möglich.

Schließlich gilt dies auch für die Auswertung anderweitig verfügbarer Daten, da beim Einsatz von *Web-Crawlern* jedenfalls eine Software eingesetzt wird, die einen maschinellen Abgleich beinhaltet. Soweit darüber hinaus Dritt-Anbieter-Cookies und Standortdaten bei IoT-Blockchain-Anwendungen ausgewertet werden sollen, ist auf Grund deren Datenmengen wiederum nur der Einsatz von maschinellen Datenabgleichen möglich.

1133 Vgl. *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (5).
1134 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6.
1135 Siehe hierzu ausführlich oben unter Kap. 3, B.III.

Insoweit liegt bei allen hier gegenständlichen Auswertungsmethoden ein maschineller Datenabgleich vor.

3. Rasterfahndung nur beim Abgleich der Daten mehrerer Speicherstellen im Verantwortungsbereich der Strafverfolgungsbehörden

Problematisch für die Anwendbarkeit des § 98a StPO ist zunächst, dass nach Rechtsprechung und herrschenden Literaturauffassungen nur dann eine Rasterfahndung vorliegen soll, wenn ein Abgleich von Daten mehrerer Speicherstellen vorliegt.[1136] Hiernach soll die bloße Datenabfrage der Strafverfolgungsbehörden bei einer (privaten) Speicherstelle dann keine Rasterfahndung darstellen, wenn die abgefragten Daten nicht dazu erhoben werden, um sie mit weiteren Datenbeständen abzugleichen.[1137] Dies soll auch gelten, wenn die Speicherstellen zunächst ihre eigenen Datenbestände nach bestimmten Prüfungsmerkmalen durchsuchen müssen, um die von der Staatsanwaltschaft verlangten Daten herauszugeben.[1138]

Problematisch ist dies im Zusammenhang mit den hier gegenständlichen Auswertungsmethoden deshalb, weil sich diese teilweise auch nur auf einen einzelnen Datensatz – etwa lediglich auf die jeweiligen Blockchain-Daten[1139] – beziehen. Es findet daher teilweise kein Abgleich mehrerer Datensätze bei den hier gegenständlichen Auswertungsmethoden statt, sondern lediglich eine systematische Analyse eines einzelnen Datensatzes.

Da aber die von Rechtsprechung und Literatur vertretene Auffassung auch durchaus kritisch betrachtet werden kann und wird[1140], stellt sich zunächst die Frage, ob dieser Auffassung hier gefolgt werden soll.

Hierzu werden nachfolgend zunächst die maßgeblichen Entscheidungen der Rechtsprechung dargestellt (hierzu unter a), b), um anschließend kurz auf die herrschende Literaturauffassung (hierzu unter c)) und die Begründung des Bundestages (hierzu unter d)) einzugehen. Daraufhin wird auf abweichende Literaturauffassungen eingegangen (hierzu unter e)) sowie

1136 BVerfG NJW 2009, 1405 (1406); OLG Stuttgart NStZ 2001, 158 (159); OLG Köln NStZ-RR 2001, 31 (32); KK-StPO/*Greven,* § 98a Rn. 5; BeckOK-StPO/*Gerhold,* § 98a Rn. 14; SK-StPO/*Wohlers/Greco,* § 98a Rn. 4.

1137 So insbesondere BVerfG NJW 2009, 1405 (1406); OLG Stuttgart NStZ 2001, 158 (159); OLG Köln NStZ-RR 2001, 31 (32).

1138 BVerfG NJW 2009, 1405 (1406).

1139 Siehe hierzu insbesondere die in Kap. 3, A. dargestellten Auswertungsmethoden.

1140 Siehe hierzu etwa *Schaefer*, NJW-Spezial 2009, 280 (280); *Jahn*, Juristische Schulung 2009, 664 (665); *Petri*, StV 2007, 266 (268f.). Hierzu nachfolgend im Einzelnen unter Kap. 5, B.II.3.e).

eine kritische Würdigung der vorstehenden Ansichten abgegeben (hierzu unter f)). Nach einem eigenen Lösungsvorschlag (hierzu unter g)) und einem kurzen Zwischenergebnis (hierzu unter h)) wird dieser Lösungsvorschlag auf die hier gegenständlichen Auswertungsmethoden angewendet(hierzu unter h)).

a) BVerfG NJW 2009, 1405ff. – Abfrage von Kreditkartendaten

Das BVerfG beschloss in einer Entscheidung aus dem Jahr 2009, dass die „Abfrage von Kreditkartendaten, die sich auf eine konkret beschriebene Tathandlung“[1141] bezogen, zulässigerweise auf § 161 Abs. 1 StPO gestützt wurden und keine Rasterfahndung im Sinne des § 98a StPO vorliege, wenn die Staatsanwaltschaft von Kreditkartenunternehmen Kundendaten herausverlangte, die bestimmte Prüfungsmerkmale bzw. bestimmte Überweisungen enthielten.[1142] Dieser Entscheidung ging folgender Sachverhalt voraus:

Die Staatsanwaltschaft Halle verlangte im Rahmen eines Ermittlungsverfahrens wegen des Verdachts des Besitzes kinderpornographischer Schriften von Instituten, die Visa- und Mastercard-Kreditkarten herausgaben, nach § 161 Abs. 1 StPO Auskunft darüber, ob und welche Kunden seit dem 01.03.2006 eine Überweisung in Höhe von € 79,99 an eine philippinische Bank mit einer bestimmten „Merchant-ID“ vorgenommen hatten.[1143] Hintergrund war, dass für den Zugang zu einer Internetseite, die kinderpornographisches Material anbot, eine entsprechende Gebühr entrichtet werden musste.[1144] Die Kreditkartenunternehmen durchsuchten daraufhin die Kreditkartenbuchungen ihrer Kunden und übermittelten der Staatsanwaltschaft die „Treffer“.[1145]

In diesem Zusammenhang nahm das BVerfG an, dass die Rasterfahndung nicht die einschlägige Ermächtigungsgrundlage sei und auch keine mit der Rasterfahndung vergleichbare Eingriffsintensität vorgelegen habe, sondern das Auskunftsverlangen zulässigerweise auf die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO gestützt werden konnte.[1146]

1141 BVerfG NJW 2009, 1405 (Ls. 2).
1142 BVerfG NJW 2009, 1405 (Ls. 3).
1143 BVerfG NJW 2009, 1405 (1405).
1144 BVerfG NJW 2009, 1405 (1405f.).
1145 BVerfG NJW 2009, 1405 (1405f.).
1146 BVerfG NJW 2009, 1405 (1406).

Zur Begründung führte das BVerfG aus, dass keine Rasterfahndung vorliege, „wenn die Strafverfolgungsbehörde von privaten Stellen Auskünfte zu speziellen Täter Daten erhält, also nicht die Gesamtdaten zum weiteren Abgleich mit anderen Dateien übermittelt bekommt“[1147]. Denn „Kern der Rasterfahndung [sei] der Abgleich der herausgefilterten Datenbestände mehrerer Speicherstellen, der die Verknüpfung verschiedener Sachbereiche [ermögliche], um ein Persönlichkeitsprofil zu erstellen. Die Suchabfrage in Dateien derselben Speicherstelle [sei] keine Rasterfahndung“.[1148]

Außerdem sei die Eingriffsintensität der Übermittlung der von der Staatsanwaltschaft verlangten Daten auch nicht mit der einer Rasterfahndung vergleichbar, sodass § 98a StPO auch nicht entsprechend anwendbar sei.[1149] Denn bei der typischen Rasterfahndung wäre das Ziel das „Hinarbeiten“[1150] auf einen bestimmten Verdächtigenkreis durch den Abgleich mehrerer allgemeiner Merkmale.[1151] Hierbei würden in der Regel „auch zahlreiche unbeteiligte Personen, die zufällig bestimmte tätertypische Merkmale [erfüllten], zum Gegenstand der Überprüfung im Ermittlungsverfahren, obwohl im Übrigen keine tatsächlichen Anhaltspunkte für ihre Eigenschaft als Verdächtige [vorlägen]“[1152]. Dagegen würde bei der gegenständlichen Suchanfrage gezielt nach genau bezeichneten Personen gesucht werden, die mit hinreichender Wahrscheinlichkeit eine strafbare Handlung begangen hätten, sodass keine erhöhte Streubreite bestünde.[1153]

Das BVerfG führt insoweit im Wesentlichen zwei Argumente an: erstens ermögliche die Datenabfrage von nur einer Speicherstelle noch nicht das Erstellen eines Persönlichkeitsbildes. Dieses könne erst durch den Abgleich der Daten mehrerer, verschiedener Speicherstellen erstellt werden. Daher sei die bloß einzelne Abfrage einer Speicherstelle nicht so eingriffsintensiv wie die typische Rasterfahndung. Zweitens weise die hier gegenständliche Datenabfrage eine weit geringere Streubreite auf, da nur genau bezeichnete Daten übermittelt würden, bei deren Vorliegen bereits der Verdacht einer Straftat begründet sei. Anders, als bei der herkömmlichen Rasterfahndung

1147 BVerfG NJW 2009, 1405 (1406).
1148 BVerfG NJW 2009, 1405 (1406) mit Verweis auf die nachfolgend dargestellten Entscheidungen: OLG Stuttgart NStZ 2001, 158 (159); OLG Köln NStZ-RR 2001, 31 und weiteren Nachweisen.
1149 BVerfG NJW 2009, 1405 (1406f.).
1150 BVerfG NJW 2009, 1405 (1406).
1151 BVerfG NJW 2009, 1405 (1406).
1152 BVerfG NJW 2009, 1405 (1406f.).
1153 BVerfG NJW 2009, 1405 (1407).

würden insoweit keine umfassenden Datenbestände zur weiteren Auswertung übermittelt, sondern lediglich die Datenbestände, bei denen bereits der Verdacht einer Straftat vorgelegen habe.

b) OLG Stuttgart NStZ 2001, 158 f.; OLG Köln NStZ -RR 2001, 31f – Entschädigung für Auskunft durch Telekommunikationsanbieter

Ähnlich, aber bereits 9 Jahre vor dem Beschluss des BVerfG und in einem anderen Zusammenhang, entschieden bereits die Oberlandesgerichte Stuttgart und Köln, dass dann keine Rasterfahndung im Sinne des § 98a vorläge, wenn die abgefragten Daten „nicht zum Abgleich mit Datenbeständen anderer Speicherstellen bestimmt“[1154] waren.[1155]

Hintergrund beider Entscheidungen war die Frage danach, in welcher Höhe die Staatsanwaltschaft zur Entschädigung für die Übermittlung von bestimmten Telekommunikationsdaten verpflichtet sei.[1156] Die Staatsanwaltschaft verlangte jeweils bei den Telekommunikationsanbietern bestimmte Telekommunikationsdaten ihrer Kunden – einerseits die Herausgabe von Verbindungsdaten von Telekommunikation in einem bestimmten Gebiet zu einem bestimmten Zeitpunkt[1157] und andererseits die Herausgabe der Telekommunikationsdaten einer bestimmten Rufnummer in einem bestimmten Zeitraum[1158]. Um diese Daten übermitteln zu können, mussten die Telekommunikationsanbieter ihre Verbindungsdaten nach den entsprechenden Prüfungsmerkmalen durchsuchen.[1159] Daraufhin verlangten die Telekommunikationsanbieter Entschädigung nach der damals geltenden Vorschrift des § 17a Abs. 4 ZSEG, nach der eine Entschädigung vorgesehen war, wenn die Datenverarbeitungsanlage eines Dritten zum Zwecke einer Rasterfahndung genutzt wurde. Die Oberlandesgerichte entschieden übereinstimmend, dass die geforderte Entschädigung nicht zu erstatten sei, da die Datenverarbeitungsanlage der Telekommunikationsanbieter nicht zum Zwecke einer Rasterfahndung genutzt worden sei.[1160]

1154 So OLG Stuttgart NStZ 2001, 158 (159).
1155 So auch OLG Köln NStZ-RR 2001, 31 (32).
1156 OLG Köln NStZ-RR 2001, 31 (31); OLG Stuttgart NStZ 2001, 158 (158f.).
1157 OLG Stuttgart NStZ 2001, 158 (159).
1158 OLG Köln NStZ-RR 2001, 31 (31)
1159 OLG Köln NStZ-RR 2001, 31 (31); OLG Stuttgart NStZ 2001, 158 (159).
1160 OLG Köln NStZ-RR 2001, 31 (31); OLG Stuttgart NStZ 2001, 158 (158f.).

Denn die Rasterfahndung sei durch folgende Arbeitsschritte gekennzeichnet: „Recherche in elektronisch gespeicherten Datenbeständen mit Hilfe von Suchanfragen und Übernahme in separate Dateien; maschineller Abgleich der so herausgefilterten Datenbestände mehrerer Speicherstellen, um Personen zu ermitteln, die als Teile der Schnittmenge die nachgefragten Merkmale erfüllen und Personen auszuscheiden, die diese Merkmale nicht erfüllen."[1161] Da aber die Telekommunikationsanbieter hier keinen maschinellen Datenabgleich vorgenommen hätten, sondern lediglich ihren ohnehin vorhandenen Datenbestand nach den vorgegebenen Daten durchsucht hätten,[1162] und auch kein sonstiger Abgleich verschiedener Datenbestände im Anschluss an die Übermittlung stattgefunden hätte, läge keine zu einer Entschädigungspflicht führende Rasterfahndung vor.[1163]

Insoweit nahmen auch die Oberlandesgerichte Stuttgart und Köln an, dass die Rasterfahndung den maschinellen Abgleich von mehreren Datenbeständen miteinander voraussetze.[1164]

c) Herrschende Literaturauffassung

Die herrschende Auffassung in der Literatur übernimmt diese Argumentation der Gerichte weitgehend und geht davon aus, dass die „Recherche in einer Datenbank oder eine Suchabfrage bei Dateien derselben Speicherstelle"[1165] keine Rasterfahndung sei.[1166]

1161 OLG Köln NStZ-RR 2001, 31 (31).
1162 OLG Köln NStZ-RR 2001, 31 (31f.).
1163 OLG Köln NStZ-RR 2001, 31 (32).
1164 OLG Köln NStZ-RR 2001, 31 (31f.); OLG Stuttgart NStZ 2001, 158 (159).
1165 KK-StPO/*Greven,* § 98a Rn. 5 mit Verweisen auf die Rechtsprechung des OLG Stuttgart NStZ 2001, 158f. und OLG Köln NStZ-RR 2001, 31f; a.A. *Schaefer*, NJW-Spezial 2009, 280 (280); *Jahn*, JuS 2009, 664 (665); *Petri*, StV 2007, 266 (268f.). Zu diesen anderen Auffassungen nachfolgend unter Kap. 5, B.II.3.e).
1166 SK-StPO/*Wohlers/Greco,* § 98a Rn. 3f.; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 8; Vgl. BeckOK-StPO/*Gerhold,* § 98a Rn. 14; *Kahler,* Massenzugriff der StA auf Kundendaten, S. 37f. mit Verweis auf *Wittig,* JuS 1997, 961 (968).

d) Begründung des Bundestages

Darüber hinaus verwies insbesondere das BVerfG in seinem Beschluss auch auf die Ausführungen des Bundestages zur Begründung der Einführung des § 98a Abs. 1 S. 2 StPO.[1167]

Hierin führt der Gesetzgeber aus, die Regelung schließe nicht aus, dass „die speichernde Stelle, sofern dies nach den für sie geltenden Gesetzen zulässig sei, ihrerseits einen Datenabgleich [vornehme] und dann die Strafverfolgungsbehörden [unterrichte]. § 98a [erfasse] nur den Datenabgleich, der unter der Verantwortung der Strafverfolgungsbehörden vorgenommen [werde]“[1168].

e) Abweichende Literaturauffassungen

In Teilen der Literatur wurde diese Rechtsprechung aber auch kritisiert:

Schaefer etwa kommt zu dem Ergebnis, dass die Rechtsprechung des BVerfG nicht einleuchte. Die Behauptung, eine Rasterfahndung läge dann nicht vor, wenn eine Suchabfrage in Dateien derselben Speicherstelle vorliege, treffe nicht zu, da „die Daten sämtlicher Kreditkartenbesitzer in den strafrechtlichen Kontrollprozess gelangt“[1169] seien. Für den Betroffenen könne es keinen Unterschied machen, ob der Datenabgleich bei den Strafverfolgungsbehörden selbst stattfinde oder an einen Dritten ausgelagert werde.[1170]

Ähnlich kritisiert auch *Petri* die Rechtsprechung des BVerfG. Zunächst stellt *Petri* fest, dass das gegenständliche Auskunftsverlangen aus Sicht der Staatsanwaltschaft tatsächlich etwas anderes als die typische Rasterfahndung darstelle.[1171] Üblicherweise verlange die Staatsanwaltschaft von mehreren Speicherstellen Daten nach § 98a Abs. 2 StPO heraus, um diese dann anhand von Rasterkriterien abzugleichen.[1172] Abweichend von diesem typischen Vorgehen, würde die Staatsanwaltschaft im gegenständlichen Verfahren den Datenabgleich bereits bei der Speicherstelle vornehmen lassen.[1173]

1167 BVerfG NJW 2009, 1405 (1406).
1168 BT-Drs. 12/989, S. 37.
1169 *Schaefer*, NJW-Spezial 2009, 280 (280).
1170 *Schaefer*, NJW-Spezial 2009, 280 (280).
1171 *Petri*, StV 2007, 266 (268).
1172 *Petri*, StV 2007, 266 (268).
1173 *Petri*, StV 2007, 266 (268).

Petri stellt daran anschließend die Frage, ob dieser tatsächliche Unterschied aus Sicht der Staatsanwaltschaft auch einen Unterschied für den Betroffenen machen könne. Um diese Frage zu beantworten, zieht *Petri* zunächst einerseits § 98c StPO heran, der einen Beleg dafür darstelle, dass auch der interne Datenabgleich eine derart gesteigerte Grundrechtsintensität aufweise, dass eine spezielle gesetzliche Regelung erforderlich sei.[1174]

Außerdem sei auch die damals geltende Befugnis zur sog. Zielwahlsuche nach § 100g Abs. 2 StPO a.F.[1175] zu beachten. Hiernach konnte Auskunft darüber verlangt werden, „ob von einem Telekommunikationsanschluß Telekommunikationsverbindungen zu Beschuldigten einer Straftat mit erheblicher Bedeutung oder zu Kontaktpersonen solcher Beschuldigter hergestellt worden sind"[1176]. Wenn eine derartige Auskunft aus Sicht des Gesetzgebers einer besonderen Regelung bedürfe, müsse dies zumindest ähnlich auch für die Auskunft von Bankdaten gelten.[1177]

Darüber hinaus müsse nach *Petri* auch die Grundrechtsintensität des Auskunftsverlangens, die für einen besonderen Gesetzesvorbehalt spreche, berücksichtigt werden, da es für den Betroffenen keinen Unterschied mache, ob der Datenabgleich bei den Strafverfolgungsbehörden oder bei privaten Stellen durchgeführt werde.[1178]

Schließlich müsse berücksichtigt werden, dass aus Sicht des Betroffenen auch dann durch eine Datenverarbeitung ein hoheitlicher Eingriff vorliege, „wenn sie auf staatliche Veranlassung hin durch Private"[1179] erfolge.

1174 *Petri*, StV 2007, 266 (268).

1175 In der Fassung, die vom 01.01.2002 bis 31.12.2007 galt.

1176 *Petri,* StV 2007, 266 (268).

1177 *Petri,* StV 2007, 266 (268), der darauf abstellt, dass zwar die Daten über Telekommunikationsverbindungen durch Art. 10 Abs. 1 GG besonders geschützt seien, aber kein signifikanter Unterschied hinsichtlich der Vertraulichkeitserwartungen der Betroffenen bei Bankdaten bestünde.

1178 *Petri,* StV 2007, 266 (268).

1179 *Petri,* StV 2007, 266 (268) mit Verweis auf den Rechtsgedanken aus BVerfGE 10, 302 (327), worin das BVerfG feststellt, dass sich der Staat von seiner Grundrechtsbindung nicht dadurch befreien kann, dass er einen „Privatmann zur Wahrung seiner öffentlichen Aufgaben bestellt und ihm die Entscheidung über den Einsatz staatlicher Machtmittel überlä[ss]t."

f) Kritische Würdigung

Die vorstehend dargestellten herrschenden Auffassungen von Rechtsprechung und Literatur differenzieren zwischen dem bloßen Durchsuchen von Datenbeständen bei lediglich einer Speicherstelle, das keine Rasterfahndung darstellen soll, und der Rasterfahndung selbst, bei der die Daten mehrerer, unterschiedlicher Speicherstellen maschinell miteinander zum Abgleich gebracht werden.[1180] Diese Differenzierung wird damit begründet, dass die Eingriffsintensität in das RiS beim bloßen Durchsuchen von Datenbeständen geringer sei.[1181] Denn einerseits wäre die Rasterfahndung dadurch besonders eingriffsintensiv, dass es durch die Verknüpfung verschiedener Sachbereiche möglich sei, ein Persönlichkeitsbild zu erstellen.[1182] Andererseits sei die Rasterfahndung besonders eingriffsintensiv, da eine große Vielzahl Unbeteiligter Gegenstand der Ermittlungen würde und damit eine hohe Streubreite vorliege.[1183] Dies wäre bei der bloßen Durchsuchung von Datenbeständen nicht der Fall, da einerseits keine verschiedenen Sachbereiche verknüpft werden könnten und andererseits lediglich eine gezielte Suche nach bestimmten Personen stattfinden würde, die durch ihr Verhalten den Verdacht strafbaren Verhaltens bereits selbst gesetzt hätten.[1184]

Dieser Begründung ist nur in den jeweils verfahrensgegenständlichen Fällen zuzustimmen, sie ist aber nicht verallgemeinerungsfähig. Denn die geringe Grundrechtsintensität auf Grund der geringen Streubreite und der nicht bestehenden Möglichkeit, Persönlichkeitsbilder zu erstellen, beruht nicht darauf, dass nur eine Speicherstelle abgefragt bzw. durchsucht wird, sondern darauf, dass die abgefragten Daten dies nicht ermöglichten. Insoweit liegt der Grund für die geringe Grundrechtsintensität hier in der begrenzten Abfrage der Daten und nicht darin, dass die Daten nur von einer Speicherstelle erhoben wurden.[1185]

1180 Siehe hierzu insbesondere BVerfG NJW 2009, 1405 (1406).
1181 BVerfG NJW 2009, 1405 (1406).
1182 BVerfG NJW 2009, 1405 (1406).
1183 BVerfG NJW 2009, 1405 (1406f.).
1184 BVerfG NJW 2009, 1405 (1407).
1185 Vgl. *Petri,* StV 2007, 266 (269), der darauf abstellt, dass die nahezu hundertprozentige Trefferquote nur darauf zurückzuführen ist, dass im gegenständlichen Verfahren ungewöhnlich konkrete Rasterkriterien verwendet wurde und dies daher nur bedingt bei der Bewertung der Eingriffsintensität berücksichtigt werden könne.

(1) Erstellen von Persönlichkeitsbildern

Zwar ist dem BVerfG in seiner Entscheidung dahingehend zuzustimmen, dass bei der verfahrensgegenständlichen Suchabfrage nur ein geringer Teilbereich von Daten betroffen war, der gerade kein Persönlichkeitsprofil ermöglichte. Dies kann allerdings nicht verallgemeinerungsfähig für die Suchanfrage bei einer einzelnen Speicherstelle angenommen werden. Denn für das Erstellen eines Persönlichkeitsprofils dürfte es praktisch nicht darauf ankommen, ob Daten verschiedener Speicherstellen miteinander abgeglichen werden, sondern darauf, wie umfangreich die Datenbestände der einzelnen Speicherstellen sind und inwieweit diese bereits miteinander in Abgleich gebracht werden können. So lassen nämlich gerade Kreditkarten- und Kontodaten umfangreiche Rückschlüsse auf die Persönlichkeit des Einzelnen zu.[1186] So könnte etwa, wenn nach einer Person, die

- alleinstehend ist,
- zwischen 20-30 Jahre alt ist,
- in einer Großstadt zur Miete wohnt,
- Student ist,
- ein sportliches Interesse hat
- und sich überwiegend in der Innenstadt aufhält,

gesucht wird, durch die Abfrage folgender Daten bereits dieses Persönlichkeitsprofil ermittelt werden:

- Geburtsdatum: zwischen dem 31.08.1990 und 31.08.2000
- Anschrift: Postleitzahlen aller deutschen Großstädte
- Buchungen:
  - monatliche Abbuchungen zwischen dem jeweils 25. und 05. des Monats, eventuell mit Verwendungszweck „Miete“
  - (Halbjährliche) Abbuchungen, deren Empfänger eine Universität oder Hochschule ist
  - Monatliche Abbuchungen von insgesamt nicht mehr als € 300,00[1187], deren Empfänger Lebensmitteleinzelhändler sind

1186 Vgl. BVerfGE 118, 168 (185f.).

1187 Durchschnittlich haben im Jahr 2018 1 Personen-Haushalte € 212,00 für Lebensmittel pro Monat ausgegeben (vgl. die Berechnung des statistischen Bundesamtes, https://www-genesis.destatis.de/genesis/online?operation=previous&levelindex=3

- Mindestens eine Abbuchung im Jahr zugunsten eines Sportartikelherstellers, oder -händlers, und/oder monatliche Abbuchungen zugunsten eines Fitnessstudios oder Sportvereins,
- Mindestens 50% der Buchungen, bei denen der Standort bekannt ist (etwa beim Abheben von Bargeld), finden in Postleitzahlen des Innenstadtbereichs statt

Erforderlich wäre bei dieser Abfrage natürlich eine genauere Bezeichnung der jeweiligen Zahlungsempfänger. So dürfte es aber durchaus möglich sein, etwa die in Deutschland ansässigen Universitäten und Hochschulen gesammelt aufzulisten und so als Zahlungsempfänger abzufragen.[1188] Alternativ hierzu wäre es sogar möglich, alle IBAN aufzulisten, die für die Rückmeldung der Studierenden verwendet werden, da diese in der Regel von den Universitäten und Hochschulen auf ihren Internetseiten angegeben werden. Ebenso dürfte es möglich sein, Lebensmittelhändler bzw. deren gängige Marken- bzw. Firmenbezeichnungen gelistet aufzuführen.[1189] Schwieriger oder jedenfalls aufwändiger dürfte es sein, alle Sportartikelhersteller und -händler, sowie alle Fitnessstudios aufzuführen.[1190] Hierzu könnte allerdings die Handelsregister und möglicherweise auch Gewerberegister durchsucht werden, um eine derartige Auflistung zu erstellen. Zu beachten ist in diesem Zusammenhang insbesondere auch, dass manche Banken derartige Auswertungen der Kontobewegungen bereits automatisch, intern vornehmen, um ihren Kunden darzustellen, welche monatlichen Ausgaben sie für welche Zwecke nutzen.[1191]

Bei dieser beispielhaften Datenabfrage würden bereits die Kundendaten herausgegeben, auf die das zuvor definierte Persönlichkeitsprofil zutrifft.

&step=3&titel=Ergebnis&levelid=1602074882535&acceptscookies=false#abreadcrumb, letzter Abruf: 20. Dezember 2021).

1188 Siehe etwa die unmittelbar abrufbare Auflistung aller aktuell existenten, staatlichen und staatlichen anerkannten Hochschulen unter: https://de.wikipedia.org/wiki/Liste_der_Hochschulen_in_Deutschland (letzter Abruf: 20. Dezember 2021).

1189 Siehe etwa wiederum die unmittelbare Auflistung der größten deutschen Lebensmitteleinzelhändler unter: https://de.wikipedia.org/wiki/Liste_von_Lebensmitteleinzelhändlern (letzter Abruf: 20. Dezember 2021).

1190 Siehe aber hierzu etwa bereits die Auflistung der größten deutschen Fitnessketten unter https://de.statista.com/statistik/daten/studie/6793/umfrage/top-10-fitnessketten-nach-anlagenzahl/ (letzter Abruf: 20. Dezember 2021).

1191 Siehe etwa die Auswertung bei der ING-DiBa AG: https://www.ing.de/hilfe/online-services/analyse/ (letzter Abruf: 20. Dezember 2021).

Je nachdem, welche weiteren Prüfungsmerkmale bei einer derartigen Abfrage bestimmt werden können, kann dieses Persönlichkeitsprofil noch weiter spezifiziert werden. So könnte es etwa theoretisch möglich sein, Rückschlüsse auf die politische Einstellung zu erhalten, wenn etwa abgefragt wird, ob in regelmäßigen Abständen Buchungen zugunsten einer politischen Partei, einer der parteinahen Stiftungen oder Ähnlichem stattfinden. Ein ähnlicher Rückschluss – etwa auf die ökologisch bewusste Einstellung – wäre beispielsweise möglich, wenn das Verhältnis der Ausgaben für Reisen untereinander abgefragt wird. Konkret, wenn etwa die Buchungen zugunsten der Deutschen Bahn im Verhältnis zu den Buchungen zugunsten von Tankstellen oder Fluggesellschaften weit überwiegt.

Diese Beispiele sollen insoweit verdeutlichen, dass die Rückschlüsse, die aus der Abfrage von Kredit- und Kontodaten gezogen werden können, beliebig erweitert werden können – je nachdem, ob und wie konkret Daten und bestimmte Prüfungsmerkmale abgefragt werden.

Sie sind darüber hinaus nicht auf Kredit- und Bankinstitute beschränkt. Sie können etwa ebenso bei Internetkonzernen und anderen Unternehmen gelten. Denn gerade Internetkonzerne sammeln diese persönlichkeitsrelevanten Daten über ihre Nutzer, um derartige Persönlichkeitsbilder zu erstellen[1192].

Hieraus wird erkennbar, dass es für die Bildung von Persönlichkeitsbildern nicht darauf ankommt, ob mehrere Speicherstellen abgefragt werden, sondern darauf, welche Daten abgefragt werden und wie umfangreich die erhobenen Daten der Speicherstelle sind. Denn dem BVerfG ist zwar im Grundsatz zuzustimmen, dass die besondere Gefahr, dass Persönlichkeitsprofile erstellt werden, gerade auch darin liegt, dass Datensätze verschiedener Speicherstellen miteinander in Abgleich gebracht werden – so dürfte sich die Genauigkeit von Persönlichkeitsbildern besonders erhöhen, wenn nicht nur die oben beispielhaft genannten Kontodaten zur Verfügung stehen, sondern diese darüber hinaus beispielsweise mit den Daten über die Einkäufe des Einzelnen von den Lebensmitteleinzelhändlern kombiniert werden könnten. Allerdings schließt das nicht aus, dass derartige Persönlichkeitsbilder bereits anhand des Abgleichs der Daten von einzelnen Speicherstellen erstellt werden.

1192 Siehe etwa die teilweise erschreckend genauen Werbeeinstellungen von Google für ihre jeweiligen Nutzer: https://adssettings.google.com/authenticated?hl=de (letzter Abruf: 20. Dezember 2021).

Festzuhalten ist daher zunächst, dass es für die Erstellung von Persönlichkeitsbildern nicht darauf ankommt, ob Datenbestände mehrerer Speicherstellen miteinander abgeglichen werden, sondern darauf, welche Daten der jeweiligen Speicherstelle zur Verfügung stehen und nach welchen Prüfungsmerkmalen diese bereits abgefragt werden können. So kann das vom BVerfG herangeführte Argument, dass nur beim Abgleich mehrere Sachbereiche die Gefahr bestehe, dass Persönlichkeitsbilder erstellt werden, nur eingeschränkt gelten. Zwar ist dem BVerfG zuzustimmen, dass der Abgleich von Daten mehrerer Speicherstellen aus unterschiedlichen Sachbereichen wohl in der Regel die Gefahr der Erstellung solcher Persönlichkeitsbilder erhöht, dies schließt aber nicht aus, dass diese Gefahr nicht auch bei der Abfrage von nur einer Speicherstelle besteht.

Insofern wäre es außerdem widersprüchlich, wenn etwa wie im Beispiel der Suche nach Terroristen der RAF eine Rasterfahndung vorläge, wenn die Daten der Einwohnermeldeämter mit den Daten aller an den Hochschulen einer Stadt eingeschriebenen Studenten abgeglichen würden, aber keine Rasterfahndung vorläge, wenn bei Banken die Daten aller Kunden abgefragt würden, die in einer bestimmten Stadt leben und regelmäßig Studiengebühren entrichten. Das Ergebnis der Datenverarbeitung wäre insoweit das Gleiche, lediglich der Weg der Ermittlung ein anderer.

(2) Streubreite

Ähnlich muss dies auch für das vom BVerfG herangeführte Argument der geringen Streubreite der Suchabfrage gelten. Denn die geringe Streubreite der übermittelten Daten in dem Verfahren des BVerfG beruhte darauf, dass die Abfrage der Kundendaten sich auf genau bezeichnete Transaktionen bezog, deren Vorliegen bereits den Verdacht einer Straftat begründeten.[1193] Insoweit beruhte die geringe Streubreite nicht darauf, dass nur eine Speicherstelle abgefragt wurde, sondern darauf, dass nur spezifische Einzeldaten abgefragt wurden. Wenn dagegen die Kundendaten im soeben dargestellten Beispiel abgefragt würden, wäre auch hiervon eine große Anzahl Unbeteiligter betroffen. Dementsprechend kann es auch für das Argument der geringen Streubreite nicht darauf ankommen, dass nur eine Speicherstelle abgefragt wird, sondern darauf, welche Daten abgefragt werden.

1193 So insbesondere BVerfG NJW 2009, 1405 (1407); a.A. *Petri*, StV 2007, 266 (268).

In diesem Zusammenhang stellt sich außerdem die Frage, ob das BVerfG dies nach seiner Entscheidung zur automatisierten Kfz-Kennzeichenkontrolle nicht ohnehin anders bewerten würde. Denn hierin stellt das BVerfG ausführlich dar, dass auch diejenigen Kfz-Halter, die nach dem Abgleich mit der Fahndungsdatenbank als „Nichttreffer" ausgesondert werden, in ihrem RiS betroffen sind.[1194] Zur Begründung führt das BVerfG an, dass auch ein spezifisch verdichtetes Interesse an den „Nichttreffern" bestünde, da andernfalls die Maßnahme wirkungslos sei – Ziel der Maßnahme sei es gerade, alle Kfz auf einer bestimmten Strecke zu kontrollieren, um so die Treffer herauszufiltern.[1195] Daher würden die „Nichttreffer" zwar unmittelbar nach dem Abgleich mit der Fahndungsdatenbank spurenlos ausgesondert werden, es bestünde aber auch ein spezifisches Interesse an den „Nichttreffern", da nur durch die vollständige Erfassung aller Kfz die Maßnahme wirksam sei.[1196] Daher seien auch die als „Nichttreffer" ausgesonderten Kfz-Halter von der Maßnahme in ihrem RiS betroffen.[1197]

Nach dieser Rechtsprechung ließe sich annehmen, dass bei einer derartigen Abfrage von Kundendaten bei Kredit- und Bankinstituten, auch bereits die Personen in ihrem RiS betroffen sind, auf die die abgefragten Prüfungsmerkmale nicht zutreffen. Erforderlich ist allerdings, dass auch hier ein vergleichbar spezifisch verdichtetes Interesse an diesen ausgesonderten „Nichttreffern" besteht. Dies dürfte hier allerdings ebenfalls der Fall sein, da auch hier das Ziel der Maßnahme darin liegt, die „Treffer" herauszufiltern, um einen Verdächtigenkreis zu erhalten. Insoweit muss auch hier gelten, dass die Maßnahme nur dann wirkungsvoll ist, wenn alle Personen bzw. Daten nach den Prüfungsmerkmalen durchsucht werden.

Zu berücksichtigen ist in diesem Zusammenhang jedoch ein tatsächlicher Unterschied zwischen automatisierter Kfz-Kennzeichenkontrolle und Abfrage von Kreditkartendaten. Denn bei der automatisierten Kfz-Kennzeichen-Kontrolle findet eine unmittelbare staatliche Erhebung statt, bei der Abfrage der Kreditkartendaten, werden die bereits vom Kreditkartenunternehmen ohnehin erhobenen Daten lediglich nach einem Abgleich mit den

1194 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.; BVerfGE 150, 244 (266).

1195 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.; BVerfGE 150, 244 (267f.).

1196 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.; BVerfGE 150, 244 (267f.).

1197 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.; BVerfGE 150, 244 (268f.).

jeweiligen Prüfungsmerkmalen herausgegeben. Insoweit wurden von den Kreditkartenunternehmen keinerlei Nichttreffer an staatliche Stellen übermittelt. In diesem Zusammenhang kann allerdings der Rechtsgedanke der Rechtsprechung des BVerfG zur Zuordnung von dynamischen IP-Adressen entsprechend herangezogen werden.[1198] Denn hiernach ist bereits dann das Telekommunikationsgeheimnis betroffen, wenn die Zuordnung einer dynamischen IP-Adresse zu einer Person bei Telekommunikationsanbietern abgefragt wird, da hierzu der Telekommunikationsanbieter die jeweiligen Verbindungsdaten in einem Vorschritt auswerten muss.[1199] Insoweit kann nichts anderes dafür gelten, wenn Kreditkartenunternehmen in einem vorangegangenen Schritt die Kontodaten ihrer Kunden auswerten müssen, um die abgefragten Kundendaten herauszugeben.

Daher ließe sich nach der geänderten Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung vertreten, dass auch die „Nichttreffer" in ihrem RiS betroffen sind.

Aus diesem Grund hängt auch die geringe Streubreite nicht davon ab, ob nur die Datenbestände einer Speicherstelle abgefragt werden, sondern davon, auf welche Art und Weise die Daten abgefragt werden. Eine erhöhte Streubreite kann daher auch bei der Abfrage von nur einer Speicherstelle vorliegen.

(3) Gesetzesbegründung des Bundestages

Problematisch ist in diesem Zusammenhang jedoch die Begründung des Bundestages. Der Gesetzgeber äußert nämlich, dass die „Regelung [...] es andererseits nicht [ausschließe], daß die speichernde Stelle, sofern dies nach den für sie geltenden Gesetzen zulässig ist, ihrerseits einen Datenabgleich [vornehme] und dann die Strafverfolgungsbehörden [unterrichte]. § 98a [erfasse] nur den Datenabgleich, der unter der Verantwortung der Strafverfolgungsbehörden vorgenommen [werde]."[1200] Aus diesem Passus wird abgeleitet, dass auch der Gesetzgeber die einzelne Datenabfrage bei nur einer Speicherstelle nicht als Rasterfahndung ansehe, selbst wenn die Speicherstelle hierzu selbst einen Datenabgleich vornimmt.[1201]

1198 BVerfGE 130, 151ff.
1199 BVerfGE 130, 151 (182).
1200 BT-Drs. 12/989, S. 37.
1201 So etwa BVerfG NJW 2009, 1405 (1406).

Die Ausführungen der Gesetzesbegründung lassen allerdings auch eine andere Auslegung zu:

Denn der Gesetzgeber spricht lediglich davon, dass § 98a Abs. 1 S. 1 StPO es nicht ausschließe, dass die jeweilige Speicherstelle selbst einen Datenabgleich vornimmt und die Strafverfolgungsbehörden hiervon unterrichtet. Im Zusammenhang mit dem zweiten Satz, nach dem es maßgeblich um den Datenabgleich „unter der Verantwortung der Strafverfolgungsbehörden"[1202] geht, lässt sich dies insoweit auch dahin auslegen, dass die Speicherstellen zwar selbst einen Datenabgleich vornehmen *können*, dieser aber dann eine Rasterfahndung des § 98a Abs. 1 StPO darstellt, wenn er auf Veranlassung der Strafverfolgungsbehörden geschieht.[1203] Historisch lässt sich dieses Auslegungsergebnis darüber hinaus darauf stützen, dass im Jahr 1992 der Gesetzgeber die Abgrenzungslinie zwischen Auskunftsverlangen, gestützt auf die §§ 161a, 94, 98 StPO, und einer Rasterfahndung nach § 98a Abs. 1 S. 1 zum Ausdruck bringen wollte.[1204] Denn es ließe sich annehmen, dass der Gesetzgeber hiermit lediglich klarstellen wollte, dass auch dann ein nur auf §§ 161a, 94, 98 StPO gestütztes Auskunftsverlangen vorliegt, wenn sich das Auskunftsverlangen an eine private Stelle richtet, die ihre Daten nicht mehr – wie damals vielleicht üblich – in Papierform ablegt, sondern bereits elektronisch speichert und insoweit zunächst einen elektronischen Datenabgleich vornehmen muss, um die angeforderten Daten zu erhalten.

Da die Gesetzesbegründung insoweit nicht eindeutig ist, lässt sich auch vertreten, dass eine Rasterfahndung auch vorliegen kann, wenn nur Daten bei einer einzelnen Speicherstelle abgefragt werden.

(4) Abweichende Literaturauffassungen

Die bereits angesprochenen, abweichenden Literaturauffassungen[1205] kommen zwar ebenfalls zu dem Ergebnis, dass die mögliche, gesteigerte Grundrechtsintensität des Auskunftsverlangens im Fall des MIKADO-Beschlusses

1202 BT-Drs. 12/989, S. 37.

1203 Vgl. insoweit ähnlich *Petri,* StV 2007, 266 (268), der darauf abstellt, dass auch dann ein hoheitlicher Eingriff durch eine Datenverarbeitung vorliege, wenn diese auf staatliche Veranlassung hin stattfinde. Hierzu verweist *Petri* auf den Rechtsgedanken des BVerfG, dass sich der Staat nicht durch Beauftragung von Privaten seiner Grundrechtsbindung entziehen kann.

1204 Siehe zu diesem Problem sogleich unter Kap. 5, B.II.3.f).

1205 Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.3.e).

dazu führt, dass § 161 Abs. 1 StPO keine ausreichende Ermächtigungsgrundlage darstellt.[1206] Offen gelassen werden dabei allerdings die Fragen, ob stattdessen § 98a Abs. 1 StPO als Ermächtigungsgrundlage einschlägig sein kann und falls ja, wie in diesem Fall eine ausreichende Trennschärfe zwischen einem herkömmlichen Auskunftsverlangen und einer Rasterfahndung gewährleistet werden kann.[1207]

(5) Zwischenergebnis

Aus dem Vorstehenden lässt sich festhalten, dass sowohl die geringe Streubreite als auch die Gefahr der Bildung von Persönlichkeitsbildern nicht davon abhängen, ob eine oder mehrere Speicherstellen abgefragt werden, sondern davon, welche Daten abgefragt werden.

Insoweit ließe sich vertreten, dass § 98a Abs. 1 StPO auch einschlägig sein kann, wenn nur der Datenbestand einer Speicherstelle abgefragt wird, wenn die Speicherstelle zur Auskunft ihren Datenbestand maschinell nach den abgefragten Prüfungsmerkmalen abgleicht.

Dies würde allerdings zu dem bereits kurz angesprochenen Abgrenzungsproblem zwischen einem bloßen Auskunftsverlangen und einer Rasterfahndung bei der Abfrage von elektronischen Datenbeständen führen.

Denn insoweit müsste berücksichtigt werden, dass bereits jedes Durchsuchen eines Datenbestandes nach bestimmten Daten, wie etwa Name, Anschrift, Geburtsdatum etc. einen maschinellen Datenabgleich einer Speicherstelle darstellt, wenn die Daten nicht händisch anhand von Akten herausgesucht werden. Dies würde aber dazu führen, dass bereits immer dann eine Rasterfahndung mit ihren hohen Voraussetzungen vorläge, wenn lediglich etwa bei einer Bank die Kontodaten eines Kunden abgefragt würden. Denn hierzu müsste bereits der Datenbestand der Bank maschinell nach den jeweils abgefragten Daten abgeglichen werden. Dies würde zu dem widersprüchlichen Ergebnis führen, dass jedes Mal eine Rasterfahndung mit ihren hohen Voraussetzungen des § 98a Abs. 1 Hs. 2 StPO vorläge, wenn lediglich bei einer Speicherstelle ein elektronischer Datenbestand abgefragt werden würde.

1206 So insbesondere *Petri,* StV 2007, 266 (269); ähnlich *Schaefer*, NJW-Spezial 2009, 280 (280). Siehe zur Voraussetzung einer geringfügigen Grundrechtsintensität der Ermächtigungsgrundlage des § 161 Abs. 1 StPO ausführlich nachfolgend unter Kap. 5, D.II.

1207 Vgl. *Petri,* StV 2007, 266 (269); *Schaefer*, NJW-Spezial 2009, 280 (280).

Insoweit bietet die vom BVerfG herangezogene formale Abgrenzung eine höhere Trennschärfe zwischen einer bloßen Datenabfrage und einer Rasterfahndung. Problematisch an dieser formalen Abgrenzung ist jedoch, dass sie dem Sinn und Zweck der hohen Anforderungen der Rasterfahndung – dem Schutz des RiS – nicht gerecht wird, wenn bereits aus dem Datenbestand einer einzelnen Speicherstelle ein umfassendes Persönlichkeitsbild erstellt werden kann und durch den maschinellen Datenabgleich auch eine große Anzahl Unbeteiligter betroffen ist.

g) Lösungsvorschlag – Rasterfahndung nur dann, wenn personenbezogene Daten eines unbestimmten Personenkreises abgefragt werden

Um dieses Abgrenzungsproblem aufzulösen, bietet sich folgende Abgrenzung zwischen Rasterfahndung und Auskunftsverlangen an:

Eine Rasterfahndung liegt nur dann vor, wenn personenbezogene Daten einer *unbestimmten* Anzahl von Personen abgefragt werden, auf die bestimmte, zuvor definierte Prüfungsmerkmale zutreffen. Dagegen liegt ein Auskunftsverlangen vor, wenn nur Daten eines *bestimmten* oder *bestimmbaren* Personenkreises abgefragt werden.

Die Grenze zwischen Rasterfahndung und Auskunftsverlangen würde dann anhand der Frage verlaufen, ob die Daten einer konkret bezeichneten Person bzw. eines bereits identifizierbaren Personenkreises abgefragt werden oder ein zuvor noch unbestimmter Personenkreis abgefragt wird. Vereinfacht läge damit die Grenze bei der Frage, ob bereits eine verdächtige Person vorliegt oder ein Verdächtigenkreis erst zu ermitteln ist.

Eine Rasterfahndung läge damit beispielsweise vor, wenn alle personenbezogenen Daten abgefragt würden, bei denen etwa eine bestimmte Buchung in einem bestimmten Zeitraum vorliegt[1208]. Keine Rasterfahndung läge dagegen vor, wenn lediglich die Kontodaten einer oder mehrerer bestimmter Personen – also alle Buchungen in einem bestimmten Zeitraum – abgefragt werden würden[1209].

Problematisch an diesem Lösungsvorschlag könnte allerdings sein, dass sich das Problem der Abgrenzung nur in die Frage verlagert, ab wann

1208 Vgl. BVerfG NJW 2009, 1405 (1406); siehe hierzu bereits oben unter Kap. 5, B.II.3.e)(3).

1209 Gegen die natürlich aus einem anderen Grund bereits ein Tatverdacht bestehen muss.

ein identifizierbarer Personenkreis vorliegt. Denn insbesondere im bereits dargestellten Fall des BVerfG zur Abfrage von Kreditkartendaten[1210] ließe sich argumentieren, dass ja gerade die Daten von identifizierbaren Personen abgefragt werden – nämlich denjenigen, bei denen die entsprechende Buchung vorliegt.

Dieses Problem ließe sich allerdings anhand des Merkmals des maschinellen Datenabgleichs auflösen. Es ließe sich darauf abstellen, ob der Personenkreis nur durch einen maschinellen Datenabgleich der abgefragten Speicherstellen ermittelt werden kann oder auch durch einen händischen Datenabgleich ermittelt werden könnte. Denn beispielsweise die Prüfung aller Kontodaten nach einer oder mehreren bestimmten Buchungen dürfte händisch praktisch[1211] nicht möglich sein und nur durch einen maschinellen Datenabgleich möglich sein. Anders wäre dies dagegen beispielsweise, wenn nur der oder die Inhaber einer oder mehrerer Konten abgefragt werden. Dies wäre auch durch einen händischen Datenabgleich – bildlich gesprochen durch die Suche in einem Aktenarchiv – möglich.

Darüber hinaus ließe sich annehmen, dass ein Auskunftsverlangen nach § 161 Abs. 1 StPO wohl in der Regel vorliegt, wenn etwa die Umsätze oder Buchungen einer bestimmten Person abgefragt werden, wohingegen in der Regel eher eine Rasterfahndung vorliegt, wenn die Personen abgefragt werden, die bestimmte Umsätze oder Buchungen aufweisen.

Insoweit ließe sich das Vorliegen einer Rasterfahndung bei der Abfrage von nur einer Speicherstelle anhand von zwei Merkmalen festmachen, durch die eine ausreichende Trennschärfe gewährleistet werden kann:

- Bezieht sich die Datenabfrage auf einen bestimmten bzw. bestimmbaren Personenkreis (dann lediglich Auskunftsverlangen) oder auf einen noch unbestimmten Personenkreis (dann Rasterfahndung)?
- Könnte der bestimmbare Personenkreis auch durch einen händischen Datenabgleich ermittelt werden (dann Auskunftsverlangen) oder ist hierzu ein maschineller Datenabgleich erforderlich (dann Rasterfahndung)

Insoweit besteht nach dieser Variante einerseits eine ausreichende Trennschärfe dahingehend, dass eine Rasterfahndung dann vorliegt, wenn noch kein Verdächtiger bzw. kein Verdächtigenkreis feststeht und dieser durch die Ermittlungsmaßnahme anhand des maschinellen Datenabgleichs auf

1210 BVerfG NJW 2009, 1405ff.

1211 Dies trifft natürlich nicht zu, wenn theoretisch unbegrenzt viele menschliche Ressourcen für den händischen Datenabgleich bestehen.

bestimmte Prüfungsmerkmale ermittelt werden soll. Keine Rasterfahndung liegt dagegen vor, wenn lediglich die Daten einer einzelnen oder mehreren bestimmten oder konkret bestimmbaren Personen abgefragt werden. Andererseits gewährleistet sie auch einen ausreichenden Schutz des RiS und der unbeteiligten Personen, wenn nur eine Speicherstelle abgefragt wird.

h) Zwischenergebnis

Nach hier vertretener Auffassung liegt eine Rasterfahndung im Sinne des § 98a Abs. 1 Hs. 2 StPO auch bei der Abfrage von nur einer Speicherstelle vor, wenn hierdurch ein zuvor noch unbestimmter Personenkreis anhand von Prüfmerkmalen ermittelt wird. Unbestimmbar ist der Personenkreis dann, wenn er nicht durch einen händischen Datenabgleich bestimmt werden kann.

i) Anwendung dieser Abgrenzung für die hier gegenständlichen Auswertungsmethoden

Dementsprechend muss zunächst die Frage beantwortet werden, ob bei den hier gegenständlichen Auswertungsmethoden nach diesen Maßstäben insoweit eine Rasterfahndung vorliegen kann.

(1) Clustering-Verfahren aus Kap. 3, A.I., II.

Bei den in Kap. 3, A.I., II. dargestellten *Entitäts-Clustering*-Verfahren und Verfahren zum Aufdecken von auffälligem Verhalten wird nur ein einheitlicher Datensatz ausgewertet, nämlich die jeweiligen Blockchain-Daten.[1212] Ob insoweit hierfür § 98a Abs. 1 Hs. 2 StPO anwendbar ist, hängt daher davon ab, ob hierdurch ein unbestimmter Personenkreis ermittelt wird. Dies hängt vom konkreten Einsatz der *Clustering*-Verfahren ab. Denn die *Clustering*-Verfahren können eingesetzt werden, um entweder alle *Bitcoin-Adressen* zu *Entitäten* zu *clustern* – also die Blockchain-Daten insgesamt

1212 Hiervon nicht erfasst, sind die in Kap. 3, A.III. dargestellten Auswertungsmethoden zum Vergleich mit bekanntem Transaktionsverhalten, da hier insoweit eine weitere Datengrundlage – die Hintergründe von einzelnen Transaktionen – verfügbar ist.

auszuwerten – oder, um die *Entität* einer einzelnen *Bitcoin-Adressen* zu ermitteln.

Wenn also die *Clustering*-Verfahren eingesetzt werden, um insgesamt die dort enthaltenen *Bitcoin-Adressen* zu Entitäten zu gruppieren, wäre insoweit der Anwendungsbereich des § 98a Abs. 1 StPO eröffnet. Denn vor der Auswertung ist noch nicht klar, wie viele *Entitäten* hierdurch ermittelt werden und auf Grund der Masse der Transaktionsdaten ist die Bestimmung auch lediglich durch eine maschinelle Auswertung möglich.

Wenn die *Clustering*-Verfahren dagegen lediglich eingesetzt werden, um die *Bitcoin-Adressen* einer *Entität* zu ermitteln, steht dagegen der zu ermittelnde Personenkreis bereits fest – nämlich die hinter der *Entität* stehende(n) Person(en). Fraglich ist jedoch, wie es zu bewerten ist, dass durch die Auswertung eine noch nicht bestimmte Anzahl von *Bitcoin-Adressen* und damit von personenbezogenen Daten ermittelt wird. Zu berücksichtigen ist jedoch, dass die hohen Voraussetzungen des § 98a Abs. 1 StPO insbesondere davor schützen sollen, dass eine große Anzahl Unbeteiligter Gegenstand strafrechtlicher Ermittlungen werden. Dies ist aber hier nicht der Fall, denn die Auswertung bezieht sich zwar auf eine unbestimmte Anzahl von *Bitcoin-Adressen,* hiervon ist aber keine unbestimmte Anzahl von Personen betroffen, sondern lediglich die jeweilige *Entität,* deren *Bitcoin-Adressen* ermittelt werden sollen. Soweit daher die *Clustering*-Verfahren nur in Bezug auf eine *Bitcoin-Adresse* vorgenommen werden, ähnelt dies eher dem Durchsuchen eines Datenbestandes bezüglich eines einzelnen Kunden.

Für die *Clustering*-Verfahren des Kap. 3, A.I.,II. muss daher gelten, dass sie dann in den Anwendungsbereich der Rasterfahndung fallen, wenn sie eingesetzt werden, um die *Bitcoin-Adressen* der Blockchain insgesamt zu *Entitäten* zu gruppieren. Dagegen ist der Anwendungsbereich des § 98a StPO nicht eröffnet, wenn sie lediglich eingesetzt werden, um alle zu einer *Entität* gehörenden *Bitcoin-Adressen* und deren Transaktionen zu ermitteln.

(2) Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens

Bei den in Kap. 3, B.I., II. dargestellten Auswertungen des Netzwerkverhaltens und der Netzwerkverbindungen, stellt sich zunächst die Frage, ob überhaupt nur eine Speicherstelle betroffen ist. Denn auf den ersten Blick werden ja die IP-Adressen als Netzwerkdaten den *Bitcoin-Adressen* als Daten der Blockchain zugeordnet. Daher ließe sich auf den ersten Blick annehmen, dass hier mehrere Speicherstellen betroffen sind.

Zu berücksichtigen ist aber, dass bei dieser Auswertungsmethode ebenfalls eine einheitliche Datengrundlage vorliegt, da in einem ersten Schritt eine Verbindung mit allen *Full-nodes* aufgebaut wird, um so aufzeichnen zu können, wann von welchem *Full-node* welche Transaktionsnachricht im Netzwerk versandt und weitergeleitet wurde.[1213] Im zweiten Schritt werden diese Daten dahingehend ausgewertet, dass ermittelt wird, von welchem *Full-node* die Transaktionsnachricht zuerst versandt wurde. So kann die bereits in der weitergeleiteten Transaktionsnachricht enthaltene *Bitcoin-Adresse* der IP-Adresse des zuerst absendenden *Full-nodes* zugeordnet werden.[1214]

Insoweit wird für die Auswertung nur die einheitliche Datengrundlage der zuvor erhobenen Daten der Weiterleitungen der Transaktionsnachrichten verwendet, sodass sich auch hier die Frage stellt, ob hierdurch ein unbestimmter Personenkreis ermittelt wird.

Ob dies der Fall ist, hängt wiederum vom konkreten Einsatz der Auswertungsmethode ab. Denn, wenn etwa alle so erhobenen Daten danach ausgewertet werden, ob und welche *Bitcoin-Adressen* einer IP-Adresse zugeordnet werden können, liegt insoweit die Ermittlung eines unbestimmten Personenkreises vor, der wiederum auf Grund der Menge an abzugleichenden Daten nur maschinell vorgenommen werden kann.

Anders wäre dies allerdings wiederum zu beurteilen, wenn die Auswertungsmethode nur dazu eingesetzt wird, um nach Möglichkeit eine einzelne oder mehrere *Bitcoin-Adressen* jeweils einer IP-Adressen zuzuordnen. Denn dann wäre das Ziel der Auswertungsmethode wiederum nicht, einen unbestimmten Personenkreis zu ermitteln, sondern lediglich die IP-Adresse einer bestimmten Person bzw. *Entität* zuzuordnen. In diesem Fall wäre dann der Anwendungsbereich des § 98a Abs. 1 StPO nicht eröffnet.

Ähnlich gilt diese differenzierte Bewertung auch bei den in Kap. 3, B.III. dargestellten *Bloom-Filter-Attacks.* Denn, soweit sie insgesamt bei allen möglichen *SPV-Clients* eingesetzt werden, um möglichst viele *Bitcoin-Adressen* einer IP-Adresse zuzuordnen, liegt insoweit wiederum die Ermittlung eines unbestimmten Personenkreises vor. Dagegen wird dann kein unbestimmter Personenkreis ermittelt, wenn lediglich bei einem einzelnen oder mehreren einzelnen *SPV-Clients* deren *Bitcoin-Adressen* ermittelt werden, um so eine IP-Adresse zuordnen zu können. Zu berücksichtigen ist jedoch, dass es praktisch wohl in der Regel wenig sinnvoll ist, lediglich

1213 Siehe hierzu bereits ausführlich oben unter Kap. 3, B.I.
1214 Siehe hierzu bereits ausführlich oben unter Kap. 3, B.I.

die *Bitcoin-Adressen* eines *SPV-Clients* zu ermitteln, da ja in der Regel ein Tatverdacht im Zusammenhang mit einer *Bitcoin-Adresse* steht und deshalb deren Identität ermittelt werden soll und nicht andersherum.

(3) Auswertung anderweitig verfügbarer Daten

Bei den in Kap. 3, C. dargestellten Auswertungsmethoden von anderweitig verfügbaren Daten werden Daten mehrerer Speicherstellen abgefragt, sodass sie insoweit jedenfalls vom Anwendungsbereich des § 98a Abs. 1 StPO umfasst sind.

(4) Zwischenergebnis

Ob bei den hier gegenständlichen Auswertungsmethoden, bei denen nur ein einzelner Datenbestand systematisch analysiert wird, eine Rasterfahndung nach § 98a StPO vorliegen kann, hängt davon ab, ob sie in Bezug auf eine oder mehrere bestimmte Person(en) bzw. *Entität(en)* eingesetzt wird.

4. Datengrundlage der Rasterfahndung

Außerdem muss nach dem Wortlaut des § 98a Abs. 1 S. 1 StPO ein maschineller Abgleich von personenbezogenen Daten mit anderen Daten vorliegen.

a) Personenbezogene Daten im Sinne des § 98a Abs. 1 StPO

Zunächst ist festzustellen, dass die von den Auswertungsmethoden betroffenen Daten personenbezogene Daten im Sinne des § 98a Abs. 1 Hs. 2 StPO sind, da sich die Definition der personenbezogenen Daten mit den Begriffsbestimmungen aus Art. 3 Nr. 1 RL (EU) 2016/680 (nachfolgend „JI-RL") und Art. 4 Nr. 1 DSGVO nach der herrschenden Literaturauffassung deckt.[1215] Umfasst sind damit, wie bereits im Rahmen des Schutzbereichs

1215 Löwe-Rosenberg/*Menges,* § 98a Rn. 3, die auf die Begriffsbestimmung des Art. 4 Nr. 1 DSGVO abstellt; vgl. MüKo-StPO/*Günther,* § 98a Rn. 17; SSW-StPO/*Jäger,* § 98a Rn. 3.

des RiS herausgearbeitet, alle „Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen“[1216]. Insoweit gelten die obigen Ausführungen[1217] zur Frage, ob die von den Auswertungsmethoden betroffenen Daten personenbezogen sind[1218], hier entsprechend. Damit sind sämtliche, ausgewertete Daten personenbezogen im Sinne des § 98a Abs. 1 Hs. 2 StPO sind.

b) Andere Daten im Sinne des § 98a Abs. 1 StPO

Darüber hinaus ist aber fraglich, ob bei der Anwendung der Auswertungsmethoden auch ein maschineller Abgleich von personenbezogenen Daten mit *anderen* Daten vorliegt.[1219]

Insoweit ist fraglich, ob sich die hier gegenständlichen, überwiegend öffentlich verfügbaren Daten der Auswertungsmethoden in den Begriff der anderen Daten, die typischerweise bei der Rasterfahndung ausgewertet werden, einordnen lassen.

Um diese Frage zu beantworten, wird zunächst dargestellt, was nach der herrschenden Literaturauffassung andere Daten im Sinne des § 98a StPO sind (hierzu unter a)), um dies anschließend kritisch zu würdigen (hierzu unter b)) und schließlich nach einem kurzen Zwischenergebnis (hierzu unter c)) einordnen zu können, ob die von den Auswertungsmethoden betroffenen Daten hierunter fallen (hierzu unter d)).

(1) Herrschende Literaturauffassung

Die herrschende Literaturauffassung nimmt an, dass Gegenstand des maschinellen Datenabgleichs nach § 98a Abs. 1 StPO nur Daten sein können, die für die Strafverfolgungsbehörden in dem Sinne fremd sind, als dass sie vorher noch nicht bei den Strafverfolgungsbehörden verfügbar waren. Insoweit könnten Gegenstand des Abgleichs nur Daten sein, die zuvor nach § 98a Abs. 2 StPO übermittelt wurden oder die zuvor freiwillig her-

1216 Löwe-Rosenberg/*Menges,* § 98a Rn. 3; SSW-StPO/*Jäger,* § 98a Rn. 3.
1217 Siehe hierzu ausführlich unter Kap. 4, B.II.c).
1218 Siehe hierzu ausführlich oben unter Kap. 4, B.II.1.c).
1219 So der Wortlaut des § 98a Abs. 1 Hs. 2 StPO.

ausgegeben wurden.[1220] Der Anwendungsbereich der Rasterfahndung sei daher nicht eröffnet, wenn Daten ausgewertet würden, die zuvor auf Grund von anderen Ermittlungsbefugnissen erlangt wurden.[1221] Dies sei auch der Fall, wenn eine technikgestützte Auswertung von EDV-Daten(-trägern), wie etwa durch ein Datenbankprogramm, vorgenommen würde.[1222]

Teilweise wird aber vertreten, dass die Grenze zur Rasterfahndung dann überschritten sein soll, wenn schriftliche Informationen technikgestützt mittels Scannern und Texterkennungsprogrammen aufbereitet werden, in ein Datenbankformat umgewandelt werden und ausgewertet werden.[1223]

Schließlich soll die Rasterfahndung nicht einschlägig sein für Daten aus öffentlich verfügbaren Quellen wie dem Internet, da es hier an einem Eingriff in das RiS fehlen soll.[1224]

Der so bestimmte Anwendungsbereich der Rasterfahndung ergebe sich zunächst aus dem Wortlaut des § 98a Abs. 1 Hs. 2 StPO, der von einem maschinellen Datenabgleich „unbeschadet §§ 94, 110, 161" spricht.[1225]

Außerdem ergebe sich dies aus der Binnensystematik des § 98a StPO, da dieser eine eigenständige Pflicht zur Übermittlung an Speicherstellen statuiere. Insofern bestünde eine eigenständige, gesetzliche Regelung zur Erhebung von Daten zum Zwecke der Rasterfahndung nach § 98a StPO in Form der Übermittlung von Daten, die bereits anderweitig von den Speicherstellen erhoben wurden.

Weiterhin sei das systematische Verhältnis zu § 98c StPO zu berücksichtigen. Denn in § 98c StPO sei ebenfalls die Befugnis zu einem maschinellen Datenabgleich enthalten. Dieser maschinelle Datenabgleich sei aber an erhebliche geringere Voraussetzungen geknüpft. Denn er enthalte keine der Voraussetzungen des § 98a – also weder die Bindung an einen Straftatenkatalog noch eine Subsidiaritätsklausel noch das Erfordernis einer richterlichen Anordnung.[1226] Dabei dürften nach § 98c StPO „vorhandene

1220 KK-StPO/*Greven,* § 98a Rn. 26 mit Verweis auf BT-Drs. 12/989, S. 37, der ausdrücklich klarstellt, dass § 98a auch für freiwillig herausgegebene Daten anzuwenden sei; SK-StPO/*Wohlers/Greco,* § 98a Rn. 3; KMR-StPO/*Jäger,* § 98a Rn. 3; Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 7; SSW-StPO/*Jäger,* § 98a Rn. 3.
1221 SSW-StPO/*Jäger,* § 98a Rn. 4.
1222 KK-StPO/*Greven,* § 98a Rn. 4.
1223 KK-StPO/*Greven,* § 98a Rn. 4.
1224 SK-StPO/*Wohlers/Greco,* § 98a Rn. 4.
1225 KK-StPO/*Greven,* § 98a Rn. 4.
1226 Gercke/Julius/Temming/Zöller/*Gercke,* § 98c Rn. 5.

Daten“[1227] maschinell miteinander abgeglichen werden. Vorhandene Daten in diesem Sinne sind nach dem Wortlaut des Gesetzes „personenbezogene Daten aus einem Strafverfahren“ und „andere[…] zur Strafverfolgung oder Strafvollstreckung oder zu Gefahrenabwehr gespeicherte[…] Daten“[1228]. Davon erfasst sind insbesondere auch Daten, die bereits im Rahmen eines Strafverfahrens auf der Grundlage einer anderweitigen Ermittlungsbefugnis – wie etwa §§ 94, 161 ff. StPO – erhoben wurden.[1229] In Betracht kommen insoweit als Datengrundlage alle im Rahmen von Strafverfahren zusammengetragenen Daten.[1230] Dass § 98c StPO dabei bereits unter deutlich geringeren Anforderungen als der maschinelle Abgleich des § 98a StPO vorgenommen werden kann, wird damit begründet, dass lediglich „bevorratetes Wissen genutzt wird“[1231] und auch im Rahmen des § 98c StPO der Grundsatz der Verhältnismäßigkeit zu beachten sei.[1232]

Ferner wird der Wortlaut des § 98b Abs. 1 S. 1 StPO herangeführt, wonach „Der Abgleich und die Übermittlung der Daten […] nur durch das Gericht […] angeordnet werden“[1233] dürfen.[1234]

Da aber die Informationsverarbeitung durch Scanner und Texterkennungssoftware der Informationsverarbeitung einer Rasterfahndung schon sehr komme, seien die Grundsätze der Rasterfahndung hierfür entsprechend anzuwenden.[1235]

(2) Kritische Würdigung

i. Binnensystematik des § 98a StPO

Dem Argument der Binnensystematik des § 98a StPO lässt sich Folgendes entgegenhalten:

Zunächst ist zu berücksichtigen, dass die Ermächtigung zum maschinellen Datenabgleich und die Pflicht zur Übermittlung der erforderlichen

1227 So die amtliche Überschrift des § 98c StPO.
1228 So der Wortlaut des § 98c S. 1 StPO.
1229 SK-StPO/*Greco*, § 98a Rn. 3; SSW-StPO/*Jäger,* § 98a Rn. 4ff.
1230 SK-StPO/*Greco*, § 98a Rn. 3; SSW-StPO/*Jäger,* § 98a Rn. 4ff.
1231 Gercke/Julius/Temming/Zöller/*Gercke,* § 98c Rn. 5.
1232 Gercke/Julius/Temming/Zöller/*Gercke,* § 98c Rn. 5.
1233 § 98b Abs. 1 S. 1 StPO.
1234 MüKo-StPO/*Günther,* § 98a Rn. 8.
1235 KK-StPO/*Greven,* § 98a Rn. 4; BeckOK-StPO/*Gerhold,* § 98a Rn. 16.

Daten in zwei unterschiedlichen Absätzen geregelt ist. Dies lässt lediglich den Rückschluss zu, dass beide Ermächtigungen in einem Zusammenhang stehen, nicht aber, dass sie voneinander abhängig sind.[1236] Denn aus der getrennten Regelung beider Ermächtigungen lässt sich eher schließen, dass der maschinelle Datenabgleich auch ohne eine vorangegangene Übermittlung nach § 98a Abs. 2 StPO zulässig ist – andersrum ist dies auf Grund der Formulierung des § 98a Abs. 2 Hs. 1 StPO („Zu dem in Absatz 1 bezeichneten Zweck") jedoch nicht möglich.

Dies wird auch durch die systematische Stellung beider Ermächtigungen innerhalb des § 98a StPO unterstrichen. Denn, wie bereits dargestellt[1237], läuft eine Rasterfahndung in anderer Reihenfolge ab – es müssen zunächst die für den Abgleich erforderlichen Daten abgefragt und übermittelt bzw. verfügbar gemacht werden, um anschließend deren Abgleich vornehmen zu können. Innerhalb des § 98a StPO steht jedoch die Befugnis zum maschinellen Datenabgleich im ersten Absatz, die Möglichkeit die Übermittlung anzuordnen dagegen im zweiten Absatz.

Die Binnensystematik des § 98a StPO lässt daher eher den Rückschluss zu, dass die Ermächtigung zum maschinellen Datenabgleich nach § 98a Abs. 1 Hs. 2 StPO unabhängig von der Übermittlung nach § 98a Abs. 2 StPO besteht.

Hieran ändert auch ein Blick auf das systematische Verhältnis zu § 98b Abs. 1 StPO nichts. Denn der Wortlaut des § 98b Abs. 1 StPO stellt zwar auf den „Abgleich und die Übermittlung" ab, hieraus ergibt sich aber nicht zwangsweise, dass beide Maßnahmen nur in einem einheitlichen Zusammenhang angeordnet werden dürfen. So ließe sich der Wortlaut dem entgegen ebenfalls dahingehend auslegen, dass gerade beide Maßnahmen selbständig und unabhängig voneinander genannt werden und gerade nicht einheitlich auf die Maßnahme der Rasterfahndung abgestellt wird.

Aus der Binnensystematik des § 98a StPO und dem Verhältnis zu § 98b Abs. 1 StPO ergibt sich daher lediglich, dass der Anwendungsbereich der Rasterfahndung nicht auf die nach § 98a Abs. 2 StPO übermittelten Daten beschränkt ist.

1236 Vgl. insbesondere BT-Drs. 12/989, S. 37.
1237 Siehe hierzu bereits unter Kap. 5, B.II.1.

ii. Systematisches Verhältnis zu § 98c StPO

Eine Begrenzung des Anwendungsbereichs der Rasterfahndung nach § 98a StPO ergibt sich aber aus dem systematischen Verhältnis zu § 98c StPO dahingehend, dass der Anwendungsbereich des § 98a StPO nicht eröffnet ist, wenn lediglich Daten maschinell ausgewertet werden, die bereits auf der Grundlage einer anderen Ermittlungsbefugnis erhoben wurden. Denn, wenn nach § 98c StPO der maschinelle Abgleich von Daten, die zuvor auf Grund anderer Ermittlungsbefugnisse erhoben wurden, ohne die Anforderungen eines Straftatenkatalogs, einer richterlichen Anordnung und einer Subsidiaritätsklausel zulässig ist, lässt dies den Rückschluss zu, dass die Intensität des Eingriffs durch einen maschinellen Abgleich von bereits vorhandenen Daten deutlich geringer ist. Insoweit trifft das von herrschenden Literaturauffassung herangeführte Argument des systematischen Verhältnisses zu § 98c StPO zu. Dies unterstreicht auch der Wortlaut des § 98a Abs. 1 Hs. 2 StPO.

iii. EDV-gestützte Auswertung von Informationen

Unklar ist dagegen jedoch die von der herrschenden Literaturauffassung vertretene Differenzierung, dass einerseits eine technikgestützte Auswertung von nach §§ 94, 110, 161 StPO erlangten EDV-Datenträgern nicht der Rasterfahndung unterfallen soll, § 98a StPO aber dann anwendbar sein soll, wenn gedruckte Informationen durch den Einsatz von Scannern und Texterfassungsprogrammen in ein Datenbankformat umgewandelt werden können. Denn soweit das Verhältnis zu § 98c StPO und der Wortlaut des § 98a Abs. 1 Hs. 2 StPO dafürsprechen, dass Daten, die auf einer anderen Ermächtigungsgrundlage erhoben wurden, maschinell abgeglichen werden können, ohne, dass die Voraussetzungen der §§ 98a, 98b StPO erfüllt sein müssen, kann die Erfassung und Aufbereitung von schriftlichen Informationen durch Scanner und Texterkennungsprogramme hieran nichts ändern. Hierin liegt insoweit nur eine weitere Datenverarbeitungsmaßnahme. Es ist nicht erkennbar, inwieweit dieser Datenverarbeitungsschritt über die Auswertung von beschlagnahmten EDV-Daten hinausgehen soll – ob nun EDV-Daten technikgestützt ausgewertet werden oder haptische Informationen technikgestützt ausgewertet werden, dürfte insbesondere mit Blick auf das Verhältnis zu § 98c StPO und Wortlaut des § 98a Abs. 1 Hs. 2 StPO keinen Unterschied machen.

Allenfalls ließe sich die von der Literatur vertretene Auffassung dahingehend verstehen, dass eine Rasterfahndung dann nicht vorliegen soll, wenn die Auswertung von EDV-Daten händisch vorgenommen wird, die Verwaltung der Daten dabei aber durch technische Unterstützung gewährleistet wird. Konkret würde das bedeuten, dass keine Rasterfahndung vorliege, wenn beschlagnahmte EDV-Daten händisch von Polizeibeamten durch das „Anklicken, Öffnen und Ansehen" von Dateien gesichtet werden und hierzu lediglich eine Software genutzt wird, in der die gesichteten Daten verwaltet werden.[1238] Dagegen könnte eine Rasterfahndung vorliegen, wenn die EDV-Daten softwaregestützt systematisch ausgewertet werden – etwa mittels einer Schlagwortsuch bei großen Datenbeständen, die händisch nicht geleistet werden kann.

Problematisch an diesem Verständnis ist jedoch weiterhin der Widerspruch zum systematischen Verhältnis zu § 98c StPO. Denn, wenn eben auch ein maschineller Datenabgleich von etwa bereits beschlagnahmten Daten nach § 98c StPO zulässig ist, wäre es insoweit nicht nachvollziehbar, weshalb lediglich bestimmte maschinelle Datenverarbeitungsmaßnahmen unter die Privilegierung des § 98c StPO fallen sollten und andere Datenverarbeitungsmaßnahmen nur nach § 98a StPO zulässig sein sollten.

Insoweit ist die von der Literatur vertretene Auffassung einer Differenzierung danach, welche Form eines maschinellen Datenabgleichs vorgenommen wird, abzulehnen. Es ist mit Blick auf das Verhältnis zu § 98c StPO nicht nachvollziehbar, weshalb die Abgrenzung von § 98a Abs. 1 StPO und § 98c StPO anhand des bei beiden Vorschriften gleich lautenden Merkmals des maschinellen Datenabgleichs vorgenommen werden soll.

iv. Auswertung öffentlich verfügbarer Daten

Soweit die Literaturauffassungen annehmen, dass § 98a StPO für die Auswertung öffentlich verfügbarer Daten im Internet mangels Grundrechts-

1238 Eine solche, von den Strafverfolgungsbehörden etwa genutzte Software ist beispielsweise der „X-Ways-Investigator" (vgl. https://www.x-ways.net/investigator/index-d.html letzter Abruf: 20. Dezember 2021). Mit dieser Software können etwa die Dateien auf beschlagnahmten und gespiegelten Datenträger gesichtet werden. Die Verwendung derartiger Programme ist insbesondere zu späteren Beweiszwecken sinnvoll, da eine solche Software insbesondere automatisch die einzelnen Datenverwaltungsschritte protokolliert und so gewährleistet wird, dass die ursprünglich beschlagnahmten Daten nicht verändert werden.

eingriff nicht gelten kann, sind dem insbesondere die Entscheidung des BVerfG zum Online-Durchsuchungsgesetz NRW[1239] und die obigen Ausführungen zu Eingriffen in das RiS bei öffentlich verfügbaren Daten entgegenzuhalten.[1240] Da auch bei der Erhebung und Auswertung öffentlich verfügbarer Daten ein Eingriff in das RiS vorliegen kann, kann insoweit die Anwendung von § 98a StPO nicht pauschal ausgeschlossen werden.

v. Zwischenergebnis

Lediglich das systematische Verhältnis zwischen § 98a StPO und § 98c StPO führt zu einer Begrenzung der Datengrundlage der Rasterfahndung nach § 98a StPO. Hieraus ergibt sich, dass die Rasterfahndung nach § 98a StPO nur dann einschlägig ist, wenn die zur Rasterfahndung verwendeten Daten nicht bereits zuvor auf der Grundlage einer anderen Ermittlungsbefugnis erhoben wurden.

Für dieses Ergebnis kann allerdings nicht die Binnensystematik des § 98a StPO herangeführt werden.

Die darüber hinaus vertretene Anwendung von § 98a StPO für bestimmte Datenverarbeitungsmaßnahmen bei der EDV-gestützten Auswertung von – auch schriftlichen – Informationen ist auf Grund des systematischen Verhältnisses zwischen § 98a und § 98c StPO abzulehnen.

(3) Zwischenergebnis

Der Anwendungsbereich des maschinellen Datenabgleichs nach § 98a Abs. 1 StPO ist nicht auf den Abgleich von Daten beschränkt, die zuvor nach § 98a Abs. 2 erhoben wurden. Erfasst sind insbesondere auch freiwillig herausgegebene Daten. Dies ergibt sich aus der Binnensystematik des § 98a StPO und dem Verhältnis zu § 98b Abs. 1 S. 1 StPO. Der Anwendungsbereich von § 98a Abs. 1 StPO ist jedoch nicht eröffnet bei Daten, die bereits auf der Grundlage einer anderen Ermächtigungsgrundlage erhoben wurden. § 98a Abs. 1 StPO betrifft insoweit nur Daten, die für die Strafverfolgungsbehörden bisher fremd – also noch nicht verfügbar – waren. Dies ergibt sich aus dem Verhältnis zu § 98c StPO.

1239 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1).
1240 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(3).

(4) Daten der Blockchain-Auswertungsmethoden als andere Daten im Sinne des § 98a Abs. 1 StPO

Insoweit stellt sich für die Eröffnung des Anwendungsbereichs des § 98a Abs. 1 StPO die Frage, ob die Daten, die von den gegenständlichen Auswertungsmethoden betroffen sind, andere Daten nach den soeben definierten Maßstäben sind.

Zunächst dürften die ausgewerteten Daten daher also noch nicht bei den Strafverfolgungsbehörden verfügbar sein. Problematisch ist dies insoweit, als dass dies von den Umständen des jeweiligen Einzelfalls abhängen dürfte. Denn maßgeblich ist insoweit, ob etwaige Daten etwa bereits in einem anderen Zusammenhang auf der Grundlage einer gesetzlichen Ermittlungsbefugnis erhoben wurden. Dies kann daher nicht einheitlich beantwortet werden. Deshalb muss für die folgende rechtliche Bewertung davon ausgegangen werden, dass etwa die Daten bei den Strafverfolgungsbehörden noch nicht verfügbar waren und insoweit fremd sind.

Dementsprechend stellt sich die Frage, ob die gegenständlich ausgewerteten Daten entweder Daten sind, die freiwillig herausgegeben wurden oder nach § 98a Abs. 2 StPO übermittelt wurden.

i. Öffentlich verfügbare Daten als freiwillig herausgegebene Daten?

In Betracht kommt hier zunächst, dass auf Grund der öffentlichen Verfügbarkeit der hier gegenständlichen Daten freiwillig herausgegebene Daten vorliegen.

Dem steht allerdings entgegen, dass mit freiwilliger Herausgabe wohl das zur Verfügung stellen für die Strafverfolgungsbehörden gemeint ist, nicht aber die Preisgabe an einen unbestimmten Personenkreis.

Es ließe sich zwar argumentieren, dass bei Daten, die einem unbestimmten Personenkreis zur Verfügung gestellt werden, auch die staatlichen Strafverfolgungsbehörden diese wie jeder Dritte zur Kenntnis nehmen können. Allerdings sind hier zwei Unterschiede zu berücksichtigen:

Einerseits geht die Erhebung und Speicherung von Daten in der Regel[1241] über die bloße Kenntnisnahme hinaus. Andererseits besteht ein tatsächlicher Unterschied zwischen der Preisgabe an einen unbestimmten Personenkreis und der freiwilligen Herausgabe an die Strafverfolgungsbehörden.

1241 Siehe hierzu etwa im Einzelnen zu der Erhebung der Inhaltsdaten von Blockchains unter Kap. 3, B.II.2.c)(1).

Denn bei der Preisgabe an einen unbestimmten Personenkreis geschieht auch dies in der Regel zu einem bestimmten Zweck – hier etwa zum Fortschreiben der Transaktionsdaten, die in der Blockchain enthalten sind, oder zur Telekommunikation der über das *Peer-To-Peer*-Netzwerk miteinander verbundenen *nodes*. Wenn diese Daten dagegen zum Zweck der Strafverfolgung erhoben und gespeichert werden, liegt insoweit ein anderer Zweck vor. Anders ist dies, wenn private oder öffentliche Speicherstellen gegenüber den Strafverfolgungsbehörden bewusst Daten zum Zwecke der Strafverfolgung herausgeben.

Daher lassen sich die Daten, die von den hier gegenständlichen Auswertungsmethoden betroffen sind, trotz ihrer öffentlichen Verfügbarkeit nicht als freiwillig herausgegebene Daten einordnen.

ii. Daten, die nach § 98a Abs. 2 StPO erhoben wurden?

Insoweit stellt sich die Frage, ob die ausgewerteten Daten solche sind, die nach § 98a Abs. 2 StPO übermittelt wurden.

Problematisch ist in diesem Zusammenhang, dass es bei den hier gegenständlichen Daten keine speichernde Stelle im herkömmlichen Sinne gibt. Denn soweit etwa die Blockchain-Daten betroffen sind, verfügt jeder *Full-node* über die vollständigen Blockchain-Daten und könnte als Speicherstelle eingeordnet werden. Insoweit ließe sich auf Grund des technischen Hintergrunds von Blockchain-Netzwerken, bei denen gerade die in der Blockchain enthaltenen Transaktionsdaten an alle Beteiligten Rechner versendet werden, zunächst vertreten, dass Daten von der Speicherstelle (etwa dem einzelnen *Full node*) im Sinne des § 98a Abs. 2 StPO übermittelt werden.

Allerdings setzt § 98a Abs. 2 StPO voraus, dass die Daten zum Zweck des § 98a Abs. 1 StPO und damit zum Zweck eines maschinellen Datenabgleichs zu Strafverfolgungszwecken übermittelt werden. Da aber die Transaktionsdaten der Blockchain, sowie Telekommunikationsdaten der Netzwerkverbindungen als auch die im Internet verfügbaren *Bitcoin-Adressen* oder anderweitigen Daten[1242] nicht zum Zweck der Strafverfolgung preisgegeben werden, ist jedenfalls diese Voraussetzung des § 98a Abs. 2 StPO nicht erfüllt.

1242 Siehe hierzu jeweils im Einzelnen oben unter Kap. 3, A., B., C.

Dementsprechend ist § 98a Abs. 2 StPO jedenfalls seinem Wortlaut nach nicht für die Erhebung und Speicherung der hier gegenständlich ausgewerteten Daten einschlägig.

iii. Entsprechende Anwendung des § 98a Abs. 2 StPO?

In Betracht käme daher lediglich eine entsprechende Anwendung des § 98a Abs. 2 StPO für die Erhebung öffentlich verfügbarer Daten.

Diese ließe sich etwa auf die Überlegung stützen, dass sowohl bei der Abfrage und Übermittlung von Daten gegenüber privaten Speicherstellen als auch bei der Erhebung von öffentlich verfügbaren Daten solche Daten, die ohnehin bereits angefallen und gespeichert wurden, lediglich zum Zweck eines maschinellen Datenabgleichs im Rahmen der Strafverfolgung verfügbar gemacht werden.

Es ließe sich insoweit argumentieren, dass der Grundrechtseingriff der Erhebung öffentlich verfügbarer Daten nicht über den der Übermittlung von bereits gespeicherten Daten hinausgeht, da in beiden Fällen jeweils nur Daten, die ohnehin bereits angefallen sind, für die Strafverfolgungsbehörden verfügbar gemacht werden. Denn soweit für die hier gegenständlichen Auswertungsmethoden Daten erhoben und gespeichert werden, sind diese öffentlich verfügbar und fallen daher bereits unabhängig von der Erhebung durch die Strafverfolgungsbehörden an. Durch die Speicherung werden sie daher ebenfalls nur für die Strafverfolgungsbehörden verfügbar gemacht – genauso wie bei der Übermittlung von anderen privaten oder öffentlichen Speicherstellen.

Dem steht allerdings die besondere, spezifische Bedeutung des Bestimmtheitsgrundsatzes im Rahmen von Eingriffen in das RiS entgegen. Denn hiernach ist bei „gestuften oder in verschiedene Eingriffe gegliederte Formen des Informationsaustausches“[1243] auf jede dieser Stufen eine hinreichende Bestimmtheit der gesetzlichen Grundlagen erforderlich. Aus dem Wortlaut eines „Übermittelns“ ergibt sich allerdings nicht klar und eindeutig, dass hiervon auch die Erhebung von öffentlich verfügbaren Daten erfasst sein soll. Vor dem Hintergrund, dass das RiS gerade auch davor schützen soll, dass der Betroffene nicht mehr überblicken kann, welche

1243 BVerfGE 130, 151 (202).

Daten der Staat über ihn erhoben hat[1244], kann insoweit der Wortlaut des „Übermittelns" nicht über dessen Wortlautgrenze hinaus ausgelegt werden.

Daher stellt § 98a Abs. 2 StPO keine Ermächtigungsgrundlage zur selbständigen Erhebung der für die Auswertungsmethoden erforderlichen Daten dar.

c) Zwischenergebnis

Die Daten, die im Rahmen der hier gegenständlichen Auswertungsmethoden ausgewertet werden, sind keine anderen Daten im Sinne des § 98a Abs. 1 StPO.

5. Zwischenergebnis

Die gegenständlich untersuchten Auswertungsmethoden fallen mangels entsprechender Datengrundlage nicht in den Anwendungsbereich von § 98a StPO.

Festzuhalten bleibt aber, dass § 98a StPO grundsätzlich für die maschinelle Datenverarbeitung einschlägig ist, jedoch auf Grund des begrenzten Wortlauts der Datengrundlage bzw. auf Grund der begrenzten Befugnis zur Erhebung von Daten für die hier gegenständlichen Auswertungsmethoden nicht einschlägig ist.

Dies dürfte auch den Hintergrund haben, dass § 98a StPO zwar eine Ermittlungsbefugnis zur Massendatenverarbeitung darstellt, bei ihrer Einführung jedoch auch maßgeblich von der bereits bekannten Maßnahme der Rasterfahndung geprägt war. Insofern dürfte das Problem der Anwendbarkeit des § 98a StPO insbesondere darin liegen, dass § 98a StPO zwar im Grundsatz eine Ermächtigungsgrundlage für die maschinelle Datenverarbeitung in Strafverfahren enthält, ihr Anwendungsbereich aber auf den typischen Ablauf einer Rasterfahndung begrenzt ist, der bereits vor der Einführung dieser Ermittlungsbefugnis bekannt war.

1244 Vgl. BVerfGE 65, 1 (43).

III. § 98c StPO – Maschineller Datenabgleich

Darüber hinaus enthält die StPO mit § 98c StPO eine weitere, im Rahmen des § 98a StPO bereits kurz angesprochene Ermächtigungsgrundlage zur maschinellen Datenverarbeitung.[1245]

Die Befugnis des § 98c StPO erstreckt sich dabei auf den maschinellen Datenabgleich von personenbezogenen Daten „aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten“[1246]. Erfasst ist insoweit der maschinelle Datenabgleich von Daten, die bereits bei den Strafverfolgungsbehörden vorhanden sind.[1247] Wie bereits kurz dargestellt[1248] unterscheiden sich die Rasterfahndung nach § 98a StPO und der maschinelle Datenabgleich nach § 98c StPO neben ihren unterschiedlichen Voraussetzungen insbesondere in der unterschiedlichen Datengrundlage.[1249] So betrifft § 98c StPO nur den maschinellen Datenabgleich von „polizeiinternen Dateien“[1250], § 98a StPO den maschinellen Datenabgleich von „polizeiexternen Dateien“[1251].

Dagegen besteht kein Unterschied hinsichtlich des maschinellen Datenabgleichs.[1252] So sind der maschinelle Datenabgleich in § 98a StPO und in § 98c StPO deckungsgleich. Daher gelten die obigen Ausführungen[1253] dazu, dass bei den gegenständlichen Auswertungsmethoden ein maschineller Datenabgleich vorliegt, hier entsprechend.

Hinsichtlich der Datengrundlage ist § 98c StPO allerdings dahingehend beschränkt, dass ein maschineller Abgleich nur von bereits erhobenen Daten – also von bevorratetem Wissen – stattfinden darf.[1254] Daher müssen die im Rahmen des § 98c StPO abgeglichenen Daten zuvor bereits auf Grund einer anderen Ermittlungsbefugnis erhoben worden sein oder auf Grund einer anderen Ermächtigungsgrundlage erhoben worden sein. In Betracht

1245 BeckOK-StPO/*Gerhold,* § 98c Rn. 2; vgl. MüKo-StPO/*Günther,* § 98c Rn. 7.
1246 Wortlaut des § 98c S. 1 StPO.
1247 KK-StPO/*Greven,* § 98c Rn. 1; Löwe-Rosenberg/*Menges,* § 98c Rn. 1; SSW-StPO/*Jäger,* § 98c Rn. 1; vgl. BT-Drs. 12/989 S. 38.
1248 Siehe hierzu bereits oben unter Kap. 5, B.II.4.b).
1249 Siehe hierzu bereits oben unter Kap. 5,C.I.2.d).
1250 Löwe-Rosenberg/*Menges,* § 98c Rn. 1 mit Verweis auf *Siebrecht*, Rasterfahndung, S. 21.
1251 Löwe-Rosenberg/*Menges,* § 98c Rn. 1.
1252 Vgl. *Siebrecht*, Rasterfahndung, S. 21.
1253 Siehe hierzu oben unter Kap. 5, B.II.2.
1254 Gercke/Julius/Temming/Zöller/*Gercke*, § 98c Rn. 1.

kommende Ermittlungsbefugnisse sind dabei insbesondere die §§ 94, 161, 163, 111, 163d.[1255]

Problematisch ist für die Anwendung des § 98c StPO für die hier gegenständlichen Auswertungsmethoden, dass die von den Auswertungsmethoden analysierten Datensätze wohl in der Regel noch nicht von den Strafverfolgungsbehörden erhoben wurden. Da aber § 98c StPO nur für bereits erhobene Daten anwendbar ist, dürfte er für die hier gegenständlichen Auswertungsmethoden nicht einschlägig sein.

IV. § 100a StPO – Telekommunikationsüberwachung

Diskutiert – und im Ergebnis abgelehnt – wurde im Rahmen der Auswertung von Blockchain-Inhalten bereits die Anwendbarkeit von § 100a StPO.[1256]

§ 100a StPO ermöglicht den heimlichen Zugriff auf Telekommunikation des Betroffenen und damit insbesondere einen Eingriff in das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG.[1257] Da aber der Schutzbereich des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG für die hier gegenständlichen Auswertungsmethoden bereits nicht eröffnet ist[1258], stellt sich die Frage, ob der Schutzbereich des Art. 10 Abs. 1 und der Anwendungsbereich des § 100a StPO deckungsgleich sind und daher § 100a StPO als einschlägige Ermächtigungsgrundlage ausscheidet.

In der Literatur wird diese Frage nicht einheitlich beantwortet. So geht zwar die überwiegende Auffassung in der Literatur davon aus, dass sich der Anwendungsbereich des § 100a StPO am Schutzbereich des Telekommunikationsgeheimnisses orientiert[1259], beide aber nicht deckungsgleich sind[1260]. So soll etwa § 100a StPO nicht ausschließlich für den Zugriff auf Telekommunikation gelten, sondern etwa der Zugriff auf E-Mails des Betroffenen, die beim Provider gespeichert sind, nicht an § 100a StPO zu messen sein,

1255 Gercke/Julius/Temming/Zöller/*Gercke*, § 98c Rn. 1.
1256 *Safferling/Rückert*, MMR 2015, 788 (788ff.); Maume/Maute Kryptowerte HdB/*Rückert,* § 23 Rn. 13; Gercke/Julius/Temming/Zöller/*Gercke,* § 100a Rn. 12.
1257 KK-StPO/*Greven,* § 100a Rn. 1; KMR-StPO/*Bär,* § 100a Rn. 4; SSW-StPO/*Eschelbach,* § 100a Rn. 2; MüKo-StPO/*Graf,* § 100a Rn. 33.
1258 Siehe hierzu bereits oben unter Kap. 4, B.I.2.
1259 KK-StPO/*Greven,* § 100a Rn. 4; KMR-StPO/*Bär,* § 100a Rn. 12.
1260 SK-StPO/*Wolter/Greco,* § 100a Rn. 13; vgl. Gercke/Julius/Temming/Zöller/*Gercke,* § 100a Rn. 10.

sondern an den Befugnissen der §§ 94 ff. StPO.[1261] Das soll jedoch nicht dazu führen, dass Eingriffe auf Grund von § 100a StPO außerhalb des Schutzbereichs von Art. 10 Abs. 1 GG liegen.[1262]

Andere Stimmen in der Literatur gehen dagegen etwa davon aus, dass der Anwendungsbereich des § 100a StPO nicht vom Schutzbereich des Art. 10 Abs. 1 GG abgekoppelt ist.[1263]

Soweit aber Literaturauffassungen keine Deckungsgleichheit annehmen, betrifft dies nur eine begrenzte Anwendbarkeit von § 100a StPO im Verhältnis zum Schutzbereich des Art. 10 Abs. 1 GG – also nur die Frage, ob § 100a StPO eine abschließende Ermächtigung zu Eingriffen in das Telekommunikationsgeheimnis enthält.[1264] Denn, wenn etwa auch die §§ 94 ff. StPO Eingriffe in das Telekommunikationsgeheimnis ermöglichen, bedeutet dies nur, dass § 100a StPO nicht für alle Eingriffe in das Telekommunikationsgeheimnis anwendbar ist.[1265]

Hier stellt sich dagegen aber nicht die abstrakte Frage nach dem Verhältnis zwischen Schutzbereich des Art. 10 Abs. 1 GG und dem Anwendungsbereich des § 100a StPO insgesamt, sondern nur konkret, ob der Anwendungsbereich des § 100a StPO über den Schutzbereich des Art. 10 Abs. 1 GG dahingehend hinausgeht, dass von § 100a StPO auch die Übertragung und Speicherung von öffentlich zugänglicher Telekommunikation[1266] bzw. Telekommunikation, die nicht menschlich veranlasst ist[1267], erfasst ist.

Aus § 100a StPO selbst ergibt sich nur, dass die Ermittlungsbefugnis über den Schutzbereich des Art. 10 Abs. 1 GG hinsichtlich gespeicherter Kommunikationsinhalte hinausgeht. Denn nach § 100a Abs. 1 S. 2, 3, Abs. 5 Nr. 1 lit. a), lit. b) StPO können auch Telekommunikationsinhalte und -umstände überwacht und aufgezeichnet werden, die auf dem informationstechnischen System des Betroffenen gespeichert sind. Insoweit geht die Befugnis des § 100a StPO über den Schutzbereich des Art. 10 Abs. 1 GG

1261 SK-StPO/*Wolter/Greco,* § 100a Rn. 12.
1262 SK-StPO/*Wolter/Greco,* § 100a Rn. 13, die sich allerdings noch auf § 100a vor der gesetzlichen Kodifizierung der sog. Quellen-TKÜ beziehen.
1263 MüKo-StPO/*Günther,* § 100a Rn. 34.
1264 SK-StPO/*Wolter/Greco,* § 100a Rn. 13.
1265 Vgl. SK-StPO/*Wolter/Greco,* § 100a Rn. 13.
1266 Aus diesem Grund scheiden bis auf die sog. *Bloom-Filter-Attacks* alle hier gegenständlichen Auswertungsmethoden aus dem Schutzbereich des Art. 10 Abs. 1 GG aus, vgl. bereits unter Kap. 4, B.I.2.
1267 Aus diesem Grund scheiden die sog. *Bloom-Filter-Attacks* aus dem Schutzbereich des Art. 10 Abs. 1 GG aus, vgl. bereits unter Kap. 4, B.I.2.b)(2).

hinaus, als das auch auf Telekommunikationsinhalte und -umstände, die bereits auf einem Endgerät gespeichert sind und daher nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sind[1268], zugegriffen werden kann.[1269] Daher ermöglicht § 100a Abs. 1 S. 3 StPO insoweit auch einen Eingriff in das IT-Grundrecht und wird daher auch als „kleine Online-Durchsuchung"[1270] bezeichnet.[1271]

Dagegen ist nicht ersichtlich, dass § 100a StPO über den Schutzbereich des Art. 10 Abs. 1 GG auch für Eingriffe in das RiS anwendbar sein soll oder zu Zugriffen auf Telekommunikation, die öffentlich zugänglich ist oder nicht menschlich veranlasst ist, ermächtigen soll.[1272]

Daher scheidet § 100a StPO auf Grund der öffentlichen Verfügbarkeit bzw. der lediglich technisch veranlassten Kommunikation der von den Auswertungsmethoden analysierten Daten als einschlägige Ermächtigungsgrundlage aus.[1273]

V. § 100b StPO – Online-Durchsuchung

Ferner könnte die Ermittlungsbefugnis des § 100b StPO, die zur sog. Online-Durchsuchung ermächtigt, für die hier gegenständlichen Auswertungsmethoden einschlägig sein.

Die im Jahr 2017 neu eingeführte Ermittlungsbefugnis des § 100b StPO ermächtigt die Strafverfolgungsbehörden dem Wortlaut nach dazu, „auch ohne Wissen des Betroffenen […] mit technischen Mittel in ein von dem Betroffenen genutztes informationstechnisches System [einzugreifen] und […] Daten daraus"[1274] zu erheben.[1275]

Der gesetzlichen Normierung der Ermittlungsbefugnis ging eine fast 10 Jahre andauernde politische und rechtliche Diskussion voraus, in deren Zusammenhang insbesondere auch die bereits dargestellte Entscheidung

1268 Siehe hierzu bereits oben unter Kap. 4, B.I.1.b).
1269 SSW-StPO/*Eschelbach,* § 100a Rn. 2.
1270 Vgl. BeckOK-StPO/*Graf,* § 100a Rn. 123.
1271 SSW-StPO/*Eschelbach,* § 100a Rn. 2.
1272 Vgl. SK-StPO/*Wolter/Greco,* § 100a Rn. 13.
1273 So im Ergebnis insbesondere auch *Safferling/Rückert*, MMR 2015, 788 (788ff.); Maume/Maute Kryptowerte HdB/*Rückert,* § 23 Rn. 13.
1274 Wortlaut des § 100b Abs. 1 Hs. 1 StPO.
1275 BeckOK-StPO/*Graf,* § 100b Rn. 5.

des BVerfG zum Verfassungsschutzgesetz NRW stand.[1276] So setzt sich etwa die Beschlussempfehlung des Bundestages zur Einführung des § 100b StPO insbesondere auch mit dem Urteil des BVerfG zum Verfassungsschutzgesetz NRW auseinander.[1277] Denn § 100b StPO ermächtigt insbesondere zu einem Eingriff in das IT-Grundrecht.[1278] Nach § 100b StPO ist einerseits die Infiltration informationstechnischer Systeme und andererseits die Datenerhebung und ein dauerhaftes *Datenmonitoring* aus den infiltrierten informationstechnischen Systemen zulässig.[1279]

Bei den hier gegenständlichen Auswertungsmethoden ist dagegen allerdings der Schutzbereich des IT-Grundrechts nicht eröffnet.[1280] Denn sowohl Blockchain-Netzwerke selbst, als auch das *Peer-To-Peer*-Netzwerk, über die die Telekommunikation für das Blockchain-Netzwerk abläuft, sind nicht vom Schutzbereich des IT-Grundrechts erfasst, da sie als offene Netzwerke ausgestaltet sind und die Nutzer daher keine berechtigte Vertraulichkeitserwartung in diese Netzwerke haben können.[1281] Zwar können auch Netzwerke selbst informationstechnische Systeme im Sinne des Schutzbereichs des IT-Grundrechts sein[1282], erforderlich ist darüber hinaus allerdings, dass der „Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt"[1283]. Insoweit ist der Schutzbereich des IT-Grundrechts insbesondere nicht berührt, wenn Daten auf dem technisch dafür vorgesehenen Weg erhoben werden, die der Inhaber des Systems für die Internetkommunikation vorgesehen hat.[1284] Da die Datenerhebung bei den gegenständlichen Auswertungsmethoden auf dem technisch für die Blockchain-Netzwerke vorgesehenen Weg stattfindet und auf Grund der dezentralen Verwaltungsstruktur von Blockchains eine

1276 BeckOK-StPO/*Graf,* § 100b Rn. 3; siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.
1277 BT-Drs. 18/12785 S. 54.
1278 BeckOK-StPO/*Graf,* § 100b Rn. 1, 8; KK-StPO/*Bruns,* § 100b Rn. 2; Gercke/Julius/Temming/Zöller/*Gercke,* § 100b Rn. 10; vgl. *Singelnstein/Derin*, NJW 2017, 2646 (2647); *Blechschmitt*, MMR 2018, 361 (365); vgl. BT-Drs. 18/12785 S. 54.
1279 Löwe-Rosenberg/*Hauck,* § 100b Rn. 106; BeckOK-StPO/*Graf,* § 100b Rn. 1; KMR-StPO/*Bär,* § 100b Rn. 14;
1280 Siehe hierzu bereits oben unter Kap. 4, B.III.3.
1281 Siehe hierzu bereits oben unter Kap. 4, B.III.3.
1282 Siehe hierzu bereits oben unter Kap. 4, B.III.2.a); BVerfGE 120, 274 (276).
1283 BVerfGE 120, 274 (315); siehe hierzu bereits oben unter Kap. 4, B.III.2.b).
1284 BVerfGE 120, 274 (344); siehe hierzu bereits oben unter Kap. 4, B.III.2.b).

Verfügung über das informationstechnische System ausscheidet, ist der Schutzbereich des IT-Grundrechts insoweit nicht eröffnet.[1285]

Der Begriff des informationstechnischen Systems orientiert sich am Schutzbereich des IT-Grundrechts, da § 100b StPO gerade als Rechtsgrundlage für Eingriffe in das IT-Grundrecht ausgestaltet ist.[1286] Außerdem ist nicht ersichtlich, weshalb der Anwendungsbereich des § 100b StPO weiter sein sollte als der Schutzbereich des IT-Grundrechts.

Daher kann § 100b StPO keine Ermächtigungsgrundlage für die hier gegenständlichen Auswertungsmethoden darstellen.

VI. § 100g StPO – Erhebung von Verkehrsdaten

Weiterhin könnte § 100g StPO für die hier gegenständlichen Auswertungsmethoden anwendbar sein – insbesondere für die in Kap. 3, B.I. dargestellte Auswertung der Verbreitung von Transaktionsnachrichten in Blockchain-Netzwerken. Denn § 100g StPO ermöglicht auch einen Eingriff in das RiS.[1287]

§ 100g StPO enthält insgesamt drei verschiedene Ermittlungsbefugnisse.[1288] Zunächst ist nach § 100g Abs. 1 StPO die Erhebung von Verkehrsdaten nach §§ 96 Abs. 1 TKG und Standortdaten, die vom Telekommunikationsanbieter zum Zwecke der Abrechnung oder Störungsbeseitigung erhoben wurden, zulässig.[1289] Darüber hinaus enthält § 100g Abs. 2 die Ermächtigung zur Erhebung von auf „Vorrat" gespeicherten Verkehrsdaten vom Telekommunikationsanbieter.[1290] Schließlich ermächtigt § 100g Abs. 3 StPO zur sog. Funkzellenabfrage und damit zur Ermittlung aller mobilen Endgeräte, die zu einer bestimmten Zeit in der betreffenden Funkzelle angemeldet waren.[1291]

1285 Siehe hierzu ausführlich oben unter Kap. 4, B.III.3.
1286 Gercke/Julius/Temming/Zöller/*Gercke,* § 100b Rn. 10; BeckOK-StPO/*Graf,* § 100b Rn. 8; vgl. BVerfG NJW 2016, 1781 (1793f.) zur präventiven Online-Durchsuchung des § 20k BKAG a.F.; vgl. BT-Drs. 18/12785 S. 54.
1287 Gercke/Julius/Temming/Zöller/*Gercke,* § 100g Rn. 1.
1288 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (83).
1289 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (83).
1290 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (84); Hdb-StA/*Andrä/Tischer*, 1. Teil, 1.Kap., E. Rn. 69.
1291 BeckOK-StPO/*Bär,* § 100g, Rn. 47; *Bär*, NStZ 2017, 81 (84f.).

Dabei ermächtigt § 100g StPO Abs. 1 zur Erhebung von Verkehrsdaten nach § 96 Abs. 1 TKG beim „Diensteanbieter" und damit nach §§ 3 Nr. 6, Nr. 24 TKG bei geschäftsmäßigen Anbietern von Diensten, die „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen". Nach § 100g Abs. 2 StPO können nach § 113b TKG gespeicherte Daten beim „Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer" im Sinne von § 3 Nr. 6 lit. a TKG[1292], also ebenfalls bei Anbietern von Diensten, die nach § 3 Nr. 24 TKG „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen", erhoben werden.

Daher stellt sich für die Anwendbarkeit von § 100g StPO zunächst die Frage, ob die hier gegenständlich ausgewerteten Blockchain-Netzwerke als *Peer-To-Peer*-Netzwerke Diensteanbieter im Sinne der §§ 3 Nr. 6, 24 TKG sind.

Dies kommt etwa in Betracht, da insbesondere diskutiert wird, ob nicht auch sog. „Over-the-Top-Anbieter" (nachfolgend als „OTT-Anbieter" bezeichnet) als Telekommunikationsdiensteanbieter im Sinne der § 3 Nr. 6, 24 TKG anzusehen sind.[1293]

OTT-Anbieter sind die Anbieter von Diensten, die entweder unmittelbare Kommunikation oder Inhalten über das offene Internet anbieten.[1294] Dies betrifft insbesondere Dienste wie WhatsApp, Skype, Google, YouTube, Netflix, die teilweise die klassischen Kommunikationsmittel wie Telefonanrufe und SMS ersetzen.[1295] Differenziert werden bei der rechtlichen Bewertung sog. OTT-Kommunikationsdienst, bei denen die Individual- und Gruppenkommunikation der Nutzer im Vordergrund steht – etwa WhatsApp, Gmail, iMessage, Skype –, und OTT-Inhaltsdienste, bei denen der Inhalt des Dienstes im Vordergrund steht – etwa Google, YouTube, Netflix.[1296]

Die Einordnung als Telekommunikationsdiensteanbieter der OTT-Kommunikationsdienste wird dabei damit begründet, dass zwar auch bei den OTT-Kommunikationsdiensten die unmittelbare Signalübertragung über das offene Internet stattfindet, die Kommunikation aber je nach techni-

1292 *Roßnagel*, NJW 2016, 533 (535).
1293 Siehe hierzu ausführlich etwa *Kühling/Schall*, CR 2015, 641 (641ff.); *Kühling/Schall*, CR 2016, 185 (185ff.); *Grünwald/Nüßing*, MMR 2016, 91 (91); *Schuster*, CR 2016, 173 (173ff.); VG Köln CR 2016, 131 ff.
1294 *Kühling/Schall*, CR 2015, 641 (641).
1295 *Kühling/Schall*, CR 2015, 641 (641f.).
1296 *Kühling/Schall*, CR 2015, 641 (642f.).

scher Ausgestaltung in der Regel[1297] auch über Server des jeweiligen OTT-Diensteanbieters abgewickelt wird.[1298]

Da insoweit nicht ausschließlich die unmittelbaren Internet-Access-Provider als Telekommunikationsdiensteanbieter erfasst sind, ließe sich auf den ersten Blick annehmen, dass auch Blockchain-Netzwerke selbst derartige Diensteanbieter sein könnten.

Dabei ist jedoch zu berücksichtigen, dass im Rahmen der Diskussion um die Einordnung von OTT-Anbietern jedenfalls davon ausgegangen wird, dass dann kein Diensteanbieter im Sinne der §§ 3 Nr. 6, 24 TKG vorliegt, wenn der unmittelbare Austausch der Daten der Kommunikation nicht über einen zentralen Server des jeweiligen Diensteanbieters abläuft, sondern über ein *Peer-To-Peer*-Netzwerk.[1299] Denn die entscheidende Signalübertragung findet hier unmittelbar zwischen den Endgeräten der beteiligten Nutzer statt.[1300]

Da aber Blockchain- und *Tor-Netzwerke* als *Peer-To-Peer*-Netzwerke ausgestaltet sind, bei denen ebenfalls die Telekommunikation unmittelbar zwischen den beteiligten Nutzern stattfindet[1301], lassen sich diese jedenfalls nicht als Diensteanbieter im Sinne der §§ 3 Nr. 6, 24 TKG einordnen.

Daher können die Ermittlungsbefugnisse des § 100g StPO für die hier gegenständlichen Auswertungsmethoden keine Anwendung finden.

VII. § 100j StPO – Bestandsdatenauskunft

In Betracht kommt ferner die Ermittlungsbefugnis des § 100j StPO nach dessen Abs. 2 Auskunft über sog. Bestandsdaten nach §§ 95, 111 TKG der Anschluss Inhaber von (dynamischen)[1302] IP-Adressen verlangt werden können.[1303]

1297 Dies hängt entscheidend von der jeweiligen technischen Ausgestaltung ab, siehe zu den einzelnen, technischen Möglichkeiten *Kühling/Schall*, CR 2015, 641 (643ff.).

1298 *Kühling/Schall*, CR 2016, 185 (186) m.w.N.

1299 *Kühling/Schall*, CR 2016, 185 (186) m.w.N.

1300 *Grünwald/Nüßing*, MMR 2016, 91 (94).

1301 Siehe hierzu bereits ausführlich oben unter Kap. 2, A.III.1.a), Kap. 3, B.II.1.

1302 Siehe zum Streitstand, ob auch dynamische IP-Adressen von der Ermittlungsbefugnis des § 100j Abs. 2 StPO erfasst sind, übersichtlich Gercke/Julius/Temming/Zöller/*Gercke,* § 100g Rn. 7.

1303 Gercke/Julius/Temming/Zöller/*Gercke,* § 100g Rn. 7; SSW-StPO/*Eschelbach,* § 100j Rn. 2.

Insbesondere bei der in Kap. 3, B.I. dargestellten Auswertungsmethode wird aber einzelnen *Bitcoin-Adressen* eine IP-Adresse zugeordnet und nicht die persönlichen Daten des Anschlussinhabers einer IP-Adresse ermittelt. Zwar dient die Zuordnung einer IP-Adresse zu einer *Bitcoin-Adresse* der Ermittlung der persönlichen Daten der *Bitcoin-Adresse* gerade über die Zuordnung der IP-Adresse. Die Ermittlungsbefugnis des § 100j Abs. 2 StPO betrifft aber nur die Ermittlung der persönlichen Daten einer IP-Adresse und nicht die vorgelagerte Ermittlung bzw. Zuordnung von IP-Adressen zu *Bitcoin-Adressen*.

Daher ist auch § 100j StPO für die hier gegenständlichen Auswertungsmethoden nicht einschlägig.

VIII. §§ 161, 163 StPO – Ermittlungsgeneralklauseln

Da keine der speziellen Ermittlungsbefugnisse einschlägig ist, bleiben als einschlägige Ermächtigungsgrundlagen nur noch die Ermittlungsgeneralklauseln der §§ 161, 163 StPO.

Nach § 161 Abs. 1 S. 1 StPO „ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln." § 161 Abs. 1 S. 1 StPO enthält insoweit einerseits eine allgemeine Auskunftspflicht bzw. Datenübermittlungspflicht gegenüber Behörden und andererseits eine Generalermittlungsklausel zu Ermittlungen jeder Art.[1304]

Auf diese Ermittlungsgeneralklauseln werden dabei von der herrschenden Literaturauffassung insbesondere auch Ermittlungen im allgemein zugänglichen Internet und die sog. Online-Streife gestützt.[1305] Dies wird in der Regel mit einer fehlenden Grundrechtsrelevanz bei der Kenntnisnahme von öffentlich zugänglichen Informationen im Internet oder bei gezielten

1304 KK-StPO/*Griesbaum,* § 161 Rn. 1; Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 2.

1305 BeckOK-StPO/*Sackreuther,* § 161 Rn. 11; KK-StPO/*Griesbaum,* § 161 Rn. 12a; SK-StPO/*Weßlau/Deiters,* § 161 Rn. 14; Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 2; ausführlich zu sog. Online-Streifen in sozialen Netzwerken: *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 130ff., 256ff.; *Bauer*, Soziale Netzwerke, S. 47ff., 121ff.

Suchen und Ermittlungen mit der geringfügigen Grundrechtsintensität von öffentlich zugänglichen Daten begründet.[1306]

Daher stellt sich die Frage, ob dies auch für die hier gegenständlichen Auswertungsmethoden gelten kann, die zwar einerseits lediglich öffentlich zugängliche Informationen auswerten, andererseits aber eine systematische Analyse dieser Daten betreffen, bei der insbesondere auch eine große Anzahl unbeteiligter Personen betroffen sein kann.[1307]

Da beide Befugnisse allerdings unter der Einschränkung des § 161 Abs. 1 S. 1 Hs. 2 stehen, wonach Maßnahmen nur auf § 161 Abs. 1 S. 1 StPO gestützt werden können, „soweit nicht andere gesetzliche Vorschriften [die] Befugnisse besonders regeln"[1308], ergibt sich hieraus, dass auf § 161 Abs. 1 S. 1 StPO nur solche Ermittlungshandlungen gestützt werden können, die nicht besonders geregelt sind.[1309]

Wie soeben ausführlich dargestellt[1310] ist keine der speziellen Ermittlungsbefugnisse für die Auswertungsmethoden einschlägig.

Darüber hinaus leitet die herrschende Literaturauffassung aus § 161 Abs. 1 S. 1 Hs. 2 StPO außerdem ab, dass eine Sperrwirkung auch für Ermittlungsmaßnahmen besteht, die in ihrer Grundrechtsintensität mit den gesetzlich geregelten Ermittlungsmaßnahmen vergleichbar sind, aber selbst nicht geregelt sind.[1311] Insoweit soll § 161 Abs. 1 S. 1 StPO nur zu solchen Ermittlungsmaßnahmen ermächtigen, die unterhalb der Schwelle von vorhandenen Eingriffsermächtigungen liegen.[1312]

Problematisch soll diese Abgrenzung insbesondere dann sein, wenn Ermittlungsmaßnahmen eine Ähnlichkeit oder Vergleichbarkeit mit speziell geregelten Ermittlungsmaßnahmen aufweisen, aber „noch oder schon nicht mehr von einer Einzelermächtigung erfasst sind"[1313]. Dies könnte bei den

1306 KK-StPO/*Griesbaum,* § 161 Rn. 12a; Löwe-Rosenberg/*Erb,* § 161 Rn. 5; *Bauer*, Soziale Netzwerke, S. 121 mit Verweis auf *Schulz/Hoffmann*, DuD 2012, 7 (13); *Ostendorf/Frahm/Doege*, NStZ 2012, 529 (537); *Kudlich*, StV 2012, 560 (566); *Klesczewski*, ZStW 123 (2011), 737 (739).

1307 Siehe ausführlich die Darstellung der Funktionsweisen der Auswertungsmethoden unter Kap. 3, zur möglichen Anwendung der Auswertungsmethoden in der Ermittlungspraxis unter Kap. 5, A.

1308 Löwe-Rosenberg/*Erb,* § 161 Rn. 5. Darüber hinaus bestehen außerdem die zunächst nicht näher betrachteten Einschränkungen der Abs. 2-4.

1309 Löwe-Rosenberg/*Erb,* § 161 Rn. 5.

1310 Siehe hierzu unter Kap. 5, B.I-VII.

1311 Löwe-Rosenberg/*Erb,* § 161 Rn. 5 m.w.N.

1312 SK-StPO/*Weßlau/Deiters,* § 161 Rn. 12; Löwe-Rosenberg/*Erb,* § 161 Rn. 5.

1313 SK-StPO/ *Weßlau/Deiters,* § 161 Rn. 9.

hier gegenständlichen Auswertungsmethoden insoweit problematisch sein, als dass – wie bereits dargestellt – eine inhaltliche Nähe zu der speziell geregelten Rasterfahndung des § 98a StPO besteht.[1314]

So wurde etwa im Rahmen des Einsatzes Verdeckter Ermittler nach §§ 110a ff. StPO und des Einsatzes sog. „nicht offen ermittelnder Polizeibeamter" (nachfolgend als „noeP" bezeichnet) diskutiert, ob sich auch der Einsatz von noeP nach den §§ 110a ff. StPO richten müsste oder und bis zu welcher Grenze er auf die §§ 161, 163 StPO gestützt werden könnte.[1315] Zwar wurde in diesem Zusammenhang auch diskutiert, ob der noeP ein Aliud oder ein Minus im Verhältnis zum Verdeckten Ermittler sei[1316], die Diskussion betrifft allerdings im Wesentlichen ebenfalls die Frage nach einer Vergleichbarkeit der Grundrechtsintensität beider Maßnahmen.[1317] So nimmt mittlerweile die herrschende Meinung und die Rechtsprechung an, dass der Einsatz von noeP zulässigerweise auf die §§ 161, 163 StPO gestützt werden könne, soweit er nicht „über einen längeren Zeitraum unter Benutzung seiner Legende [gegenüber] einer oder mehreren Personen auftritt.[1318] Denn beim Einsatz von noeP bestünde nicht die Eingriffsintensität, die bei einem verdeckten Ermittler vorliegen würde.[1319]

Auf die Grundrechtsintensität der hier gegenständlichen Auswertungsmethoden wird im Folgenden – auch unter Berücksichtigung einer etwaigen Vergleichbarkeit zu der in § 98a StPO geregelten Rasterfahndung – ausführlich im Rahmen der Voraussetzungen des § 161 Abs. 1 StPO eingegangen.[1320] Daher soll hier nur kurz darauf eingegangen werden, dass bei den hier gegenständlichen Auswertungsmethoden wesentliche Unterschiede zu der in § 98a StPO geregelten Rasterfahndung bestehen, sodass wohl

1314 Siehe hierzu bereits ausführlich oben unter Kap. 5, C.I.2.

1315 Siehe hierzu etwa *Krey/Jaeger*, NStZ 1995, 516 (517f.); *Rogall*, JZ 1996, 259 (262); *Beulke/Rogat*, JR 1996, 515 (518); *Roxin*, StV 1998, 43 (43ff.); *Weisser*, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafr. 2018, 59 (61).

1316 So nimmt etwa SK-StPO/ *Weßlau/Deiters,* § 161 Rn. 9 unter Verweis auf unter anderem *Krey/Jaeger*, NStZ 1995, 516 (517f.); *Rogall*, JZ 1996, 259 (262); *Beulke/Rogat*, JR 1996, 515 (517f.) an, dass der Einsatz von noeP eine Aliud im Verhältnis zum Einsatz von verdeckten Ermittlern darstelle und daher grundsätzlich auf §§ 161, 163 StPO gestützt werden könne.

1317 *Krey/Jaeger*, NStZ 1995, 516 (518); *Rogall*, JZ 1996, 259 (262); *Beulke/Rogat*, JR 1996, 515 (517f.); *Weisser*, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafr. 2018, 59.

1318 BGHSt 41, 64 (Ls. 1).

1319 Vgl. BVerfG NJW 2012, 833 (840).

1320 Siehe hierzu nachfolgend unter Kap. 5, D.II.

in diesem Sinne von einem Aliud im Verhältnis zur Rasterfahndung ausgegangen werden muss.

Denn bei der Rasterfahndung soll ein Verdächtigenkreis von bestimmten Personen, auf die bestimmte Merkmale zutreffen, dadurch ermittelt werden, dass personenbezogene Daten mit anderen Daten, die von mehreren Speicherstellen übermittelt werden, maschinell abgeglichen werden.[1321] Zwar finden im Rahmen der hier gegenständlichen Auswertungsmethoden ebenfalls maschinelle Datenabgleiche auf bestimmte Prüfungsmerkmale statt, die wesentlichen Unterschiede zur Rasterfahndung liegen aber einerseits darin, dass bestimmte Datensätze bei den hier gegenständlichen Auswertungsmethoden systematisch analysiert werden und nicht nur eine Rasterung von Daten anhand bestimmter Kriterien stattfindet.[1322] Dieser Unterschied führt zwar noch nicht zur Nichtanwendbarkeit des § 98a StPO, da auch die systematische Datenauswertung wohl unter den Begriff des maschinellen Datenabgleichs des § 98a Abs. 1 StPO fällt[1323], soll aber hier nochmal unterstreichen, dass eine Wesensverschiedenheit zu der typischen Rasterfahndung besteht. Darüber hinaus ist die Datengrundlage insoweit eine andere, als dass im Rahmen von § 98a StPO nur freiwillig von Speicherstellen herausgegebene Daten und nach § 98a Abs. 2 StPO übermittelte Daten Gegenstand dieser Rasterung sein können. Da sich die hier gegenständlichen Auswertungsmethoden aber auf öffentlich zugängliche Daten beschränken, die von den Ermittlungsbehörden erhoben werden müssen, besteht hierin ein weiterer wesentlicher Unterschied.[1324]

Dies führt im Ergebnis dazu, dass die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO einschlägige Ermächtigungsgrundlage für die hier gegenständlichen Auswertungsmethoden ist.

IX. Zwischenergebnis

Keine der auch nur entfernt in Betracht kommenden, speziellen Ermittlungsbefugnisse ist für die gegenständlichen Auswertungsmethoden einschlägig. Daher kann eine Ermächtigungsgrundlage für die Auswertungsmethoden nur in den Ermittlungsgeneralklauseln der §§ 161, 163 StPO liegen. Ob die Auswertungsmethoden auch zulässigerweise auf diese Er-

1321 Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.
1322 Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.
1323 Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.2.
1324 Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.4.

mittlungsgeneralklauseln gestützt werden können, muss nachfolgend untersucht werden.

C. Verfassungsmäßigkeit der Ermittlungsgeneralklauseln §§ 161, 163 StPO

Damit die Ermittlungsgeneralklauseln als taugliche Ermächtigungsgrundlage für die Anwendung der gegenständlichen Auswertungsmethoden auch eine ausreichende verfassungsrechtliche Rechtfertigung der Grundrechtseingriffe sein können, müssen diese zunächst formell und materiell verfassungsgemäß sein.

An der formellen Verfassungsmäßigkeit der §§ 161, 163 StPO bestehen keinerlei Zweifel.

Auch an der materiellen Verfassungsmäßigkeit bestehen keine grundsätzlichen Zweifel. Sie wird allerdings ausführlich geprüft, da sich insbesondere das Bestimmtheitsgebot und der Verhältnismäßigkeitsgrundsatz auf die Reichweite der Ermittlungsbefugnis der §§ 161, 163 StPO auswirken.

I. Zitiergebot des Art. 19 Abs. 1 S. 2 GG

1. Anforderungen des Zitiergebotes

Erforderlich ist nach Art. 19 Abs. 1 S. 2 GG bei der Einschränkung von Grundrechten grundsätzlich, dass der Gesetzgeber das sog. Zitiergebot beachtet. Das bedeutet, dass der Gesetzgeber bei Gesetzen durch die oder auf deren Grundlage Grundrechte beschränkt werden (können), die möglicherweise beschränkten Grundrechte benennen muss.[1325] Dies dient einerseits einer Warn- und Besinnungsfunktion für den Gesetzgeber, denn dieser soll sich bei der Verabschiedung von grundrechtsbeschränkenden Gesetzen der Beschränkung bewusst sein.[1326] Außerdem dient das Zitiergebot auch dem Rechtsanwender und dem Grundrechtsträger in Form einer Informations- und Hinweisfunktion.[1327]

Der Anwendungsbereich des Zitiergebotes ist nach dem BVerfG jedoch in mehreren Hinsichten eingeschränkt.

1325 HGR Bd. III/*Axer,* § 67 Rn. 1.
1326 HGR Bd. III/*Axer,* § 67 Rn. 9.
1327 HGR Bd. III/*Axer,* § 67 Rn. 9 m.w.N.

So sind hiervon zunächst vorkonstitutionelle Gesetze ausgenommen, da der vorkonstitutionelle Gesetzgeber anderen Anforderungen unterlag und andernfalls ein Widerspruch zum in Art. 123 GG normierten Grundsatz der Rechtskontinuität bestünde.[1328]

Darüber hinaus nimmt das BVerfG an, dass auch nachkonstitutionelle Gesetze vom Zitiergebot ausgenommen sind, wenn Grundrechtsbeschränkungen, die bereits vor Inkrafttreten des Zitiergebotes bestanden, lediglich „unverändert oder mit geringen Abweichungen"[1329] übernommen werden. Das BVerfG begründet dies damit, dass das Zitiergebot nur davor schützen solle, dass der Gesetzgeber neue Grundrechtsbeschränkungen beschließt, ohne hierüber Rechenschaft abzulegen.[1330]

Ferner gibt das BVerfG vor, dass das Zitiergebot nur bei der Einschränkung von Grundrechten Anwendung findet, wenn diese auf der Grundlage einer ausdrücklichen Ermächtigung eingeschränkt werden.[1331] Dies begründet das BVerfG insbesondere damit, dass das Zitiergebot als bloße Formvorschrift einer besonders engen Auslegung unterliege, da es andernfalls zu einer leeren Förmlichkeit erstarren würde.[1332] Insoweit gelte das Zitiergebot „nur für Gesetze, die darauf abzielen, ein Grundrecht über die in ihm selbst angelegten Grenzen […] hinaus einzuschränken."[1333] Es finde daher keine Anwendung für die allgemeine Handlungsfreiheit, die von vornherein nur „unter dem Vorbehalt der verfassungsmäßigen Ordnung gewährleistet"[1334] sei. Unklar bzw. offengelassen hat das BVerfG in diesem Zusammenhang allerdings bisher, ob auch das allgemeinen Persönlichkeitsrechts bzw. das RiS vom Anwendungsbereich des Zitiergebotes ausgenommen ist.[1335]

Da nach der Rechtsprechung das RiS als Ausprägung des allgemeinen Persönlichkeitsrechts der Schrankentrias des Art. 2 Abs. 1 Hs. 2 GG[1336] genauso unterliegt, wie die allgemeine Handlungsfreiheit, ließe sich zunächst

1328 HGR Bd. III/*Axer,* § 67 Rn. 17 m.w.N.
1329 BVerfGE 5, 13 (16); BVerfGE 15, 288 (293); BVerfGE 16, 194 (199f.); BVerfGE 35, 185 (189); BVerfGE 61, 82 (113); HGR III./*Axer,* § 67 Rn. 18.
1330 BVerfGE 5, 13 (16); HGR III./*Axer,* § 67 Rn. 18 m.w.N. und der Kritik zu dieser von der Rechtsprechung vertretenen Ansicht.
1331 BVerfG NJW 1991, 1471 (1474).
1332 BVerfG NJW 1970, 1268 (1268f.).
1333 BVerfG NJW 1970, 1268 (1269).
1334 BVerfG NJW 1970, 1268 (1269).
1335 So BeckOK-GG/*Enders,* Art. 19 Rn. 14 mit Verweis auf BVerfGE 120, 274 (340, 343), wonach nur ein Verstoß gegen das Zitiergebot für den Eingriff in das Telekommunikationsgeheimnis durch das heimliche Aufklären des Internets vorlag.
1336 Siehe hierzu bereits oben unter Kap. 5, A.I.

annehmen, dass Beschränkungen des RiS nicht in den Anwendungsbereich des Zitiergebotes fallen.[1337]

Dem ließe sich allerdings entgegenhalten, dass auf Grund der Verbindung mit Art. 1 Abs. 1 GG erhöhte Anforderungen an Einschränkungen des allgemeinen Persönlichkeitsrechts bzw. dem aus ihm abgeleiteten RiS bestehen, woraus die Schlussfolgerung gezogen werden könnte, dass insoweit auch bei der Einschränkung des RiS das Zitiergebot zu beachten sei.

Diesem Argument steht allerdings entgegen, dass das Zitiergebot nach der Begründung des BVerfG bei der allgemeinen Handlungsfreiheit als bloße Formvorschrift keine Anwendung finden soll, da es im Bereich der allgemeinen Handlungsfreiheit als Auffanggrundrecht zu einer bloßen Förmlichkeit erstarren würde.[1338] Diese teleologische Argumentation könnte auch auf die Einschränkung des allgemeinen Persönlichkeitsrechts bzw. dessen Ausprägung in Form des RiS übertragen werden.

Insoweit stellt sich die Frage, ob das allgemeine Persönlichkeitsrecht und seine Ausprägung des RiS ebenfalls nur Auffanggrundrechte im Verhältnis zu besonderen Privatsphäregrundrechten der Art. 10, 13 GG darstellen.

Für ein derartiges Spezialitätsverhältnis spricht, dass das allgemeine Persönlichkeitsrecht eine „lückenschließende[…] Gewährleistung"[1339] darstellt. Allerdings sollen die vom allgemeinen Persönlichkeitsrecht gewährleisteten Elemente den besonderen Freiheitsgarantien „in ihrer konstituierenden Bedeutung für die Persönlichkeit"[1340] nicht nachstehen.

Hieraus ergibt sich, dass das allgemeine Persönlichkeitsrecht zwar im Grundsatz in einem Spezialitätsverhältnis zu den besonderen Freiheitsrechten – im Bereich des RiS zu den besonderen Privatsphäregrundrechten der Art. 10, 13 GG – steht, dieses aber in seinem Gewährleistungsgehalt den speziellen Freiheitsrechten nicht nachsteht. Dieses Verhältnis muss insoweit auch für die Einschränkbarkeit gelten.

Daher lässt sich die teleologische Argumentation des BVerfG nicht auf das Erfordernis des Zitiergebotes bei der Einschränkung des RiS übertragen.

1337 So auch Löwe-Rosenberg/*Menges,* Vor §§ 94 ff. Rn. 48; *Ihwas,* Strafverfolgung in sozialen Netzwerken, S. 88 m.w.N., der insbesondere auf BVerfGE 10, 89 (99); BVerfGE 28, 36 (46) verweist, die allerdings nicht Einschränkung des RiS betreffen, sondern Einschränkungen der allgemeinen Handlungsfreiheit und der Meinungsfreiheit.

1338 BVerfG NJW 1970, 1268 (1269).

1339 BVerfGE 120, 274 (303).

1340 BVerfGE 120, 274 (303).

Für dieses Ergebnis spricht insbesondere auch die in der Literatur weit verbreitete Kritik an der vom BVerfG vertretenen begrenzten Anwendbarkeit des Zitiergebotes. Hiernach sei es widersprüchlich, im Rahmen der Regelungsvorbehalte – wie etwa bei Art. 12 Abs. 1 S. 2 GG – grundsätzlich die abwehrrechtlichen Schutzmechanismen anzuwenden, hiervon aber Art. 19 Abs. 1 S. 2 GG auszunehmen.[1341] Außerdem sei die unterschiedliche Ausgestaltung von Grundrechtsvorbehalten kein Grund dafür, das Zitiergebot nur bei speziellen Gesetzesvorbehalten anzuwenden, da das Zitiergebot dem Gesetzgeber die Grundrechtsrelevanz seines Handelns aufzeigen soll und dies nicht davon abhängen könne, auf welchem Grundrechtsvorbehalt die Einschränkung beruhe.[1342] Der Gesetzgeber reglementiere unabhängig von der jeweiligen Grundlage die Grundrechtsausübung, sodass jeweils die mit dem Zitiergebot verfolgte Warnfunktion bestehen müsse.[1343]

Aus diesen Gründen findet das Zitiergebot des Art. 19 Abs. 1 S. 2 GG Anwendung für die gesetzliche Grundlage eines Eingriffs in das RiS.[1344] Dieses Ergebnis wird außerdem dadurch unterstützt, dass der Gesetzgeber teilweise für Einschränkungen des allgemeinen Persönlichkeitsrechts oder des RiS das Zitiergebot ausdrücklich beachtet.[1345]

2. Das Zitiergebot bei der Ermittlungsgeneralklausel des § 161 StPO

Die Vorschrift des § 161 StPO ist bereits Bestandteil der ursprünglichen Fassung der StPO aus dem Jahr 1877 gewesen, sodass sich hier die Ausnahme für vorkonstitutionelles Recht vom Zitiergebot annehmen ließe.[1346]

Problematisch könnte jedoch sein, dass § 161 StPO in seiner ursprünglichen Fassung lediglich eine Aufgabenzuweisung der Staatsanwaltschaft ent-

1341 Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. 1 Rn. 55.
1342 HGR III./*Axer,* § 67 Rn. 25.
1343 HGR III./*Axer,* § 67 Rn. 25.
1344 So insbesondere auch mit ausführlicher Begründung und weiteren Nachweisen HGR III./*Axer,* § 67 Rn. 24; Sachs-GG/*Sachs,* Art. 19 Rn. 29; *Martini,* JA 2009, 839 (843); *Krausnick,* JuS 2007, 1088 (1089); a.A. *Ihwas,* Strafverfolgung in sozialen Netzwerken, S. 87, der allerdings ohne weitere Begründung hierzu u.a. auf die Entscheidungen BVerfGE 10, 89 (99); BVerfGE 28, 36 (46) verweist, in denen das BVerfG jedoch lediglich feststellt, dass das Zitiergebot auf Grund der vorstehend bereits dargestellten Gründen nicht im Rahmen der allgemeinen Handlungsfreiheit und der Meinungsfreiheit gelten kann.
1345 Sachs-GG/*Sachs,* Art. 19 Rn. 29, der u.a. Auf § 32 VSG NRW und § 28 HaSiG NRW verweist.
1346 *Kochheim,* KriPoZ 2018, 314 (315).

hielt und erst durch das Strafverfahrensänderungsgesetz mit Wirkung zum 01.11.2000 zu einer Ermittlungsbefugnis umgestaltet wurde.[1347] Hintergrund war die bis in die 70er Jahre vorherrschende Auffassung, die Staatsanwaltschaft sei grundsätzlich zu allen Maßnahmen der Sachverhaltserforschung berechtigt und hierfür sei der allgemeine Auftrag zur Sachverhaltserforschung samt Aufgabenzuweisung der §§ 161, 163 StPO ausreichend.[1348]

Das BVerfG nimmt aber an, dass auch solche Grundrechtsbeschränkungen, die bereits vor Inkrafttreten des Zitiergebotes bestanden haben und lediglich unverändert oder mit geringfügigen Änderungen übernommen werden, nicht dem Zitiergebot unterliegen.[1349]

Die Ermittlungsgeneralklauseln wurden lediglich auf Grund eines veränderten Verständnisses von Grundrechtseingriffen von Aufgabenzuweisungen zu Ermittlungsbefugnissen umgestaltet[1350] – die Grundrechtsbeschränkungen hierdurch blieben jedoch die gleichen. Insoweit unterliegt die Änderung der §§ 161, 163 StPO durch das Strafverfahrensänderungsgesetz nicht dem Zitiergebot.[1351]

II. Verbot des Einzelfallgesetzes, Art. 19 Abs. 1 S. 1 GG

Weiterhin muss eine grundrechtsbeschränkende gesetzliche Grundlage nach Art. 19 Abs. 1 S. 1 GG grundsätzlich allgemein gelten und nicht nur für den Einzelfall.[1352] Erforderlich ist insoweit eine abstrakt-generelle Regelung, die für eine unbestimmte Vielzahl künftiger Anwendungsfälle gilt.[1353]

Das BVerfG beschränkt jedoch wiederum den Anwendungsbereich des Verbots des Einzelfallgesetzes auf Grundrechte, die unter einem ausdrück-

1347 *Kahler,* Massenzugriff der StA auf Kundendaten, S. 39.
1348 *Kahler,* Massenzugriff der StA auf Kundendaten, S. 39.
1349 BVerfGE 5, 13 (16); BVerfGE 15, 288 (293); BVerfGE 16, 194 (199f.); BVerfGE 35, 185 (189); BVerfGE 61, 82 (113); HGR III./*Axer,* § 67 Rn. 18.
1350 *Kahler,* Massenzugriff der StA auf Kundendaten, S. 39.
1351 *Kochheim,* KriPoZ 2018, 314 (315), der zur Begründung auf BVerfGE 124, 43 (66) verweist. Das BVerfG stellt in dieser Entscheidung allerdings lediglich fest, dass das Zitiergebot für die Vorschriften der Beschlagnahme (§§ 94ff. StPO) nicht gilt, da diese vorkonstitutionelles Recht seien. Darüber hinaus dürfte sich der Gesetzgeber wohl der Beschränkung des RiS durch die Schaffung der Ermittlungsgeneralklauseln jedenfalls bewusst gewesen sein, da er sie in der Begründung zum Gesetzesentwurf ausdrücklich nennt, vgl. BT-Drs. 14/1484, S. 16.
1352 HStR Bd. IX/*Hillgruber,* § 201 Rn. 39.
1353 HStR Bd. IX/*Hillgruber,* § 201 Rn. 39.

lichen Gesetzesvorbehalt stehen.[1354] Für diese Auslegung spricht u.a. der Wortlaut des Art. 19 Abs. 1 S. 1 GG, der von Grundrechtseinschränkungen spricht.[1355] Auch diese Rechtsprechung des BVerfG ist mit einer ähnlichen Argumentation wie im Rahmen des Zitiergebotes in der Literatur kritisiert worden. Nach dieser Kritik spräche zwar der Wortlaut des Art. 19 Abs. 1 S. 1 GG für eine Begrenzung des Anwendungsbereichs, dagegen fehle es an einem sachlichen Grund hierfür.[1356] Denn der Sinn und Zweck des Einzelfallgesetzverbotes – dass durch die gesetzliche Regelung eines Einzelfalls der Freiheitsanspruch eines Einzelnen in diskriminierender Weise verletzt werden könnte – würde auch bei allen anderen Grundrechten zutreffen.[1357] Diese von der Literatur vertretene Ansicht überzeugt, sodass hier eine gesetzliche Grundlage dem Verbot des Einzelfallgesetzes genügen muss.

Die hier gegenständlichen Ermittlungsgeneralklauseln lassen sich wohl als das rechtliche Gegenteil von Einzelfallgesetzen auffassen, sodass hiermit jedenfalls Art. 19 Abs. 1 S. 1 GG gewahrt ist.

III. Wesensgehaltsgarantie, Art. 19 Abs. 2 GG

Ferner setzt Art. 19 Abs. 2 GG voraus, dass der Wesensgehalt eines Grundrechts in keinem Fall angetastet wird.[1358]

Unklar ist in diesem Zusammenhang wiederum, ob dies nur für Grundrechte mit ausdrücklichem Gesetzesvorbehalt gilt oder für alle Grundrechte Anwendung findet.[1359] Gegen einen eingeschränkten Anwendungsbereich sprechen allerdings folgende, überzeugende Gründe:

Anders als Art. 19 Abs. 1 GG spricht bereits der Wortlaut für eine Anwendung auf alle Grundrechte, da diese in „keinem Fall" in ihrem „Wesensgehalt angetastet werden" dürfen.[1360] Dies überzeugt auch aus systematischer Sicht, da die Wesensgehaltsgarantie in einem eigenen Absatz des Art. 19 GG

1354 HStR Bd. IX/*Hillgruber,* § 201 Rn. 40; BeckOK-GG/*Enders,* Art. 19 Rn. 5; Dürig/Herzog/Scholz/*Remmert,* Art. 19 Rn. 29 mit einer Aufzählung, welche Grundrechte insoweit unmittelbar vom Anwendungsbereich des Art. 19 Abs. 1, S. 1 GG erfasst sind.

1355 So Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. 1 Rn. 30.

1356 HGR III/*Lege,* § 66 Rn. 118; HStR Bd. IX/*Hillgruber,* § 201, Rn. 40; ähnlich auch Dürig/Herzog/Scholz/*Remmert,* Art. 19 Rn. 31.

1357 HStR Bd. IX/*Hillgruber,* § 201, Rn. 40.

1358 HStR Bd. IX/*Hillgruber,* § 201, Rn. 98.

1359 BeckOK-GG/*Enders,* Art. 19 Rn. 21ff.

1360 Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. 2 Rn. 22.

enthalten ist und dies insoweit gegen einen einheitlich zu bestimmenden Anwendungsbereich von Art. 19 Abs. 1 und Abs. 2 GG spricht.[1361] Schließlich spricht auch der Sinn und Zweck des Art. 19 Abs. 2 GG, der ein „Leerlaufen" von Grundrechten verhindern soll, gegen eine Beschränkung des Anwendungsbereichs.[1362] Daher wird hier nicht von einem nur auf bestimmte Grundrechte beschränkten Anwendungsbereich ausgegangen, sodass die Wesensgehaltsgarantie auch für Beschränkungen des RiS gilt.

Durch die Wesensgehaltsgarantie geschützt ist insbesondere das individuelle subjektive Grundrecht des Einzelnen, da die Wesensgehaltsgarantie absolute Geltung beansprucht und insoweit ein objektives Verständnis nicht maßgeblich sein kann.[1363] Darüber hinaus gilt die Wesensgehaltsgarantie aber auch flankierend für den objektiven Gehalt von Grundrechten, um eine strukturelle Freiheitssicherung zu gewährleisten.[1364]

Inhaltlich schützt die Wesensgehaltsgarantie den Kernbestand von Grundrechten und insoweit ein Mindestmaß des tatbestandlich geschützten Schutzbereichs. Dieser Kernbestand ist für jedes Grundrecht autonom zu ermitteln.[1365] So ist etwa insbesondere der für das allgemeine Persönlichkeitsrecht abgeleitete Kernbereich privater Lebensgestaltung absolut geschützt und daher eingriffsresistent.[1366] Weiterhin darf der Mensch keinesfalls zum „bloßen Objekt der Staatsgewalt werden, indem, durch die Art der ergriffenen Maßnahmen die Subjektqualität grundsätzlich in Frage gestellt wird'"[1367]. Hiernach ist jedenfalls die Grenze bei einer staatlichen Rundumüberwachung erreicht.[1368]

Da auf die Ermittlungsgeneralklauseln nach einhelliger Auffassung nur geringfügige Grundrechtseingriffe gestützt werden können, ist jedenfalls der wesentliche Kernbereich des RiS – insbesondere die Grenze der staatlichen Rundumüberwachung – hierdurch nicht berührt. Dass eine derartige staatliche Rundumüberwachung jedenfalls nicht nach § 161 StPO zulässig sein kann, ergibt sich bereits aus einem einfachen Vergleich: denn nach

1361 Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. Rn. 22.
1362 Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. Rn. 22.
1363 HStR Bd. IX/*Hillgruber,* § 201, Rn. 102f.; Dürig/Herzog/Scholz/*Remmert,* Art. 19 Abs. 2 Rn. 20.
1364 HStR Bd. IX/*Hillgruber,* § 201, Rn. 102f.
1365 HStR Bd. IX/*Hillgruber,* § 201, Rn. 101.
1366 HGR Bd. IV/*Rudolf,* § 90, Rn. 67.
1367 HGR Bd. IV/*Rudolf,* § 90, Rn. 67 mit Verweis auf BVerfGE 109, 279 (312f.).
1368 HGR Bd. IV/*Rudolf,* § 90, Rn. 67.

§ 161 StPO ist zwar die kurzfristige Observation grundsätzlich zulässig[1369], eine längerfristige Observation bedarf nach § 163f Abs. 1 StPO jedoch gesteigerten Anforderungen.[1370]

IV. Parlamentsvorbehalt und Wesentlichkeitslehre

Im engen Zusammenhang mit der Wesensgehaltsgarantie und dem nachfolgend dargestellten Bestimmtheitsgebot stehen darüber hinaus die Anforderungen des Parlamentsvorbehalts und der Wesentlichkeitslehre.[1371]

Der vom BVerfG entwickelte Parlamentsvorbehalt geht über den allgemeinen Gesetzesvorbehalt dahingehend hinaus, dass für bestimmte Regelungen und Entscheidungen eine parlamentarische Entscheidung erforderlich ist.[1372] Ein solcher Parlamentsvorbehalt kann insbesondere bei Eingriffen in das allgemeine Persönlichkeitsrecht relevant werden und damit auch für Beschränkungen des RiS notwendig sein.[1373] Grund hierfür ist die demokratische Legitimation, denn im Bereich von grundrechtsrelevanten Eingriffen muss der demokratisch legitimierte Gesetzgeber die wesentlichen Entscheidungen selbst treffen.[1374]

Der Parlamentsvorbehalt steht in engem Zusammenhang mit der vom BVerfG entwickelten Wesentlichkeitslehre.[1375] Denn der Parlamentsvorbehalt wird durch die Wesentlichkeitslehre ausgefüllt.[1376] Nach der Wesentlichkeitstheorie muss der parlamentarische Gesetzgeber in grundlegenden normativen Bereichen, insbesondere im Bereich der Grundrechtsausübung die wesentlichen Entscheidungen selbst treffen.[1377] Dies beinhaltet insoweit auch ein Delegationsverbot an den parlamentarischen Gesetzgeber – er

1369 BeckOK-StPO/*Sackreuther,* § 161 Rn. 11.
1370 Siehe hierzu und zu weiteren Abgrenzungen und Vergleichen der nach § 161 StPO zulässigen Ermittlungsmaßnahmen im Verhältnis zu den speziell geregelten Ermittlungsmaßnahmen nachfolgend ausführlich unter Kap. 5, D.II.1.
1371 *Kielmansegg*, JuS 2009, 118 (121).
1372 HStR Bd. V/*Ossenbühl,* § 101 Rn. 14; *Kielmansegg*, JuS 2009, 118 (119); *Voßkuhle*, JuS 2007, 118 (119).
1373 Stern-Becker-GG/*Horn,* Art. 2 Rn. 97.
1374 *Kielmansegg*, JuS 2009, 118 (121).
1375 HStR Bd. V/*Ossenbühl,* § 101 Rn. 53.
1376 HStR Bd. V/*Ossenbühl,* § 101 Rn. 53.
1377 *Voßkuhle*, JuS 2007, 118 (119).

kann die wesentlichen Entscheidungen nicht delegieren und muss sie selbst treffen.[1378]

Problematisch ist in diesem Zusammenhang allerdings die Abgrenzungsfrage, ab wann eine „wesentliche" Entscheidung vorliegt.[1379] Eine klare Abgrenzungslinie dieser Frage dürfte in der Regel wohl kaum möglich sein.[1380] Das BVerfG hat in diesem Zusammenhang festgesetzt, dass jedenfalls die wesentlichen Entscheidungen in den offenliegenden Rechtssphären im Bereich der Grundrechtsausübung vom Gesetzgeber selbst getroffen werden müssen.[1381] Insofern muss der Gesetzgeber insbesondere die Abwägung zwischen Gemeinschaftsinteressen und den Freiheitsrechten des Einzelnen selbst treffen.[1382]

Dementsprechend muss bei den einschlägigen Ermittlungsgeneralklauseln die wesentliche Abwägung der widerstreitenden Interessen durch den parlamentarischen Gesetzgeber vorgenommen worden sein. Widerstreitende Interessen sind hier das berechtigte Interesse an einer effektiven Strafverfolgung, wozu auch die Möglichkeit gehört, auf neue Kriminalitätsformen mit neuen Ermittlungsmethoden angemessen reagieren zu können.[1383] Dem steht das ebenfalls berechtigte Interesse der von Grundrechtseingriffen betroffenen Personen entgegen, nicht unberechtigt Gegenstand intensiver Grundrechtseingriffe zu werden. Da der Gesetzgeber hier ausdrücklich auf lediglich begrenzte Grundrechtseingriffe abstellt und diese im Verhältnis zum Interesse an effektiver Strafverfolgung als angemessen betrachtet[1384], ist der Parlamentsvorbehalt und in dessen Rahmen die Wesentlichkeitslehre durch die einschlägigen Ermittlungsgeneralklauseln gewahrt.

V. Bestimmtheitsgebot

Darüber hinaus setzt das Bestimmtheitsgebot bzw. Gebot der Normenklarheit, das vom BVerfG teilweise aus dem Rechtsstaatsprinzip und teilweise aus den einzelnen Grundrechten (in Verbindung mit dem Rechtsstaats-

1378 HStR Bd. V/*Ossenbühl,* § 101 Rn. 53.
1379 HStR Bd. V/*Ossenbühl,* § 101 Rn. 53; *Voßkuhle*, JuS 2007, 118 (119).
1380 HStR Bd. V/*Ossenbühl,* § 101 Rn. 53.
1381 BVerfG NJW 1978, 807 (810).
1382 BVerfG NJW 1976, 1309 (1310).
1383 BT-Drs. 14/1484, S. 17.
1384 BT-Drs. 14/1484, S. 17.

prinzip) abgeleitet wird[1385]„ voraus, dass eine gesetzliche Grundlage, die zu Eingriffen in Grundrechte ermächtigt, Anlass, Zweck und Grenzen von Grundrechtseingriffen bereichsspezifisch, präzise und bestimmt regeln muss.[1386] Dabei beinhaltet das Bestimmtheitsgebot kein Optimierungsgebot[1387], erforderlich ist aber jedenfalls, dass sich die Voraussetzungen und Rechtsfolgen einer gesetzlichen Ermächtigung hinreichend klar aus der gesetzlichen Bestimmung unter Anwendung der üblichen juristischen Auslegungsmethoden ergeben.[1388] Beurteilungsmaßstab ist dabei der Bürger als Normadressat.[1389] Die Anforderungen an das Maß der Bestimmtheit sind dabei nicht einheitlich, sondern hängen insbesondere von der Intensität des jeweiligen Grundrechtseingriffs und dem jeweiligen Regelungsgegenstand ab.[1390]

Das Bestimmtheitsgebot verfolgt insgesamt drei Funktionen[1391]: zunächst soll staatliches Handeln für den betroffenen Bürger vorhersehbar und berechenbar sein (erste Funktion).[1392] Außerdem soll im Bereich der Grundrechtseingriffe der parlamentarische Gesetzgeber auf Grund der erforderlichen Gewaltenteilung der Exekutive steuernde Handlungsmaßstäbe vorgeben (zweite Funktion).[1393] Schließlich soll das Bestimmtheitsgebot die gerichtliche Justitiabilität gewährleisten (dritte Funktion).[1394]

Für Eingriffe in das RiS hat das Bestimmtheitsgebot darüber hinaus die spezifische Funktion, dass der Verwendungszweck der betroffenen Informationen präzise zu umgrenzen ist, um das verfassungsrechtliche

1385 Vgl. zur unterschiedlichen Herleitung *Bauer*, Soziale Netzwerke, S. 70 mit Verweisen für eine Herleitung aus den jeweiligen Grundrechten auf BVerfGE 110, 33 (53); BVerfGE 113, 348 (375); BVerfGE 118, 168 (186); für eine Herleitung aus dem Rechtsstaatsprinzip mit Verweisen auf BVerfGE 115, 320 (365); BVerfGE 120, 274 (315f.); BVerfGE 120, 378 (407).

1386 BVerfGE 100, 313 (359f.); BVerfGE 110, 33 (53); *Bauer*, Soziale Netzwerke, S. 69; *Kielmansegg*, JuS 2009, 118 (121).

1387 *Bauer*, Soziale Netzwerke, S. 72; Dürig/Herzog/Scholz/*Grzeszick,* Art. 20 VII. Rn. 61.

1388 *Bauer*, Soziale Netzwerke, S. 72; Dürig/Herzog/Scholz/*Grzeszick,* Art. 20 VII. Rn. 61; *Kielmansegg*, JuS 2009, 118 (121).

1389 *Bauer*, Soziale Netzwerke, S. 72.

1390 BVerfGE 110, 33 (55); BVerfGE 120, 378 (408); BVerfGE 125, 260 (328); *Bauer*, Soziale Netzwerke, S. 73; Dürig/Herzog/Scholz/*Grzeszick*, Art. 20 VII. Rn. 59f.

1391 Siehe hierzu ausführlich *Bauer*, Soziale Netzwerke, S. 71 m.w.N.

1392 Siehe hierzu ausführlich *Bauer*, Soziale Netzwerke, S. 71 m.w.N.

1393 Siehe hierzu ausführlich *Bauer*, Soziale Netzwerke, S. 71 m.w.N.

1394 Siehe hierzu ausführlich *Bauer*, Soziale Netzwerke, S. 71 m.w.N.

Gebot der Zweckbindung der erhobenen Informationen zu verstärken.[1395] Dieses Gebot erstreckt sich dabei bei gestuften Eingriffen in das RiS oder bei „gegliederten Formen des Informationsaustausches"[1396] auf jede dieser Stufen.[1397] Dies begründet das BVerfG damit, dass die persönlichkeitsrelevante Bedeutung der Informationserhebung erst dadurch erkennbar wird, dass der Betroffene Kenntnis über die Verwendung und deren Grenzen erlangt.[1398] Dabei differenziert das BVerfG in seinen Anforderungen allerdings zwischen „personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben und verarbeitet werden […] und solchen, die für statistische Zwecke bestimmt sind"[1399], da es eine Wesenseigenschaft der Statistik sei, dass die Auswertung der erhobenen Daten nicht von vorneherein festgelegt werden könne.[1400] Daher müssen nach dem BVerfG der statistischen Datenverarbeitung klar definierte Verarbeitungsschranken entgegengesetzt werden, um sicherzustellen, dass der Einzelne nicht zum bloßen Informationsobjekt werde.[1401]

Für Eingriffe in das RiS muss daher mindestens in der gesetzlichen Grundlage angegeben sein, welche staatliche Stelle zur Erfüllung welcher Aufgabe zur jeweiligen Informationserhebung berechtigt sein soll.[1402]

Das Bestimmtheitsgebot steht im Spannungsverhältnis zum Gebot abstrakt-genereller gesetzlicher Regelungen.[1403] Der Gesetzgeber darf sich daher auch unbestimmter Rechtsbegriffe bedienen, soweit diese durch die juristische Auslegung konkretisiert werden können und verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justitiabilität des Handelns gefährdet sind.[1404]

Möglich sind insoweit auch Generalklauseln.[1405] Sie können allerdings nur geringfügige Grundrechtseingriffe rechtfertigen und solche, die nicht dem Eingriffsszenario bzw. dem Ausforschungspotenzial einer speziell geregelten Ermittlungsmaßnahme ähneln.[1406] So hat das BVerfG insbesondere

1395 BVerfGE 130, 151 (202).
1396 BVerfGE 130, 151 (202).
1397 BVerfGE 130, 151 (202).
1398 BVerfGE 65, 1 (45).
1399 BVerfGE 65, 1 (45).
1400 BVerfGE 65, 1 (47).
1401 BVerfGE 65, 1 (48).
1402 BVerfGE 118, 168 (188).
1403 *Kielmansegg*, JuS 2009, 118 (121).
1404 BVerfGE 118, 168 (188).
1405 Siehe hierzu ausführlich *Bauer*, Soziale Netzwerke, S. 78 m.w.N.
1406 *Bauer*, Soziale Netzwerke, S. 78 m.w.N.

angenommen, dass das Bestimmtheitsgebot auch für die strafprozessuale Ermittlungsgeneralklausel des § 161 Abs. 1 StPO gewahrt ist, wenn auf dieser Grundlage Kundendaten bei Kreditkartenunternehmen abgefragt würden, die vorher genau bezeichnet wurden.[1407] Denn auch wenn die Möglichkeiten der Datenerhebungen und des Datenumfangs weit gefasst sind, seien die Ermittlungen der StPO streng auf den Zweck der Aufklärung und Verfolgung von Straftaten begrenzt.[1408]

Dementsprechend sind die hier einschlägigen Ermittlungsgeneralklauseln zwar eine relativ unbestimmte Ermächtigungsgrundlage, genügen aber trotzdem den Anforderungen an das Bestimmtheitsgebot, da einerseits nur geringfügige Grundrechtseingriffe hierdurch gerechtfertigt werden können und andererseits eine hinreichend bestimmte Zweckbegrenzung besteht.[1409]

VI. Verhältnismäßigkeitsgrundsatz

Schließlich hat das BVerfG – wiederum teilweise aus dem Rechtsstaatsprinzip und teilweise aus den Grundrechten selbst[1410] – den Grundsatz der Verhältnismäßigkeit als Grenze der Einschränkbarkeit von Grundrechten abgeleitet.[1411] Der Verhältnismäßigkeitsgrundsatz bildet den Hauptmaßstab für die Einschränkung von Grundrechten.[1412] Hiernach muss bei der Einschränkung von Grundrechten ein legitimer Zweck verfolgt werden, das gewählte Mittel geeignet und erforderlich sein, um das Ziel zu erreichen und muss auch im engeren Sinne verhältnismäßig bzw. angemessen sein

1407 BVerfG NJW 2009, 1405 (1407). Fraglich ist, ob das BVerfG nach seiner Rechtsprechungsänderung zur automatisierten KfZ-Kennzeichenerfassung (siehe hierzu bereits ausführlich oben unter Kap. 4, B.2.b)(1)iv.) an dieser Rechtsprechung festhalten wird, da es im hier zitierten Urteil noch davon ausgeht, dass ein Eingriff in das RiS lediglich für die übermittelten Daten besteht und nicht für alle anderen Daten. Die oben ausführlich dargestellte Argumentation des BVerfG, dass ein Eingriff in das RiS auch für sog. „Nichttreffer" besteht, da andernfalls die Maßnahme wirkungslos sei und daher auch ein spezifisches Interesse an den „Nichttreffern" bestünde, könnte auch in diesem Zusammenhang Anwendung finden.

1408 BVerfG NJW 2009, 1405 (1407).

1409 So auch *Bauer,* Soziale Netzwerke, S. 123, ebenfalls mit Verweis auf BVerfG NJW 2009, 1405 (1407);*Buermeyer,* Informationelle Selbstbestimmung und effektiver Strafvollzug, S. 174f.; vgl. insbesondere BT-Drs. 14/1484, S. 16.

1410 So etwa BVerfGE 65, 1 (44); Siehe hierzu *Hufen,* Staatsrecht II, § 9 Rn. 15f.

1411 HStR Bd. IX/*Hillgruber,* § 201 Rn. 51.

1412 HStR Bd. IX/*Hillgruber,* § 201 Rn. 52 mit Verweis auf BVerfGE 75, 108 (154f.); BVerfGE 80, 137 (153); BVerfGE 90, 145 (172).

– darf also nicht außer Verhältnis zu der mit der Maßnahme einhergehenden Grundrechtseinschränkung stehen.[1413] Insoweit hat das BVerfG den allgemeinen grundrechtlichen Gesetzesvorbehalt zu einem Vorbehalt eines verhältnismäßigen Gesetzes ausgebaut.[1414] Im Kern dient dieser Grundsatz damit der Abwägung der widerstreitenden Interessen und insoweit einer Zweck-Mittel-Relation.[1415] Dabei beschränkt sich die gerichtliche Überprüfbarkeit allerdings darauf, dass die Maßnahme und deren Grundrechtseingriff nicht außer Verhältnis zum mit ihr verfolgten Zweck stehen darf und damit auf eine Negativ-Prüfung – eine positive Prüfung, dass die Zweck-Mittel-Relation verhältnismäßig ist, wird dagegen nicht vorgenommen.[1416] Außerdem muss sowohl die gesetzliche Grundlage, auf deren Grundlage die Maßnahme beruht, als auch die Anwendung der konkreten Einzelfallmaßnahme dem Grundsatz der Verhältnismäßigkeit genügen.[1417]

1. Legitimer Zweck, Geeignetheit und Erforderlichkeit

Ob ein legitimer Zweck verfolgt wird, kann ebenfalls nur negativ festgestellt werden.[1418] Denn grundsätzlich ist der Gesetzgeber frei in der Festlegung seiner Zwecke, soweit der Zweck nicht verfassungswidrig ist.[1419] Damit ergibt sich die Negativdefinition, dass „legitim […] grundsätzlich jedes öffentliche Interesse [ist], das verfassungsrechtlich nicht ausgeschlossen ist“[1420]. Das Bedürfnis nach wirksamer Strafverfolgung und Verbrechensbekämpfung ist daher ein legitimer Zweck.[1421]

Die Geeignetheit setzt voraus, dass das gewählte Mittel den anvisierten Zweck mindestens fördern kann.[1422] Im Rahmen der Geeignetheit besteht ebenso wie beim legitimen Zweck ein weiter Einschätzungsspielraum des

1413 HStR Bd. IX/*Hillgruber,* § 201 Rn. 51.
1414 HStR Bd. IX/*Hillgruber,* § 201 Rn. 53.
1415 HStR Bd. IX/*Hillgruber,* § 201 Rn. 51.
1416 *Bauer*, Soziale Netzwerke, S. 88 mit Verweis auf BVerfGE 120, 378 (428); BVerfGE 124, 43 (62).
1417 *Bauer*, Soziale Netzwerke, S. 94.
1418 HStR Bd. IX/*Hillgruber,* § 201 Rn. 55.
1419 HStR Bd. IX/*Hillgruber,* § 201 Rn. 54.
1420 HStR Bd. IX/*Hillgruber,* § 201 Rn. 54 mit Verweis auf BVerfGE 124, 300 (331).
1421 BVerfGE 107, 299 (316); BVerfGE 100, 313 (389) m.w.N.; BeckOK-InfoMedienR/*Gersdorf,* GG Art. 2 Rn. 75; *Bauer*, Soziale Netzwerke, S. 89; *Eisenmenger,* Grundrechtsrelvanz virtueller Streifenfahrten, S. 268.
1422 HStR Bd. IX/*Hillgruber,* § 201 Rn. 61.

Gesetzgebers.[1423] Ungeeignet ist daher nur ein Mittel, wenn es „von vornherein untauglich" ist, das bezweckte Ziel zu erreichen oder zu fördern.[1424]

Die Anforderung der Erforderlichkeit setzt voraus, dass kein sachlich ebenso geeignetes, aber weniger grundrechtsbeschränkendes Mittel besteht.[1425] Auch hier besteht ein weiter Einschätzungsspielraum des Gesetzgebers.[1426] Insoweit darf kein weiteres Mittel bestehen, dass bei gleicher Eignung zur Erreichung des Zwecks, Grundrechte weniger beschränkt.[1427]

Auf Grund der sich ständig wandelnden Kriminalitätsformen, ist es für die Strafverfolgungsbehörden auch notwendig, ohne jeweils langwierige Gesetzgebungsprozesse angemessen auf neue Kriminalitätsformen reagieren zu können.[1428] Hierzu ist insoweit eine gesetzliche Ermächtigungsgrundlage erforderlich, auf die derartig neue Ermittlungsmethoden gestützt werden können. Insoweit liegt in der Schaffung einer Generalermittlungsklausel ein legitimer Zweck, der geeignet und erforderlich ist, vor.[1429]

2. Verhältnismäßigkeit im engeren Sinne bzw. Angemessenheit

Kern jeder Verhältnismäßigkeitsprüfung ist die Prüfung der sog. Verhältnismäßigkeit im engeren Sinne bzw. der Angemessenheit. Erforderlich ist nach der ständigen Rechtsprechung des BVerfG, dass „die Einbußen an grundrechtlich geschützter Freiheit nicht in einem unangemessenen Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient."[1430] Insoweit müssen die dem Einzelnen möglicherweise erwachsenden Grundrechtsbeschränkungen gegen die der Allgemeinheit hieraus erwachsenden Vorteile in einer Gesamtabwägung aller Umstände miteinander abgewogen werden und dürfen nicht außer Verhältnis stehen.[1431] Erforderlich ist daher einerseits eine Bewertung der Intensität

1423 HStR Bd. IX/*Hillgruber,* § 201 Rn. 66.
1424 BVerfGE 100, 313 (373); *Bauer*, Soziale Netzwerke, S. 89.
1425 HStR Bd. IX/*Hillgruber,* § 201 Rn. 63.
1426 *Bauer*, Soziale Netzwerke, S. 90; HStR Bd. IX/*Hillgruber,* § 201 Rn. 66.
1427 HStR Bd. IX/*Hillgruber,* § 201 Rn. 64.
1428 Vgl. *Kahler,* Massenzugriff der StA auf Kundendaten, S. 124.
1429 Vgl. *Kahler,* Massenzugriff der StA auf Kundendaten, S. 124.
1430 BVerfGE 90, 145 (173); BVerfGE 109, 279 (349ff.); BVerfGE 100, 313 (375f.); BVerfGE 120, 274 (321f.); *Bauer*, Soziale Netzwerke, S. 91.
1431 BVerfGE 90, 145 (173); HStR Bd. IX/*Hillgruber,* § 201 Rn. 72 m.w.N.

der Grundrechtseingriffe und andererseits eine Bewertung, ob diese nicht außer Verhältnis zu dem angestrebten Zweck steht.[1432]

Insoweit stehen sich im Rahmen der Ermittlungsgeneralklauseln einerseits das berechtigte Interesse an einer effektiven Strafverfolgung, für die gerade auch Generalklauseln erforderlich sind, und der grundrechtliche Schutz der von den Ermittlungsmaßnahmen betroffenen Personen entgegen. Da die Ermittlungsgeneralklauseln weder an gesteigerte Verdachtsmomente noch an bestimmte, (besonders) schwere Straftaten anknüpfen, rechtfertigen sie nur Grundrechtseingriffe mit geringer Intensität. Da insoweit die Ermittlungsmöglichkeiten, die auf §§ 161, 163 StPO gestützt werden können, hinreichend begrenzt sind, besteht durch die Ermittlungsgeneralklauseln ein angemessenes Verhältnis dieser widerstreitenden Interessen.

VII. Zwischenergebnis

Die Ermittlungsgeneralklauseln der §§ 161, 163 StPO stellen grundsätzlich eine ausreichende, gesetzliche Grundlage zur Rechtfertigung von Eingriffen in das RiS dar, auf die die Auswertungsmethoden gestützt werden könnten. Als Folgen der verfassungsrechtlichen Anforderungen – insbesondere des Bestimmtheits- und Verhältnismäßigkeitsgrundsatzes – ist jedoch festzuhalten, dass §§ 161, 163 StPO nur zu geringfügigen Grundrechtseingriffen ermächtigt, sodass nachfolgend auch eingehend zu untersuchen ist, ob bei der Anwendung der Auswertungsmethoden ein solcher, geringfügiger Grundrechtseingriff vorliegt.

D. Können die gegenständlichen Auswertungsmethoden zulässigerweise auf §§ 161, 163 StPO gestützt werden?

Nach der vorstehend ausführlich untersuchten Einschlägigkeit und Verfassungsmäßigkeit der Ermittlungsgeneralklauseln, muss nun untersucht werden, ob die Auswertungsmethoden auch zulässigerweise auf die Ermittlungsgeneralklauseln gestützt werden können. Hierzu müssen die Voraussetzungen der Ermittlungsgeneralklauseln erfüllt sein.

Nach herrschender Auffassung setzt § 161 Abs. 1 StPO lediglich voraus, dass ein Anfangsverdacht vorliegt (hierzu unter I.) und, dass die jeweiligen

1432 HStR Bd. IX/*Hillgruber,* § 201 Rn. 72.

Ermittlungshandlungen nur einen geringfügigen Grundrechtseingriff darstellen (hierzu unter II.).[1433]

I. Anfangsverdacht

Nach § 161 Abs. 1 S. 1 StPO dürfen „Ermittlungen jeder Art" nur „zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck" vorgenommen werden. § 160 Abs. 1 bis 3 StPO enthält den sog. Ermittlungs- und Untersuchungsgrundsatz und bestimmt, dass die Staatsanwaltschaft zur Erforschung des Sachverhalts verpflichtet ist, wenn sie „durch eine Anzeige oder auf anderem Weg von dem Verdacht einer Straftat Kenntnis"[1434] erlangt.[1435] § 160 Abs. 2 und Abs. 3 StPO bestimmen darüber hinaus den Umfang dieser Ermittlungspflicht und bestimmen insoweit, dass die Staatsanwaltschaft auch zur Ermittlung von entlastenden Tatsachen und der für die Bestimmung der Rechtsfolgen erforderlichen Tatsachen verpflichtet ist.

Auf Grund der Verweisung des § 161 Abs. 1 S. 1 StPO auf § 160 Abs. 1 StPO ist für § 161 Abs. 1 StPO das Vorliegen eines Anfangsverdachts erforderlich und damit das Vorliegen zureichender tatsächlicher Anhaltspunkte einer Straftat im Sinne des § 152 Abs. 2 StPO.[1436]

Da die hier gegenständlichen Auswertungsmethoden in der Ermittlungspraxis sowohl eingesetzt werden können, um die Identität der jeweils beteiligten *Entitäten* zu ermitteln als auch, um entweder den Verdacht einer Straftat zu begründen oder bei Einsatz der Auswertungsmethoden unmittelbar den Verdacht einer Straftat zu begründen[1437], stellt sich hier insbesondere die Frage, welche Anforderungen an das Vorliegen eines Anfangsverdachts gestellt werden müssen.

1433 BeckOK-StPO/*Sackreuther,* § 161 Rn. 4; Meyer-Goßner/Schmitt/*Köhler,* § 161 Rn. 1; MüKo-StPO/*Kölbel,* § 161 Rn. 7; *Petri*, StV 2007, 266 (267).

1434 So der Wortlaut des § 160 Abs. 1 StPO.

1435 BeckOK-StPO/*Sackreuther,* § 160 Rn. 1.

1436 BVerfG NJW 2009, 1405 (1407); BeckOK-StPO/*Sackreuther,* § 161 Rn. 4; *Bauer*, Soziale Netzwerke, S. 123.

1437 Siehe zu den verschiedenen Einsatzmöglichkeiten in der Ermittlungspraxis ausführlich oben unter Kap. 5, A.

I. Voraussetzungen eines Anfangsverdachts

Der Anfangsverdacht setzt nach § 152 Abs. 2 zureichende tatsächliche Anhaltspunkte dafür voraus, dass eine Straftat begangen worden ist.[1438]

a) Kein Anfangsverdacht beim proaktiven Aufklären von Dunkelfeldern

Diese Anhaltspunkte müssen bei den Strafverfolgungsbehörden vorliegen, bevor Ermittlungsmaßnahmen, durch die in Grundrechte eingegriffen wird, angewendet werden. Ermittlungsgeneralklauseln – und alle anderen Ermittlungsbefugnisse der StPO – können daher nicht angewendet werden, um bisherige Dunkelfelder proaktiv aufzuhellen.[1439]

b) Objektive Anhaltspunkte

Zureichende tatsächliche Anhaltspunkte im Sinne des § 152 Abs. 2 StPO setzten voraus, dass objektive Anhaltspunkte bestehen, die nach kriminalistischer Erfahrung das Vorliegen einer Straftat als möglich erscheinen lassen.[1440] Ausreichend sind aber Anhaltspunkte, aus denen sich auch nur eine geringe Wahrscheinlichkeit einer Straftat ergibt.[1441] Insoweit können grundsätzlich auch noch ungeprüfte Angaben, Gerüchte und einseitige Behauptungen ausreichen, um einen Anfangsverdacht zu begründen.[1442] Denn das Ermittlungsverfahren dient gerade zur Klärung des Anfangsverdachts.[1443]

1438 BGH NJW 1994, 2839 (2849); *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 257.

1439 SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6; Löwe-Rosenberg/*Mavany,* § 152 Rn. 28, 53; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 251.

1440 SK-StPO/*Weßlau/Deiters,* § 152 Rn. 12; Gercke/Julius/Temming/Zöller/*Zöller,* § 152 Rn. 12; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 128; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13.

1441 Löwe-Rosenberg/*Mavany,* § 152 Rn. 30; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13f.

1442 Löwe-Rosenberg/*Mavany,* § 152 Rn. 30; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13f.

1443 Löwe-Rosenberg/*Mavany,* § 152 Rn. 30; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13f.

Nicht ausreichend sind dagegen bloße hypothetische Vermutungen – insbesondere, wenn hierdurch große Teile des sozialen Lebens durchleuchtet werden, nur weil die Möglichkeit besteht, dass dabei Straftaten ermittelt werden können.[1444]

Außerdem nicht ausreichend sind offensichtlich haltlose Behauptungen, worunter insbesondere Behauptungen von bekannten Querulanten fallen sollen.[1445]

c) Hindeuten auf eine konkrete Straftat

Die Tatsachengrundlage muss außerdem auf eine konkrete Straftat hindeuten.[1446] Nicht ausreichend ist insoweit, dass die allgemeine Möglichkeit der Straftatbegehung besteht.[1447]

So reicht es für einen Anfangsverdacht nicht aus, wenn etwa von einem bestimmten Ort statistische Anhaltspunkte dafür bestehen, dass dort eine erhöhte Anzahl von Straftaten in der Regel begangen werden.[1448]

Insoweit begrenzt das Erfordernis des Anfangsverdachts auch die Ermittlungstätigkeit der Strafverfolgungsbehörden.[1449] Denn Aufgabe des Ermittlungsverfahrens ist die Verdachtsklärung eines konkreten Anfangsverdachts einer konkreten Straftat.[1450] Die Ermittlungshandlungen müssen insoweit mit einer konkreten Straftat in Zusammenhang stehen oder mit ihr in Verbindung stehen und im weitesten Sinne beweisthematisch sein.[1451]

Nicht erforderlich ist dagegen, dass die Anhaltspunkte bereits auf eine bestimmte Person hindeuten.[1452] So muss und kann ein Ermittlungsverfahren auch gegen Unbekannt eingeleitet werden.[1453]

1444 Löwe-Rosenberg/*Mavany,* § 152 Rn. 28 m.w.N.
1445 Löwe-Rosenberg/*Mavany,* § 152 Rn. 31.
1446 Löwe-Rosenberg/*Mavany,* § 152 Rn. 32; *Haas*, Vorermittlungen und Anfangsverdacht, S. 16.
1447 Löwe-Rosenberg/*Mavany,* § 152 Rn. 32.
1448 *Singelnstein*, NStZ 2018, 1 (7).
1449 Löwe-Rosenberg/*Erb,* § 161 Rn. 45.
1450 Löwe-Rosenberg/*Erb,* § 161 Rn. 45.
1451 Löwe-Rosenberg/*Erb,* § 161 Rn. 45.
1452 Löwe-Rosenberg/*Mavany,* § 152 Rn. 30; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 13; *Haas*, Vorermittlungen und Anfangsverdacht, S. 16.
1453 Löwe-Rosenberg/*Mavany,* § 152 Rn. 30; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 13.

d) Exkurs – Vorermittlungen

Noch nicht abschließend geklärt ist, ob auch sog. Vorermittlungen überhaupt zulässig sind und, ob sie auf die Ermittlungsgeneralklauseln gestützt werden können.

Begrifflich muss zunächst festgelegt werden, dass hiermit – wie von der überwiegenden Literatur ebenfalls – die Situation bezeichnet wird, dass zwar bereits Anhaltspunkte für eine Straftat bestehen, diese aber noch nicht ausreichen, um einen Anfangsverdacht zu begründen.[1454] Insoweit werden in diesem Verfahrensstadium Ermittlungen der Strafverfolgungsbehörden vorgenommen, um die Frage zu klären, ob ein Anfangsverdacht vorliegt.[1455] Dies sind die sog. Vorermittlungen.

Abzugrenzen sind Vorermittlungen von sog. Vorfeld- bzw. Initiativermittlungen (nachfolgend einheitlich als „Vorfeldermittlungen" bezeichnet). Vorfeldermittlungen zeichnen sich gegenüber Vorermittlungen dadurch aus, dass ihr Ziel darin liegt, überhaupt erst Anhalts- oder Anknüpfungspunkte für einen Verdacht zu ermitteln, die zuvor noch nicht vorlagen.[1456] Insoweit besteht weitgehende Einigkeit darüber, dass Vorfeldermittlungen auf Grund des jedenfalls fehlenden Anfangsverdachts nicht als Ermittlungen auf die Befugnisse der Strafprozessordnung gestützt werden können.[1457]

Dagegen bestehen bei den Vorermittlungen bereits Anhaltspunkte für eine Straftat. Allerdings stellen sich für deren Zulässigkeit mehrere Fragen:

- Sind Vorermittlungen überhaupt zulässig?
- Bis zu welcher Grenze sind Vorermittlungen zulässig?
- Können Vorermittlungen auf die Ermittlungsgeneralklauseln gestützt werden?

Der Sinn und Zweck von Vorermittlungen besteht darin, zu klären, ob genügend Anhaltspunkte für eine Straftat dahingehend vorliegen, dass die Einleitung eines förmlichen Ermittlungsverfahrens geboten erscheint.[1458]

1454 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 127f.; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13; *Eisenmenger*, in: Grundrechtsrelevanz virtueller Streifenfahrten, S. 328.

1455 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 127f.; *Haas*, Vorermittlungen und Anfangsverdacht, S. 13; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252.

1456 *Eisenmenger*, :, S. 252; *Haas*, Vorermittlungen und Anfangsverdacht, S. 41f.

1457 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252 m.w.N.

1458 *Haas*, Vorermittlungen und Anfangsverdacht, S. 13.

Noch nicht vollständig geklärt, aber überwiegend anerkannt ist, dass die Strafverfolgungsbehörden bzw. die Staatsanwaltschaft zu diesem Zweck tätig werden dürfen.[1459] Zur Begründung wird insbesondere angeführt, dass hierfür zunächst die Existenz des § 159 StPO spreche[1460], der eine möglichst frühzeitige „Prüfung und Entscheidung darüber ermögliche[n][…] soll, ob ein Ermittlungsverfahren wegen eines Tötungsdelikts einzuleiten ist"[1461]. Für die Zulässigkeit der Vorermittlungsmaßnahmen soll außerdem sprechen, dass andernfalls keine dem Gleichheitssatz gerecht werdende Strafverfolgung gewährleistet sei, da es sonst vom Zufall abhänge, ob eine Strafanzeige ausreichend schlüssig begründet sei oder nicht.[1462] Insoweit ist grundsätzlich von der Zulässigkeit derartiger Vorermittlungen auszugehen.

Fraglich ist allerdings, zu welchen Ermittlungshandlungen die Staatsanwaltschaft im Rahmen dieser Vorermittlungen berechtigt ist. In der Regel werden hier beispielhaft Ermittlungshandlungen wie die informatorische Befragung[1463], das Anfordern von Gutachten und technischen Erkenntnissen[1464], die Nutzung offen zugänglicher Medienberichterstattung[1465] und formlose Fragen zur näheren Orientierung[1466] als zulässige Vorermittlungen genannt. Unklar ist jedoch, ob die Staatsanwaltschaft im Rahmen derartiger Vorermittlungen auch Maßnahmen ergreifen darf, die in Grundrechte eingreifen.

Die überwiegende Auffassung in der Literatur verneint dies.[1467] So sollen im Rahmen der Vorermittlungen nur solche Ermittlungen zulässig sein, durch die nicht in Grundrechte eingegriffen wird.[1468]

1459 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 129 m.w.N; Löwe-Rosenberg/*Erb,* Vor. §§ 158 ff. Rn. 17.

1460 Löwe-Rosenberg/*Erb,* Vor. §§ 158 ff. Rn. 17.

1461 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 129 m.w.N.

1462 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 129 m.w.N. Siehe zur Zulässigkeit strafprozessualer Vorermittlungen ausführlich *Haas*, Vorermittlungen und Anfangsverdacht.

1463 BGH NStZ 1983, 86; Gercke/Julius/Temming/Zöller/*Gercke,* § 152 Rn. 6; Löwe-Rosenberg/*Mavany,* § 152 Rn. 43.

1464 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130.

1465 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130.

1466 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130.

1467 Löwe-Rosenberg/*Erb,* Vor. §§ 158ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.; Gercke/Julius/Temming/Zöller/*Gercke,* § 152 Rn. 6.

1468 Löwe-Rosenberg/*Erb,* Vor. §§ 158ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.; Gercke/Julius/Temming/Zöller/*Gercke,* § 152 Rn. 6.

Abweichend hiervon wird teilweise auch vertreten, dass im Rahmen von Vorermittlungen lediglich Ermittlungen, deren Grundrechtsrelevanz unterhalb einer Bagatellschwelle liegt, zulässig sein sollen.[1469] Da hier allerdings – insbesondere auf Grund fehlender Trennschärfe – nicht von einem derartigen Bagatellvorbehalt im Rahmen des Eingriffs in Grundrechte ausgegangen wird[1470], muss insoweit auch die Zulässigkeit von Bagatelleingriffen im Rahmen von Vorermittlungen ausscheiden.

Somit sind allenfalls Ermittlungsmaßnahmen im Rahmen von Vorermittlungen zulässig, die nicht in Grundrechte eingreifen.[1471] Da nach der Rechtsprechung des BVerfG die grundsätzliche Kenntnisnahme von öffentlich zugänglichen Daten keinen Eingriff in das RiS darstellt, soweit nicht die Grenze einer gezielten Speicherung überschritten ist[1472], kommt insoweit etwa ein derartiger Datenabruf, der lediglich zur Orientierung der Strafverfolgungsbehörden dient, in Betracht.[1473]

Weitgehend einheitlich wird dagegen die Frage beantwortet, ob derartige Vorermittlungen auf die Ermittlungsgeneralklauseln gestützt werden können.[1474] Dies ist nicht der Fall, da die Ermittlungsgeneralklauseln gerade einen Anfangsverdacht voraussetzen.[1475] Wenn nämlich die nach den Ermittlungsgeneralklauseln zulässigen Ermittlungsmaßnahmen zur Klärung des Anfangsverdachts eingesetzt werden dürfen, wäre es widersprüchlich sie bereits vor dem Vorliegen des Anfangsverdachts anzuwenden.[1476]

Zusammenfassend ist festzuhalten, dass Vorermittlungen – also einzelne Ermittlungshandlungen der Staatsanwaltschaft zu Abklärung, ob die Voraussetzungen eines Anfangsverdachts vorliegen – zulässig sind, soweit hierdurch kein Grundrechtseingriff vorliegt. Diese Vorermittlungen können

1469 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130.
1470 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(2)i.
1471 Insoweit wäre allenfalls das Herunterladen der Blockchain-Daten im Rahmen derartiger Vorermittlungen möglich. Siehe zum Eingriff in das RiS beim Herunterladen von Blockchain-Daten bereits oben unter Kap. 4, B.II.2.c)(1).
1472 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b).
1473 Vgl. Löwe-Rosenberg/*Mavany,* § 152 Rn. 44.
1474 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130; Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.
1475 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130 Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.
1476 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130; Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.

allerdings nicht auf die Ermittlungsgeneralklauseln gestützt werden, da die hierfür erforderliche Schwelle des Anfangsverdachts noch nicht erreicht ist – sie soll ja gerade ermittelt werden.

e) Exkurs – Strafverfolgungsvorsorge

Ebenfalls viel diskutiert wurden Maßnahmen der sog. Strafverfolgungsvorsorge.[1477] Maßnahmen der Strafverfolgungsvorsorge sind solche, die der „Aufklärung von Delikten oder die Ermittlung von Verdächtigen von Delikten, die in der Zukunft erwartet werden, ermöglichen oder erleichtern soll"[1478].

Zu unterscheiden sind in diesem Zusammenhang zwei verschiedene Fallkonstellationen:

Einerseits besteht die Möglichkeit, unabhängig von einem konkreten Anfangsverdacht und einem konkreten Ermittlungsverfahren bereits Daten und Informationen zu erheben, um eine mögliche spätere Strafverfolgung zu erleichtern.[1479] Für die hier gegenständlichen Auswertungsmethoden könnte dies etwa der Fall sein, wenn für die in Kap. 3 B.I. dargestellte Auswertung von Netzwerkverbindungen zunächst auf Vorrat, unabhängig von einem konkreten Verdacht, die Verbindungsdaten eines Blockchain-Netzwerks erhoben werden[1480], um später – etwa in einem Verdachtsfall – durch die Auswertung dieser Verbindungsdaten eine *Bitcoin-Adresse* einer IP-Adresse zuzuordnen.

Andererseits besteht außerdem die Möglichkeit, die im Rahmen eines konkreten Ermittlungsverfahrens bereits erhobenen Daten der Auswertungsmethoden zu speichern, um diese in weiteren möglichen Strafverfahren zu verwenden.[1481] Dies könnte etwa der Fall sein, wenn entweder

1477 Siehe etwa *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 86ff.; *Bock*, ZIS 2006, 129 (129ff.); *Graulich*, NVwZ 2014, 685 (686) jeweils m.w.N.

1478 *Graulich*, NVwZ 2014, 685 (686). So auch *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 86f.; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 255.

1479 Vgl. *Graulich*, NVwZ 2014, 685 (686). Siehe zur rechtlichen Zulässigkeit derartiger Maßnahmen nach dem Strafprozessrecht sogleich.

1480 Siehe zur technischen Funktionsweise und der Notwendigkeit einer vorangehenden Speicherung der Netzwerkdaten oben unter Kap. 3, B.II.

1481 Vgl. *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 87; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 255f.

Erkenntnisse über die Identität hinter einer bestimmten *Bitcoin-Adresse* gespeichert werden oder, wenn Erkenntnisse über Hintergründe von bestimmten Transaktionen gespeichert werden. So wäre es insbesondere möglich, zu speichern, welche Transaktionen im Zusammenhang mit dem Verdacht von Geldwäsche stehen, um so die oben dargestellte Auswertungsmethode eines *Labelling*-Verfahrens[1482] mit diesen Transaktionsdaten zu „trainieren" und so weitere Transaktionen zu ermitteln, die möglicherweise im Zusammenhang mit Geldwäsche stehen.[1483]

Rechtlich umstritten war in diesem Zusammenhang insbesondere, ob Maßnahmen der Strafverfolgungsvorsorge dem präventiven Polizeirecht oder dem repressiven Strafprozessrecht zuzuordnen sind.[1484] Hintergrund dieser Streitfrage war die Frage danach, ob der Bundesgesetzgeber oder der jeweilige Landesgesetzgeber zur Regelung dieser Maßnahmen zuständig waren.[1485]

Denn nach Art. 74 Abs. 1 Nr. 1 GG liegt die konkurrierende Gesetzgebungskompetenz für das „gerichtliche Verfahren" beim Bundesgesetzgeber.[1486] Soweit Maßnahmen der Strafverfolgungsvorsorge also dem repressiven gerichtlichen Verfahren zuzuordnen sind und der Bundesgesetzgeber diese Maßnahmen im Rahmen der StPO rechtlich abschließend geregelt hat, könnte der Landesgesetzgeber insoweit keine Regelung hierzu erlassen.[1487]

Nach der Rechtsprechung des BVerfG sind Maßnahmen, die der Vorsorge noch gar nicht begangener, sondern in ungewisser Zukunft bevorstehender Straftaten dienen, Maßnahmen des gerichtlichen Verfahrens nach Art. 74 Abs. 1 Nr. 1 GG.[1488]

Zwar finden die Maßnahmen der Strafverfolgungsvorsorge zeitlich präventiv statt, betreffen aber gegenständlich das repressiv ausgerichtete Strafverfahren.[1489] Denn die so erhobenen Daten und Informationen sind dazu

1482 Siehe zur technischen Funktionsweise und der Notwendigkeit von Trainingsdaten von *Labelling*-Verfahren oben unter Kap. 3, A.III.3.
1483 Siehe zu dieser Auswertungsmöglichkeit bereits oben unter Kap. 3, A.III.3.
1484 Siehe hierzu ausführlich *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 87ff. m.w.N.
1485 Vgl. *Graulich*, NVwZ 2014, 685 (686ff.).
1486 BVerfGE 113, 348 (370f.); *Graulich*, NVwZ 2014, 685 (686f.).
1487 Vgl. BVerfGE 113, 348 (371).
1488 BVerfGE 113, 348 (369).
1489 BVerfGE 113, 348 (370).

bestimmt, in ungewisser Zukunft in ein Ermittlungs- oder Hauptverfahren einzufließen.[1490]

Insoweit sind Maßnahmen der Strafverfolgungsvorsorge dem Bereich des Strafverfahrens zuzuordnen. Daher ist auch zur erstmaligen Erhebung der jeweiligen Daten jedenfalls der Anfangsverdacht einer Straftat erforderlich.[1491]

Auf die Frage, ob die durch den Einsatz der Auswertungsmethoden ermittelten Erkenntnisse und Ergebnisse für künftige Strafverfahren gespeichert und genutzt werden dürfen, muss einer weiteren Untersuchung vorbehalten bleiben, dürfte sich jedoch wohl nach § 484 StPO richten.[1492]

f) Legales Verhalten zur Begründung eines Anfangsverdachts?

Problematisch und in Literatur und Rechtsprechung lange Zeit diskutiert wurde außerdem, inwieweit legales Verhalten einen Anfangsverdacht begründen kann.[1493] Unproblematisch ist das möglich, wenn bereits eine konkrete Straftat bekannt ist, die möglichen Täter aber noch unbekannt sind und insoweit das legale Verhalten lediglich auf die Tatbeteiligung einer bestimmten Person hindeutet.[1494]

Problematischer ist dagegen, ob auch ein legales Verhalten, das aber nach kriminalistischer Erfahrung oftmals in Verbindung mit der Begehung von Straftaten steht, einen Anfangsverdacht begründen kann.[1495]

Rechtsprechung und herrschende Literaturauffassung nehmen hier an, dass auch ein an sich legales Verhalten den Verdacht einer Straftat begründen kann – allerdings nur, wenn weitere Anhaltspunkte bestehen, die auf das Vorliegen einer Straftat hindeuten.[1496]

1490 BVerfGE 113, 348 (370).

1491 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 256; Vgl. *Bock*, ZIS 2006, 129 (132).

1492 Siehe hierzu nachfolgend ausführlich unter Kap. 5, D.I.2c)(1).

1493 Vgl. Löwe-Rosenberg/*Mavany,* § 152 Rn. 36; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 12e; vgl. BVerfG NJW 1994, 2079 (2079f.); *Hoven*, NStZ 2014, 361 (365f.).

1494 Löwe-Rosenberg/*Mavany,* § 152 Rn. 36; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 12e; *Hoven*, NStZ 2014, 361 (364f.).

1495 Löwe-Rosenberg/*Mavany,* § 152 Rn. 36; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 12e.

1496 Löwe-Rosenberg/*Mavany,* § 152 Rn. 36; SK-StPO/*Weßlau/Deiters,* § 152 Rn. 12e; BVerfG StV 2010, 665 (665f.); OLG Hamburg NJW 1984, 1635 (1635f.).

g) BVerfG NJW 2009, 1405ff. – Abfrage von Kreditkartendaten

Schließlich ist auch für die Bestimmung der Kriterien eines Anfangsverdachts auf den bereits angesprochenen[1497] Nichtannahmebeschluss des BVerfG 17.02.2009[1498] zur Abfrage von Kreditkartendaten einzugehen.[1499] Denn nach der Entscheidung des BVerfG reicht es für die nach §§ 161 Abs. 1, 152 Abs. 2 StPO erforderlichen zureichenden tatsächlichen Anhaltspunkte einer Straftat aus, wenn konkrete Tatumstände – wie etwa im Fall des BVerfG ein bestimmter Buchungsbetrag zugunsten eines bestimmten Zahlungsempfängers unter Angabe einer bestimmten Merchant-ID[1500] – vorliegen, die auf das Vorliegen einer Straftat hindeuten.

h) Zwischenergebnis

Ein Anfangsverdacht erfordert tatsächliche, objektive Anhaltspunkte, die nach kriminalistischer Erfahrung auf das Vorliegen einer konkreten Straftat hindeuten. Derartige Anhaltspunkte liegen nicht bei allgemeinen Dunkelfeldern vor, sodass § 161 Abs. 1 StPO nicht für das proaktive Aufhellen von Dunkelfeldern angewendet werden kann. Die erforderlichen, objektiven Tatumstände begrenzen darüber hinaus die Ermittlungsmaßnahmen dahingehend, dass sich diese auf die Klärung des konkreten Verdachts beschränken müssen.

Kein für § 161 Abs. 1 StPO erforderlicher Anfangsverdacht liegt bei sog. Vorermittlungen vor. Auch Maßnahmen der Strafverfolgungsvorsorge sind nur bei Vorliegen eines Anfangsverdachts zulässig.

Legales Verhalten kann nur dann einen Anfangsverdacht begründen, wenn entweder bereits klar ist, dass eine Straftat begangen wurde und das legale Verhalten nur auf eine verdächtige Person hindeutet oder, wenn zu dem legalen Verhalten weitere Anhaltspunkte hinzutreten, die nach kriminalistischer Erfahrung auf eine Straftat hindeuten.

1497 Siehe hierzu bereits im Rahmen der Frage nach der Einschlägigkeit der Rasterfahndung nach § 98a StPO oben unter Kap. 5, B.II.3.a).
1498 BVerfG NJW 2009, 1405 (1405ff.).
1499 Siehe hierzu bereits die Sachverhaltsdarstellung des Nichtannahmebeschlusses oben unter Kap. 5, B.II.3.a).
1500 BVerfG NJW 2009, 1405 (Ls. 1); siehe hierzu bereits oben unter Kap. 5, B.II.3.a).

Ein Anfangsverdacht kann darüber hinaus bereits durch das Vorliegen einer konkret bezeichneten Transaktion begründet werden, wenn diese möglicherweise im Zusammenhang mit strafbarem Verhalten steht.

2. Anfangsverdacht bei der Anwendung der Auswertungsmethoden

Dementsprechend stellt sich die Frage, ob bei dem hier gegenständlichen Einsatz der Auswertungsmethoden ein Anfangsverdacht vorliegt, der diesen Anforderungen entspricht. In diesem Zusammenhang sind die bereits zuvor dargestellten Fallkonstellationen[1501] des Einsatzes der Auswertungsmethoden zu unterscheiden.

a) Einsatz zur Verdachtsbegründung

Soweit die hier gegenständlichen Auswertungsmethoden eingesetzt werden, um etwa durch bestimmte *Clustering*-Verfahren und die Nachverfolgung von Transaktionen den Verdacht einer Straftat zu begründen[1502], kann dies nicht auf § 161 Abs. 1 StPO gestützt werden. Denn bereits durch den Einsatz eines *Clustering*-Verfahrens liegt ein Eingriff in das RiS vor.[1503] Zu diesem Zeitpunkt bestehen allerdings für diesen Anwendungsfall noch keinerlei Anhaltspunkte für das Vorliegen einer Straftat, denn die Auswertungsmethoden sollen ja gerade eingesetzt werden, um derartige Anhaltspunkte zu erhalten.[1504]

Da die Ermächtigungsgrundlagen der StPO aber gerade nicht zum proaktiven Aufhellen von Dunkelfeldern angewendet werden können[1505], kann der verdachtsbegründende Einsatz der Auswertungsmethoden nicht auf § 161 Abs. 1 StPO gestützt werden.

1501 Siehe hierzu bereits unter Kap. 5, A.
1502 Siehe hierzu bereits oben unter Kap. 5, A.I.
1503 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c)(1).
1504 Siehe hierzu bereits oben unter Kap. 5, A.I.
1505 SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6; Löwe-Rosenberg/*Mavany,* § 152 Rn. 28, 53; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 251. Siehe hierzu bereits oben unter Kap. 5, D.I.1.d).

b) Einsatz zur Ermittlung nach bestehendem Verdacht

Anders dürfte dies zu beurteilen sein, wenn die Auswertungsmethoden eingesetzt werden, nachdem die Strafverfolgungsbehörden Anhaltspunkte dafür haben, dass etwa eine *Bitcoin-Adresse* im Zusammenhang mit einer Straftat verwendet wurde.[1506]

Soweit etwa im Rahmen einer nicht offensichtlich unrichtigen Strafanzeige den Strafverfolgungsbehörden mitgeteilt wird, dass beispielsweise eine bestimmte *Bitcoin-Adresse* zum Handel mit illegalen Waren auf einem *Darknet-Handelsplatz* oder zur Zahlungsabwicklung einer Erpressung verwendet wird, bestehen insoweit objektive Anhaltspunkte für das Vorliegen einer Straftat. Damit läge der für die Ermittlungsgeneralklauseln erforderliche Anfangsverdacht vor.

c) Einsatz von Ermittlungsmethoden, durch die unmittelbar ein Anfangsverdacht begründet werden kann

Problematisch ist dagegen die bereits dargestellte Konstellation, in der durch den Einsatz der Auswertungsmethoden unmittelbar der Verdacht für strafbares Verhalten begründet werden kann.[1507] Dies betrifft insbesondere die Auswertungsmethode der sog. *Labelling*-Verfahren.[1508] Bei diesen *Labelling*-Verfahren wird ein zweischrittiges Verfahren angewendet, das auf künstlicher Intelligenz beruht.[1509] Dabei werden in einem ersten Schritt Transaktionsdaten durch sog. *Classifier*-Algorithmen ausgewertet.[1510] Bei den im ersten Schritt ausgewerteten Transaktionsdaten müssen die Hintergründe der jeweiligen Transaktionen bekannt sein – etwa, dass sie im Rahmen eines sog. *Exchange-Services,* also eines Wechselgeldanbieters, ausgeführt wurden.[1511] Die *Classifier*-Algorithmen analysieren dann systematisch diese Transaktionsdaten im Vergleich zu anderen Transaktionsdaten und

1506 Siehe zu dieser Einsatzmöglichkeit bereits oben unter Kap. 5, A.II.
1507 Siehe hierzu bereits oben unter Kap. 5, A.III.
1508 Siehe hierzu bereits oben unter Kap. 3, A.III.3.
1509 Siehe hierzu bereits oben unter Kap. 3, A.III.3; *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).
1510 Siehe hierzu bereits oben unter Kap. 3, A.III.3; *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).
1511 Siehe hierzu bereits oben unter Kap. 3, A.III.3; *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

ermitteln so die typischen Besonderheiten und Transaktionsmuster von Transaktionen eines bestimmten Hintergrundes – etwa eines *Exchange-Services.*[1512] Anschließend können die in der Blockchain enthaltenen Transaktionsdaten nach derartigen Transaktionsmustern durchsucht werden, sodass etwa *Entitäten* ermittelt werden können, mit denen wahrscheinlich die Transaktionen eines *Exchange-Services* abgewickelt werden.[1513] Denkbar, aber praktisch bisher noch nicht umgesetzt, ist, dass gerade dieses Verfahren auch für Transaktionen im Zusammenhang mit Geldwäsche oder anderen strafbaren Handlungen angewendet wird. So wäre es möglich durch die Transkationen, die im Zusammenhang mit einem bestimmten strafbaren Verhalten stehen, deren Transaktionsmuster zu ermitteln und im Anschluss die Blockchain-Daten nach Transaktionen zu durchsuchen, die ein ähnliches Muster aufweisen und daher wahrscheinlich auch im Zusammenhang mit dem bestimmten strafbaren Verhalten stehen.[1514] Erforderlich wäre hierzu allerdings eine ausreichende Datengrundlage – also Kenntnis über genügend Transaktionen, die im Zusammenhang mit einem bestimmten strafbaren Verhalten stehen.

Insoweit stellt sich die Frage, ob hier der für die Ermittlungsgeneralklauseln erforderliche Anfangsverdacht vorliegt. Dies ist in zweifacher Hinsicht fraglich.

Einerseits muss der Anfangsverdacht bereits im ersten Schritt der Auswertungsmethode vorliegen. Denn strafrechtliche Ermittlungen auch bzgl. nur einer bestimmten Transaktion sind nur zulässig, soweit auch für diese ein Anfangsverdacht bestand. Insoweit müssen etwa für den Anwendungsbereich der Geldwäsche genügend einzelne Ermittlungsverfahren geführt worden sein, bei denen ein Anfangsverdacht der Geldwäsche vorlag. Dass nur derart zulässige Ermittlungsverfahren geführt wurden, wird für die nachfolgende Bewertung angenommen. Die Daten dieser Ermittlungsverfahren müssten dann in rechtlich zulässigerweise gespeichert werden, um für spätere Ermittlungen abstrakt Transaktionsmuster bestimmen zu können, die auf Geldwäsche hindeuten.

Andererseits stellt sich außerdem die Frage, ob ausreichende tatsächliche Anhaltspunkte für einen Anfangsverdacht vorliegen, wenn Blockchain-Daten nach einem abstrakten Transaktionsmuster durchsucht werden, das

1512 Siehe hierzu bereits oben unter Kap. 3, A.III.3; *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

1513 Siehe hierzu bereits oben unter Kap. 3, A.III.3; *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

1514 Siehe hierzu bereits oben unter Kap. 5, A.III.

durch die systematische Analyse von Transaktionen von bereits geführten Ermittlungsverfahren ermittelt wurde.

Hieraus ergeben sich entsprechende zwei Fragen:

- Inwieweit können die Erkenntnisse aus bereits zuvor geführten Strafverfahren, die wohl in der Regel nur einzelne oder eine geringe Mehrzahl von Transaktionen betreffen, für das Erstellen von abstrakten Transaktionsmustern verwendet werden?
- Liegen bei einem so ermittelten Transaktionsmuster, nach dem dann die Blockchain-Daten durchsucht werden, ausreichende objektive Anhaltspunkte für einen Anfangsverdacht vor?

(1) Verwertung von Daten aus einzelnen, vorangegangen Strafverfahren

Die erstgenannte Frage betrifft insoweit eine Maßnahme der Strafverfolgungsvorsorge, denn die Erkenntnisse aus einem konkreten Strafverfahren sollen gespeichert und verwertet werden, um die Strafverfolgung in einem weiteren, zukünftigen Strafverfahren zu ermöglichen oder zu erleichtern.[1515]

Als strafprozessuale Grundlage für diese Verwertung kommt dabei insbesondere § 484 StPO in Betracht. Denn § 484 StPO regelt die „Zulässigkeit und den Umfang der (vorsorglichen) Verarbeitung personenbezogener Daten aus Strafverfahren für die Zwecke künftiger Strafverfahren und damit eine Zweckumwandlung (Umwidmung) der Daten."[1516] Nach § 484 Abs. 1 StPO ist die Verarbeitung bestimmter, in § 484 Abs. 1 Nr. 1-5 StPO genau bezeichneter Daten für die Zwecke künftiger Strafverfolgung in Dateisystemen der Strafverfolgungsbehörden zulässig.[1517] Hiervon umfasst sind jedoch nur Personendaten des Beschuldigten (Nr. 1), die zuständige Stelle und das Aktenzeichen (Nr. 2), die nähere Bezeichnung der Straftaten, insbesondere die Tatzeiten, Tatorte und die Höhe etwaiger Schäden (Nr. 3), die Tatvorwürfe (Nr. 4) und die Einleitung und Erledigung des Verfahrens (Nr. 5). Hierunter fallen die für die *Labelling*-Verfahren erforderlichen Transaktionsdaten mit deren Tathintergründen wohl nicht.

Darüber hinaus ist nach § 484 Abs. 2, Abs. 3 StPO die Verarbeitung weiterer, personenbezogener Daten von Beschuldigten nur zulässig, „soweit

1515 Siehe hierzu bereits oben unter Kap. 5, D.I.1.e); *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 87.
1516 BeckOK-StPO/*Wittig*, § 484.
1517 Vgl. BeckOK-StPO/*Wittig*, § 484 Rn. 1.

dies erforderlich ist, weil […] Grund zu der Annahme besteht, dass weitere Strafverfahren gegen den Beschuldigten zu führen sind"[1518] und die nach § 484 Abs. 3 StPO erforderliche Rechtsverordnung des BMJV die jeweiligen Daten erfasst. Insoweit würden die für die *Labelling*-Verfahren erforderlichen Transaktionsdaten hierunter fallen. Damit wäre grundsätzlich nach § 484 Abs. 2 S. 1 StPO erforderlich, dass die berechtigte Annahme besteht, dass gegen den Beschuldigten weitere Strafverfahren zu führen sind. Problematisch ist, dass dies jedoch zumindest nicht die Regel sein dürfte.

Insoweit wäre eine genaue Speicherung der Daten über die einzelnen Transaktionsdaten des jeweiligen Strafverfahrens wohl nicht möglich.

In Betracht käme jedoch eine abstrahierte Speicherung der jeweiligen Transaktionsdaten, insoweit, dass nur die Inhalte – also etwa die Höhe der Transaktion, die Anzahl der beteiligten *Inputs* und *Outputs* etc. – der gegenständlichen Transaktionen in der Form gespeichert werden, dass ein Rückschluss auf die jeweils beteiligten Personen, *Bitcoin-Adressen* oder *Entitäten* nicht mehr möglich ist und dementsprechend keine personenbezogenen Daten mehr vorliegen. Insoweit würden hierbei nur die Ergebnisse der systematischen Analyse der Transaktionsdaten, nicht aber deren konkreten Transaktionen gespeichert werden – ebenso wenig wie Anhaltspunkte, die anhand der Blockchain einen Rückschluss auf die jeweiligen Transaktionen zulassen. Wichtig wäre hierzu allerdings, dass anhand der so gespeicherten Daten auch kein Rückschluss mehr auf die ursprünglich gegenständlichen Transaktionen mehr möglich ist. So müsste beachtet werden, dass jedenfalls keine einzigartigen Transaktionsmuster gespeichert werden anhand derer ein Rückschluss auf die ursprünglichen Transaktionen möglich ist. Welche Anforderungen insoweit an die Anonymisierung der Transaktionsdaten zu stellen wären, hinge insoweit vom jeweiligen Einzelfall ab.[1519]

Dementsprechend wäre das für das zweischrittige *Labelling*-Verfahren erforderliche Speichern und Auswerten von Transaktionen mit bekanntem, strafrechtlich relevantem Hintergrund nur in einer abstrakten Weise zulässig, bei dem kein Rückschluss auf die dahinterstehenden Personen möglich ist.

1518 Wortlaut des § 484 Abs. 2 S. 1 StPO.

1519 Vgl. *Art. 29 Datenschutzgruppe,* WP 216, S. 4, 28, die darstellen, dass die Wirksamkeit von Anonymisierungsmöglichkeiten vom jeweiligen Einzelfall abhängen.

(2) Anfangsverdacht bei abstrakten Transaktionsmustern

Die zweitgenannte Frage betrifft das Problem, ob bereits durch ein so ermitteltes, abstraktes Transaktionsmuster ausreichende, objektive Anhaltspunkte für das Vorliegen einer Straftat bestehen.

Für das Vorliegen derartiger Anhaltspunkte spricht die Rechtsprechung des BVerfG zur Abfrage von Kreditkartendaten[1520], wonach bereits ein Anfangsverdacht vorliegt, wenn bestimmte, genau bezeichnete Transaktionen gesucht werden, die auf das Vorliegen einer Straftat hindeuten.

Insoweit ließe sich annehmen, dass auch dann ausreichende, objektive Anhaltspunkte für eine Straftat vorliegen, wenn nach Transaktionen gesucht wird, die auf ein bestimmtes, zuvor genau bezeichnetes Transaktionsmuster hindeuten.

Erforderlich für derartige, objektive Anhaltspunkte für eine Straftat wäre allerdings, dass ein Transaktionsmuster hinreichend genau abgrenzbar ist und nicht lediglich auf grundsätzlich strafbares oder auffälliges Verhalten hindeutet, sondern auf konkrete einzelne Straftaten. Insoweit müsste das jeweilige Transaktionsmuster genaue Merkmale aufweisen, die insbesondere in Abgrenzung von anderen Transaktionsmustern oder herkömmlichem Transaktionsverhalten auf ein bestimmtes, strafbares Verhalten hindeuten. Außerdem müsste dieses Transaktionsmuster mit einer ausreichenden Wahrscheinlichkeit auf ein derartig strafbares Verhalten hindeuten. Nicht ausreichen kann insoweit ein bloßes, subjektives Empfinden der Strafverfolgungsbehörden, dass derartiges Transaktionsverhalten auf strafbares Verhalten hindeutet. Erforderlich wäre daher ein Transaktionsmuster, dass durch ein vorangegangenes, hinreichendes Auswertungsverfahren, Merkmale definiert, die sich eindeutig von nicht bzw. nicht derart strafbarem Verhalten abgrenzen lässt.

Fraglich ist allerdings, ob und inwieweit die Rechtsprechung des BVerfG auch für die Frage des Vorliegens eines Anfangsverdachts bei der Suche nach bestimmten Transaktionsmustern angewendet werden kann.

Denn auf den ersten Blick werden zwar sowohl bei der Kreditkartenabfrage als auch bei der Suche nach Transaktionsmustern jeweils nur Informationen anhand von zuvor abstrakt definierten Maßstäben – den jeweils genau zu bezeichnenden Transaktionen – ermittelt.

1520 BVerfG NJW 2009, 1405 (1405ff.).

Allerdings muss beachtet werden, dass im Fall des BVerfG bereits bekannt war, dass auf der verfahrensgegenständlichen Internetplattform kinderpornographisches Material angeboten wurde. Durch die Abfrage der Staatsanwaltschaft bei den Kreditkartenunternehmen sollten insoweit nur die Täter des § 184b Abs. 4 a.F.[1521] ermittelt werden. Im Vergleich hierzu wird bei der Suche nach abstrakten Transaktionsmustern, die auf bestimmtes, strafbares Verhalten hindeuten, in einem ersten Schritt strafbares Verhalten gesucht und erst im Anschluss die Täter dieses strafbaren Verhaltens. Insoweit wird bei der Kreditkartenabfrage nach Personen, bei der eine bestimmte Transaktion vorliegt, gesucht, wohingegen bei der Suche nach Transaktionsmustern das Vorliegen einer bestimmten Transaktion ermittelt werden soll.

Ein maßgeblicher Unterschied besteht daher darin, dass bei Beginn der jeweiligen Ermittlungshandlung einerseits bei der Suche nach Transaktionsmustern nur abstrakt definierte Merkmale bekannt sind, die mit einer hohen Wahrscheinlichkeit auf bestimmte Straftaten hindeuten. Andererseits besteht bei der Kreditkartenabfrage bereits die Kenntnis davon, dass es das Angebot eines strafbaren Verhaltens gegeben hat, dessen Täter nur noch ermittelt werden müssen. Dementsprechend besteht der maßgebliche Unterschied darin, dass einerseits (bei der Kreditkartenabfrage) nur Täter einer bereits bekannten Straftat ermittelt werden sollen, wohingegen andererseits (bei der Suche nach Transaktionsmustern) zunächst überhaupt strafbares Verhalten ermittelt werden soll.

Auf Grund dieses Unterschieds liegt insoweit bei der Suche nach Transaktionsmustern der für § 161 Abs. 1 StPO erforderliche Anfangsverdacht nicht vor.

d) Zwischenergebnis

Der für § 161 Abs. 1 StPO erforderliche Anfangsverdacht liegt weder beim verdachtsbegründenden Einsatz noch bei der Suche nach zuvor genau definierten Transaktionsmustern, die auf das Vorliegen einer bestimmten Straftat hindeuten, vor.

Dagegen liegt ein Anfangsverdacht vor, wenn die Strafverfolgungsbehörden auf Grund anderweitiger Umstände, Kenntnis von einem möglicher-

1521 In der damals geltenden Fassung vom 01.04.2004.

weise strafbaren Verhalten erlangen und zur weiteren Ermittlung die hier gegenständlichen Auswertungsmethoden einsetzen.

e) Exkurs – verdachtsbegründender Einsatz als zulässige Vorermittlungen?

In Betracht kommt darüber hinaus ein als Vorermittlung zulässiger Einsatz der Auswertungsmethoden. Problematisch hieran ist jedoch einerseits, dass auch in diesem Anwendungskontext noch keine Anhaltspunkte für das Vorliegen einer Straftat vorliegen.[1522] Denn die Vorermittlungen sollen nur zulässig sein, um zu klären, ob beim Vorliegen von Anhaltspunkten ein für § 161 Abs. 1 StPO ausreichender Anfangsverdacht besteht oder nicht. Bei einem Einsatz zur Verdachtsbegründung würden die Auswertungsmethoden dagegen unabhängig von Anhaltspunkten für strafbares Verhalten eingesetzt, um Anhaltspunkte für Straftaten zu erhalten.

Darüber hinaus ist problematisch, dass derartige Vorermittlungen allerdings wohl nur zulässig sind, soweit hierdurch keine Grundrechtseingriffe vorliegen. Dagegen liegt bereits bei den zur Verdachtsbegründung erforderlichen *Clustering*-Verfahren ein Eingriff in das RiS vor, sodass derartige Vorermittlungen jedenfalls insoweit nicht zulässig wären.

II. Lediglich geringfügiger Grundrechtseingriff

§ 161 Abs. 1 StPO ermächtigt nur zu solchen Ermittlungshandlungen, mit denen ein lediglich geringfügiger Grundrechtseingriff einhergeht. Nachfolgend ist daher zu untersuchen, ob bei der Anwendung der hier gegenständlichen Auswertungsmethoden ein lediglich geringfügiger Grundrechtseingriff vorliegt.

Bisher fehlt es in der Literatur allerdings an einer systematischen Darstellung von Faktoren, die die Grundrechtsintensität steigern bzw. verringern.[1523] Daher stellt sich die Frage, wie die hier erforderliche Bewertung der Grundrechtsintensität der hier gegenständlichen Auswertungsmethoden vorgenommen werden kann.

1522 Siehe hierzu bereits oben unter Kap. 5, A.I.

1523 So *Rückert,* ZStW 129 (2017), 302 (319) m.w.N, der für sog. Online-Ermittlungen im öffentlich zugänglichen Internet eine Abwägung intensitätssteigernder und intensitätsverringernder Faktoren vornimmt.

Allerdings haben sich einerseits in Literatur und Rechtsprechung bestimmte Ermittlungsmaßnahmen herausgebildet, die wohl zulässigerweise auf die Ermittlungsgeneralklauseln gestützt werden können. Andererseits hat das BVerfG in mehreren Entscheidungen bereits Kriterien herausgearbeitet, die für die Bewertung der Grundrechtsintensität herangezogen werden können.

Daher wird nachfolgend zunächst auf die nach Literatur und Rechtsprechung wohl nach § 161 Abs. 1 StPO zulässigen Ermittlungsmaßnahmen eingegangen, um durch einen Vergleich mit speziell geregelten Ermittlungsbefugnissen Faktoren herauszuarbeiten, die sich auf die Grundrechtsintensität auswirken (hierzu unter 1.). Anschließend wird auf die vom BVerfG herausgearbeiteten Kriterien zu Bewertung der Grundrechtsintensität eingegangen (hierzu unter 2.) und schließlich die Grundrechtsintensität der hier gegenständlichen Auswertungsmethoden bewertet (hierzu unter 3.).

1. Herkömmliche Ermittlungsmaßnahmen, die wohl nach § 161 Abs. 1 StPO zulässig sind

Nach herrschender Literaturauffassung sollen die folgenden Ermittlungsmaßnahmen als weniger grundrechtsintensive Maßnahmen zulässigerweise auf § 161 Abs. 1 StPO gestützt werden können[1524]:

- Einfache Fahndungsmaßnahmen[1525]
- Erkundigungen im Umfeld einer Person und Vernehmungen von Zeugen, Sachverständigen und dem Beschuldigten[1526]
- Augenscheinseinnahme[1527]
- Einsatz von V-Leuten[1528]
- Kurzfristige Observationen[1529]

1524 Die folgende Aufzählung entspricht weitgehend BeckOK-StPO/*Sackreuther,* § 161 Rn. 11 und KMR-StPO/*Noltensmeier-von Osten,* § 161 Rn. 21.

1525 So auch Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 2; *Hilger*, NStZ 2000, 561 (564); .

1526 Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 20.

1527 Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 20.

1528 So auch Meyer-Goßner/Schmitt/*Schmitt,* § 161 Rn. 1 mit Verweis auf BGH NStZ 2010, 528.

1529 In Abgrenzung zu der in § 163f besonders geregelten längerfristigen Observation, vgl BeckOK-StPO/*Sackreuther,* § 161 Rn. 11.

– Einsatz von sog. Scheinkäufern zur Aufklärung von Betäubungsmittelstraftaten[1530]
– Ermittlungen im Internet – etwa das Abrufen von Daten durch Einwählen in ein Kommunikationsforum oder das Einwählen in Mailboxen mittels einer Gastkennung[1531] oder auch das Ermitteln im Darknet mit computergenerierter Kinderpornografie[1532]
– Allgemeine Erhebung personenbezogener Daten – etwa mittels Anfrage gegenüber privaten Stellen wie Kreditkartenunternehmen[1533]

Einige dieser Ermittlungsmaßnahmen weisen Ähnlichkeiten und/oder Überschneidungen zu speziell geregelten Ermittlungsbefugnissen auf. Insoweit wird nun nachfolgend auf diese ähnlichen Ermittlungsmaßnahmen eingegangen, um anhand der jeweiligen Unterschiede Faktoren herauszuarbeiten, die auf eine Intensitätssteigerung hindeuten.

a) Einfache Fahndungsmaßnahmen und kurzfristige Observationen

So sollen etwa einfache Fahndungsmaßnahmen und kurzfristige Observationen auf die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 StPO gestützt werden können.

Einfache Fahndungsmaßnahmen sind dabei wohl etwa „unauffällige und nur einen kleinen Personenkreis erfassende Nachfragen, Nachforschungen in allgemein zugänglichen Quellen und […] Auskünfte aus dem Melderegister und ähnlichen Unterlagen“[1534].

Die Bestimmung, was einfache Fahndungsmethoden sind, soll sich darüber hinaus insbesondere aus der Abgrenzung zu den speziell geregelten Fahndungsmethoden, wie etwa der Rasterfahndung (§ 98a StPO), der Einrichtung von Kontrollstellen (§ 111 StPO), der Kontrollfahndung (§ 163d StPO), der polizeilichen Beobachtung (§ 163e StPO), der längerfristigen

1530 Verweis auf BGHSt 41, 64 (66); BGH NStZ 2010, 527.
1531 Verweis auf *Soiné*, NStZ 2010, 596 (601f.).
1532 Verweis auf *Wittmer/Steinebach*, MMR 2019, 650 (650).
1533 Verweis auf BVerfG NJW 2009, 1405 (1405ff.). Siehe hierzu bereits ausführlich oben unter Kap. 5, B.II.3.a), D.I.1.g). Vgl. insoweit, dass auch im Rahmen der Europäischen Ermittlungsanordnung eine entsprechende Erhebung von Bankauskünften nach §§ 160, 161a StPO vom Gesetzgeber als zulässig erachtet wird, BT-Drs. 18/9757, S. 40.
1534 Löwe-Rosenberg/*Erb,* § 161 Rn. 49.

Observation (§ 163f StPO) oder den speziell in §§ 131 ff. StPO geregelten Vorschriften zur Fahndung ergeben.[1535]

Aus dieser Abgrenzung zu den speziell geregelten Maßnahmen ergibt sich etwa die Grenze der Zulässigkeit für kurzfristige Observationen nach § 161 Abs. 1 StPO. Denn diese sollen nach § 161 Abs. 1 StPO zulässig sein, soweit sie zeitlich hinter den längerfristigen Observationen nach § 163f StPO zurückbleiben.[1536]

Daher sollen nachfolgend die einzelnen, besonderen Fahndungsmethoden und Observationen mit den nach § 161 Abs. 1 StPO zulässigen Fahndungsmaßnahmen und kurzfristigen Observationen verglichen werden.

(1) Vergleich mit der Rasterfahndung, § 98a StPO

So betrifft etwa die Rasterfahndung nach § 98a StPO gerade umfangreiche Datensätze, um aus einem großen Personenkreis einen kleineren Verdächtigenkreis zu ermitteln.[1537] Hinsichtlich des Umfangs der Informationen geht die Rasterfahndung also weit über die im Rahmen der einfachen Fahndungsmethoden verfügbaren Informationen von einfachen Nachfragen und Nachforschungen in einem kleinen Personenkreis hinaus. Diese umfangreichen Informationen können darüber hinaus nicht nur aus allgemein zugänglichen Quellen, den Meldebehörden und ähnlichen Unterlagen stammen, sondern § 98a Abs. 2 StPO enthält eine zwangsweise durchsetzbare Pflicht zur Datenübermittlung gegenüber speichernden Stellen.[1538] Insoweit können im Rahmen der Rasterfahndung insbesondere auch Informationen ausgewertet werden, die lediglich bei privaten Stellen gespeichert werden.[1539] Die so erhebbaren Informationen können schließlich im Rahmen einer Rasterfahndung gerade in Form eines systematischen, maschinellen Datenabgleich ausgewertet werden, um eine bestimmte Schnittmenge von Prüfungsmerkmalen – den Verdächtigenkreis – zu ermitteln.[1540] Von dieser Auswertung betroffen sind dabei in der Regel gerade auch viele Personen, gegen die nicht auf Grund eines bestimmten Verhaltens bereits ein Verdacht

1535 Löwe-Rosenberg/*Erb,* § 161 Rn. 49; SK-StPO/*Weßlau/Deiters,* § 161 Rn. 15.
1536 BeckOK-StPO/*von Häfen,* § 163f Rn. 3; BVerfG StraFo 2009, 453. Hierzu im Einzelnen sogleich unter Kap. 5, D.II.1.a)(3).
1537 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.
1538 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.4.
1539 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.4.
1540 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.2.

besteht.[1541] Denn die Rasterfahndung gleicht ja gerade viele Datensätze miteinander ab, um eine kleine Schnittmenge dieser Datensätze zu erhalten.[1542] Von diesem Abgleich können daher gerade auch ganz einfache Daten, wie etwa die Immatrikulation an einer Hochschule für ein bestimmtes Studienfach erfasst sein.[1543] Insoweit besteht außerdem eine hohe sog. Streubreite.[1544] Denn von der Maßnahme kann gerade auch eine hohe Anzahl unbeteiligter Personen betroffen sein.[1545] Dem lässt sich zwar grundsätzlich entgegenhalten, dass auch im Rahmen von Erkundigungen und Nachfragen im Umfeld einer Person wohl gerade auch Personen betroffen sein werden, die in keinem Zusammenhang mit einem strafbaren Verhalten stehen, dieser Personenkreis dürfte allerdings sehr viel kleiner sein, als im Rahmen der Rasterfahndung nach § 98a StPO.

Die spezielle Befugnis der Rasterfahndung geht also hinsichtlich des Umfangs und der Zugänglichkeit der Informationen, sowie deren Auswertbarkeit und der Streubreite der Ermittlungsmaßnahme weit über die im Rahmen einfacher Fahndungsmethoden möglichen Eingriffe hinaus. Dass insoweit mit der Rasterfahndung ein intensiverer Grundrechtseingriff einhergeht, ergibt sich dabei insbesondere aus den besonderen Anforderungen für die Zulässigkeit der Rasterfahndung im Vergleich zu den einfachen Voraussetzungen des § 161 Abs. 1 StPO. Denn § 161 Abs. 1 StPO setzt lediglich einen Anfangsverdacht voraus, die Rasterfahndung nach § 98a StPO ist hingegen nur zulässig, wenn:

- ein Anfangsverdacht einer
- „Straftat von erheblicher Bedeutung
  - auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
  - auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),
  - auf dem Gebiet der gemeingefährlichen Straftaten,

1541 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.2.

1542 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, C.II.1.

1543 Dies war etwa der Fall bei der Suche nach potenziellen „Schläfern" im Anschluss an die Anschläge des 11. September 2001, vgl. *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 97.

1544 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 3 mit Verweis auf BVerfG NJW 2006, 1941 (1944f.).

1545 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 3 mit Verweis auf BVerfG NJW 2006, 1941 (1944f.); BVerfGE 125, 260 (318).

  - gegen Leib oder Leben, die sexuelle Selbstbestimmung oder die persönliche Freiheit,
  - gewerbs- oder gewohnheitsmäßig oder
  - von einem Bandenmitglied oder in anderer Weise organisiert"[1546] vorliegt,
- die Erforschung des Sachverhalts oder der Aufenthaltsort des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre[1547] und
- die Rasterfahndung gerichtlich angeordnet wurde bzw. bei Gefahr im Verzug von der Staatsanwaltschaft[1548].

Zusammenfassend setzt die Zulässigkeit der Rasterfahndung damit einen „Anfangsverdacht, der sich […] auf eine katalogmäßig beschriebene Straftat beziehen muss, die […] von erheblicher Bedeutung ist und es gilt […] die qualifizierte Subsidiaritätsklausel"[1549] sowie das Erfordernis einer grundsätzlich gerichtlichen Anordnung. Aus diesen im Vergleich erhöhten Anforderungen ergibt sich daher, dass bei einer derartigen Fahndungsmethode eben auch ein gesteigerter Grundrechtseingriff vorliegt.

(2) Vergleich mit der Einrichtung von Kontrollstellen und Kontrollfahndung, §§ 111, 163d StPO

Ähnlich ergeben sich diese intensitätssteigernden Faktoren auch aus dem Vergleich zu den Fahndungsmethoden der §§ 111 Abs. 1 S. 2, 163d Abs. 1 StPO. Denn auch diese betreffen einen größeren Umfang von erhebbaren Informationen sowie deren mögliche Auswertungen und können sich gegen eine große Anzahl von Personen richten, die nicht durch ein ihnen vorwerfbares Verhalten einen Anlass für die Maßnahme gegeben haben. Daher sind die Maßnahmen der §§ 111, 163d StPO nur unter zusätzlichen, hohen Voraussetzungen zulässig.

Nach § 111 Abs. 1 StPO können an öffentlich zugänglichen Orten Kontrollstellen eingerichtet werden und dort die Identitäten der Personen erhoben werden, die diese Kontrollstellen passieren.[1550] Die so erhobenen

1546 So der Wortlaut des § 98a Abs. 1 S. 1 StPO
1547 Vgl. § 98a Abs. 1 S. 2 StPO.
1548 Vgl. hierzu im Einzelnen § 98b StPO.
1549 KK-StPO/*Greven,* § 98a Rn. 9.
1550 KMR-StPO/*Pauckstadt-Maihold,* § 111 Rn. 12.

Identitätsdaten können außerdem nach § 163d Abs. 1 StPO in einer Datei gespeichert werden.[1551] In dieser Datei können ferner auch die Daten von grenzpolizeilichen Kontrollen[1552] gespeichert werden. Darüber hinaus ist es nach § 163d Abs. 1 StPO insbesondere möglich, die Informationen dieser Datei – also sowohl die Daten der öffentlichen Kontrollstellen nach § 111 StPO als auch die Daten der grenzpolizeilichen Kontrollen – mit anderen Datenbeständen der Strafverfolgungsbehörden abzugleichen.[1553]

Gegenstand dieser besonderen Fahndungsmethoden sind insoweit einerseits umfangreiche Datenerhebungen aus Quellen, die nicht allgemein zugänglich sind und die eine hohe Anzahl unverdächtiger Personen betreffen – nämlich die Identitätsdaten aller Personen, die die Kontrollstellen des § 111 StPO passieren oder von einer grenzpolizeilichen Maßnahme betroffen sind.[1554] Denn die Erhebung der Daten findet zwar im öffentlichen Raum statt, nicht allgemein zugänglich sind aber gerade die Identitätsdaten aller betroffenen Personen.

Andererseits ist darüber hinaus eine systematische Auswertung dieser umfangreichen Daten auch durch einen Abgleich mit Daten, die bereits bei den Strafverfolgungsbehörden verfügbar sind, möglich.[1555] Die speziellen Fahndungsmethoden der §§ 111, 163d StPO gehen insoweit ebenfalls sowohl hinsichtlich des Umfangs als auch der Verfügbarkeit der Informationen sowie der Form der Auswertung weit über die Möglichkeiten im Rahmen der einfachen Fahndungsmethoden hinaus.

Dabei ergibt sich die erhöhte Grundrechtsintensität dieser Besonderheiten der Maßnahme wiederum daraus, dass die Einrichtung der Kontrollstellen nach § 111 StPO nur zulässig ist, soweit

1551 BeckOK-StPO/*von Häfen,* § 163d Rn. 3f.

1552 Dies sind etwa die nach § 23 BPolG erhebbaren Identitätsdaten, vgl. BeckOK-StPO/*von Häfen,* § 163d Rn. 4.

1553 BeckOK-StPO/*von Häfen,* § 163d Rn. 2f.

1554 BeckOK-StPO/*von Häfen,* § 163d Rn. 3f.

1555 KK-StPO/*Moldenhauer,* § 163d Rn. 15; BeckOK-StPO/*von Häfen,* § 163d Rn. 2. Ausgeschlossen ist aus systematischen Gründen im Rahmen der Auswertung allerdings wohl ein maschineller Datenabgleich nach bestimmten Prüfkriterien, wie er in § 98a Abs. 1 StPO vorgesehen ist, siehe hierzu KK-StPO/*Moldenhauer,* § 163d Rn. 16.

- ein Anfangsverdacht[1556] einer Straftat
  - nach § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Straftat),
  - nach § 89c Abs. 1-4 StGB (Terrorismusfinanzierung)
  - nach § 129a StGB (Bildung terroristischer Vereinigungen) auch in Verbindung mit § 129b Abs. 1 StGB oder einer der dort genannten Straftaten oder
  - nach § 250 Abs. 1 Nr. 1 StGB (Schwerer Raub) vorliegt,
- die Einrichtung der Kontrollstellen richterlich bzw. bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet wurde
- und Tatsachen die Annahme rechtfertigen, dass dies zur Ergreifung des Täters oder zur Sicherstellung von Beweismitteln, die der Aufklärung der Straftat dienen können.

Insoweit ist die Errichtung der Kontrollstellen nach § 111 StPO nur unter sehr strengen Voraussetzungen zulässig, nämlich insbesondere der Verdacht einer der genau bezeichneten Straftaten. Die Voraussetzungen des § 111 StPO gehen angesichts dieser sehr genau bezeichneten, besonders schweren Straftaten noch über die Anforderungen der Rasterfahndung hinaus. Ein Grund hierfür könnte darin liegen, dass die Streubreite der Errichtung von Kontrollstellen nach § 111 StPO noch höher ist als die der Rasterfahndung. Denn bei der Rasterfahndung werden Prüfungsmerkmale miteinander abgeglichen, die vermutlich auf den Täter zutreffen – also etwa ein bestimmtes Studienfach. Allerdings muss in diesem Zusammenhang auch beachtet werden, dass ein derartiges Prüfungsmerkmal im Rahmen einer Rasterfahndung, wie ein bestimmtes Studienfach, noch kein vorwerfbares Verhalten darstellt und insoweit kein Anlass dafür besteht, lediglich auf Grund dieses Prüfungsmerkmals Gegenstand einer staatlichen Ermittlungsmaßnahme zu werden. Selbst, wenn ein Betroffener mehrere der Prüfungsmerkmale der Rasterfahndung erfüllt, wird dies in der Regel noch nicht den Verdacht eines strafbaren bzw. vorwerfbaren Verhaltens begründen, denn die Prüfungsmerkmale dürften in der Regel lediglich bestimmtes, legales Verhalten – etwa das Barzahlen der Stromrechnung[1557] – betreffen. Andererseits muss beachtet werden, dass im Rahmen der Kontrollstellen und deren Datenauswertung Personen unabhängig von einem bestimmten

1556 BeckOK-StPO/*Huber,* § 111 Rn. 3.

1557 So etwa im Rahmen der sog. Stromkundenprogramme bei der Suche nach RAF-Terroristen, vgl. *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110f.

Anlass betroffen werden. Denn der einzige Grund der Identitätskontrolle ist das Aufhalten bzw. Passieren eines bestimmten Ortes zu einem bestimmten Zeitpunkt. Insoweit besteht zwar im Rahmen beider Maßnahmen kein dem Betroffenen vorwerfbares Verhalten, das Anlass für die Ermittlungsmaßnahme begründen würde, die Kontrollfahndung nach §§ 111, 163d StPO hängt jedoch im Vergleich zur Rasterfahndung noch weniger von einem Anlass ab. Denn, ob eine Person von einer Rasterfahndung betroffen ist, hängt zumindest davon ab, ob sie eines der Prüfungsmerkmale, die vermutlich auch auf den Täter einer Straftat zutreffen, erfüllt.

Darüber hinaus ist in diesem Zusammenhang zu berücksichtigen, dass im Rahmen der Rasterfahndung die Betroffenheit des Einzelnen gerade davon abhängt, ob dadurch, dass der Betroffene mehrere Prüfungsmerkmale erfüllt, auch ein entsprechend erhöhter Anlass dafür besteht, dass er von der Maßnahme betroffen ist. Denn das Ziel der Rasterfahndung ist es ja gerade, aus einem großen Datensatz diejenigen Personen auszuscheiden, die nicht alle Prüfungsmerkmale der Rasterfahndung erfüllen. Zwar kann dadurch, dass der Betroffene mehrere oder alle der jeweiligen Prüfungsmerkmale der Rasterfahndung erfüllt, noch nicht der Verdacht eines vorwerfbaren Verhaltens, das Anlass für die Ermittlungsmaßnahme geben würde, begründet werden. Ob und inwieweit der Einzelne aber von der Ermittlungsmaßnahme betroffen ist, hängt im Rahmen der Rasterfahndung jedoch jedenfalls davon ab, ob es durch das Erfüllen der Prüfungsmerkmale zumindest einen Anlass hierfür gibt. Insoweit ließe sich annehmen, dass im Rahmen der Rasterfahndung eine stufenweise Gefahr besteht, von dieser oder einer weiterführenden staatlichen Ermittlungsmaßnahme betroffen zu sein. Dies trifft gerade nicht auf die Kontrollfahndung der §§ 111, 163d StPO zu. Denn die Identitätskontrolle, Speicherung und Auswertung dieser Daten ist lediglich von dem Prüfungsmerkmal abhängig, ob der Betroffene zu einem bestimmten Zeitpunkt einen bestimmten Ort passiert hat.

Hieraus lässt sich insoweit ableiten, dass die Grundrechtsintensität nicht nur allgemein davon abhängt, ob überhaupt ein Anlass dafür besteht, dass der Einzelne von einer Ermittlungsmaßnahme betroffen ist, sondern auch davon abhängt, ob dieser Anlass von bestimmten (mehreren) Tatsachen abhängt.

Dass insgesamt eine erhöhte Grundrechtsintensität bei den Maßnahmen der §§ 111, 163d StPO besteht, ergibt sich wiederum aus den erhöhten Anforderungen der Maßnahmen. Denn die Speicherung und der Abgleich der Daten, die nach § 111 StPO und im Rahmen grenzpolizeilicher Kontrollen erhoben wurden, ist nach § 163d StPO nur zulässig, soweit der

Verdacht einer der in § 111 StPO genannten Straftaten vorliegt. Erforderlich ist darüber hinaus wiederum die richterliche bzw. bei Gefahr im Verzug die staatsanwaltschaftliche Anordnung, sowie die Erforderlichkeit der Maßnahme zur Ergreifung des Täters oder zur Aufklärung der Straftat führen kann und deren Verhältnismäßigkeit.

Der Abgleich der lediglich grenzpolizeilichen Daten ist darüber hinaus auch zulässig, wenn der Verdacht einer der in § 100a Abs. 2 Nr. 6-9, Nr. 11 StPO genannten Straftaten vorliegt. § 100a Abs. 2 Nr. 6-9, Nr. 11 StPO betrifft bestimmte genau bezeichnete Straftaten des Außenwirtschaftsgesetzes, des Betäubungsmittelgesetzes, des Grundstoffüberwachungsgesetzes, des Kriegswaffenkontrollgesetzes und des Waffengesetzes.

Aus diesen insgesamt sehr hohen Anforderungen für Ermittlungsmaßnahmen der §§ 111, 163d StPO ergibt sich insoweit auch eine sehr hohe Grundrechtsintensität. Die Gründe dieser hohen Grundrechtsintensität dürften dabei im Umfang der erheb- und auswertbaren Daten, sowie der Möglichkeit zur EDV-gestützten Auswertung und der hohen Streubreite der Maßnahmen liegen.

(3) Vergleich mit längerfristiger Observation, § 163f StPO

Ferner ergibt sich auch aus dem Vergleich der nach § 161 Abs. 1 StPO zulässigen kurzfristigen Observation mit der längerfristigen Observation nach § 163f StPO, dass die Grundrechtsintensität erhöht ist, wenn umfangreichere Daten erhoben werden. Denn im Rahmen einer längerfristigen Observation nach § 163f StPO können auf Grund des längeren Zeitraums umfangreichere Informationen erhoben werden. Nach § 163f Abs. 1 StPO ist nämlich die Beobachtung eines Beschuldigten, die länger als 24 Stunden andauert (§ 163f Abs. 1 S. 1 Nr. 1 StPO) oder an mehr als zwei Tagen stattfindet (§ 163f Abs. 1 S. 1 Nr. 2 StPO) nur unter den weiteren Voraussetzungen des § 163f StPO zulässig.[1558] Insoweit ergibt sich auch hieraus, dass eine weitergehende Informationserhebung – also die Informationserhebung aus einer länger andauernden Beobachtung – nur unter zusätzlichen Voraussetzungen zulässig ist.[1559]

Darüber hinaus lässt sich hieraus wiederum ableiten, dass sich die Streubreite intensitätssteigernd auswirkt. Denn mit zunehmender Beobachtungs-

1558 Vgl. BeckOK-StPO/*von Häfen,* § 163f Rn. 3.
1559 Vgl. BeckOK-StPO/*von Häfen,* § 163f Rn. 3.

zeit dürfte auch die Gefahr, dass unbeteiligte Dritte, die lediglich zufällig Kontakt zu der observierten Person haben, von der Maßnahme betroffen sind, erhöht sein.[1560]

Allerdings bestehen für die längerfristige Observation nach § 163f StPO geringere Anforderungen als im Rahmen der bereits dargestellten Fahndungsmaßnahmen der §§ 98a, 111, 163d StPO. Denn die längerfristige Observation nach § 163f StPO ist bereits zulässig bei dem Verdacht „eine[r] Straftat von erheblicher Bedeutung"[1561]. Insoweit ist im Rahmen des § 163f StPO anders als bei §§ 98a, 111, 163d StPO keine bestimmte Katalogstraftat erforderlich.[1562] Ausreichen sollen insoweit insbesondere Verbrechen, schwer aufklärbare Straftaten der organisierten Kriminalität sowie Serien- und Bandenstraftaten.[1563]

Erforderlich ist allerdings wiederum eine richterliche bzw. bei Gefahr im Verzug eine staatsanwaltliche Anordnung und, dass andere Maßnahmen erheblich weniger erfolgversprechend sind oder die Aufklärung wesentlich erschwert würde.[1564]

Insoweit geht die längerfristige Observation nach § 163f StPO in ihren Anforderungen einerseits über die kurzfristige Observation, die im Rahmen der Generalermittlungsklausel nach § 161 Abs. 1 StPO zulässig sein soll, hinaus. Andererseits bleibt sie aber in ihren Anforderungen hinter den bereits dargestellten Maßnahmen der §§ 98a, 111, 163d StPO zurück.

Dies könnte zum einen daran liegen, dass zwar umfangreichere Daten über den Beschuldigten durch die längerfristige Beobachtung erhoben werden können, bei der Erhebung aber keine Zugangsbeschränkungen überwundern werden. Denn die längerfristige Observation findet nur im öffentlichen Raum statt und überwindet insoweit insbesondere keine berechtigten Privatsphäreerwartungen des Betroffenen, wie sie etwa in Räumen bestehen, die in den Schutzbereich des Art. 13 GG fallen. Insoweit bleibt die längerfristige Observation hinsichtlich der Zugänglichkeit der Informationen sowie des erwartbaren Inhalts der Informationen hinter den Maßnahmen nach §§ 98a, 111, 163f StPO zurück. In diesem Zusammenhang dürfte sich auch intensitätsverringernd auswirken, dass nach § 163f StPO – anders als bei §§ 98a, 111, 163d StPO – kein EDV-gestützter Datenabgleich

1560 Vgl. *Rückert*, ZStW 129 (2017), 302 (329f.).
1561 So der Wortlaut des § 163f Abs. 1 S. 1 StPO.
1562 BeckOK-StPO/*von Häfen*, § 163f Rn. 6.
1563 BeckOK-StPO/*von Häfen*, § 163f Rn. 6.
1564 Vgl. § 163f Abs. 1 S. 2 StPO.

möglich ist, wobei dieser wohl im Rahmen einer Observation von nur einer Person auch in der Ermittlungspraxis nicht hilfreich sein dürfte.

Zum anderen besteht zwar im Verhältnis zur kurzfristigen Observation die Gefahr einer erhöhten Streubreite, im Vergleich zu den bereits dargestellten Fahndungsmaßnahmen der §§ 98a, 111, 163d StPO dürfte diese jedoch wesentlich geringer ausfallen, sodass auch hierin ein Grund für die im Vergleich zu §§ 98a, 111, 163 StPO geringeren Anforderung liegen kann. Denn grundsätzlich richtet sich die längerfristige Observation nur gegen den Beschuldigten (§ 163f Abs. 1 S. 1 Hs. 1 StPO). Die längerfristige Observation anderer Personen ist dagegen nach § 163f Abs. 1 S. 3 StPO nur zulässig, wenn „auf Grund bestimmter Tatsachen anzunehmen ist, dass [die anderen Personen] mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird, dass die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Täters führen wird“[1565]. Dritte dürfen außerdem nach § 163f Abs. 2 StPO nur dann von der Maßnahme betroffen werden, wenn dies unvermeidbar ist.

(4) Vergleich mit Ausschreibung zur polizeilichen Beobachtung, § 163e StPO

Schließlich ergibt sich aus dem Vergleich zur Ausschreibung zur polizeilichen Beobachtung nach § 163e StPO, dass eine erhöhte Grundrechtsintensität bei der Auswertung und Verknüpfung von ohnehin bereits vorliegenden Daten besteht.

Denn nach § 163e StPO ist es möglich, dass eine Person oder bestimmte Identifizierungsnummern/-kennzeichen (§ 163e Abs. 2StPO) zur polizeilichen Beobachtung ausgeschrieben wird. Das bedeutet, dass die Personal- oder anderen Identifizierungsdaten, die im Rahmen von polizeilichen Kontrollen erhoben werden, für die polizeiliche Beobachtung des Betroffenen genutzt werden können.[1566] Zweck der Maßnahme soll es sein, dass hierdurch ein punktuelles Bewegungsbild des Betroffenen erstellt werden kann.[1567]

Zulässig ist die Ausschreibung zur polizeilichen Beobachtung nach § 163e StPO allerdings nur bei dem Verdacht einer erheblichen Straftat, einer richterlichen bzw. bei Gefahr im Verzug einer staatsanwaltlichen Anordnung

1565 Wortlaut des § 163f Abs. 1 S. 3 StPO.
1566 BeckOK-StPO/*von Häfen,* § 163e Rn. 4.
1567 BeckOK-StPO/*von Häfen,* § 163e Rn. 2 mit Verweis auf BT-Drs. 12/989, S. 43.

und, wenn andere Maßnahmen erheblich weniger erfolgversprechend sind. Insoweit sind Voraussetzungen der längerfristigen Beobachtung nach § 163f StPO und der Ausschreibung zur polizeilichen Beobachtung nach § 163e StPO die gleichen.

Allerdings ermächtigt § 163e StPO nicht zur Erhebung dieser Informationen.[1568] Lediglich die Auswertung von Informationen, die ohnehin im Rahmen einer zulässigen polizeilichen Kontrolle erhoben wurden, ist nach § 163e StPO möglich.

Hieraus ergibt sich insoweit, dass auch die Auswertung von bereits zulässigerweise erhobenen Informationen eine erhöhte Grundrechtsintensität besteht.

Da aber § 163e StPO gegenüber Dritten nur unter den ähnlichen, zusätzlichen Voraussetzungen wie die längerfristige Observation Dritter zulässig ist (vgl. § 163e Abs. 1 S. 3 StPO), ergibt sich hinsichtlich der Streubreite hier Entsprechendes.

(5) Zwischenergebnis

Zusammenfassend ergibt sich aus den vorstehenden Vergleichen der „einfachen Fahndungsmethoden" und der „kurzfristigen Observation" nach § 161 Abs. 1 StPO mit den speziellen, ähnlichen Ermittlungsbefugnissen der §§ 98a, 111, 163d, 163f, 163e StPO, sowie dem Vergleich dieser speziellen Ermittlungsbefugnisse untereinander Folgendes zu intensitätssteigernden und -verringernden Faktoren von Grundrechtseingriffen:

Die Grundrechtsintensität hängt einerseits davon ab, wie umfangreich die Informationen sind, die im Rahmen der jeweiligen Ermittlungsmaßnahme über den Einzelnen erhoben werden. Hierbei hängt die Intensität auch davon ab, ob die erhobenen Informationen allgemein zugänglich sind oder nur durch Überwindung etwaiger Zugangsbeschränkungen erhoben werden können. So ist die Grundrechtsintensität jedenfalls erhöht, wenn die betroffene Person eine berechtigte Vertraulichkeitserwartung hinsichtlich der erhobenen Informationen hat.

Darüber hinaus hängt die Intensität außerdem davon ab, wie die so erhobenen Informationen ausgewertet werden. So ist etwa die systematische und technikgestützte Auswertung der Informationen jedenfalls intensitätserhöhend.

1568 BeckOK-StPO/*von Häfen,* § 163e Rn. 2.

Schließlich hängt die Intensität der Grundrechtseingriffe auch davon ab, ob und wie viele Personen von der Maßnahme betroffen sind, die durch ihr Verhalten keinen Anlass für die Maßnahme gegeben haben. Dabei ist außerdem zu berücksichtigen, dass die Intensität wohl auch davon abhängt, inwieweit die Betroffenheit des Einzelnen insgesamt von bestimmten Anlässen bzw. Prüfungsmerkmalen abhängt. So ist die Grundrechtsintensität wohl geringer, wenn die Betroffenheit des Einzelnen zumindest vom Vorliegen bestimmter einzelner oder mehrere Tatsachen abhängt.

b) Erkundigungen im Umfeld einer Person und Vernehmungen von Zeugen, Sachverständigen und dem Beschuldigten

Soweit darüber hinaus auf der Grundlage von § 161 Abs. 1 S. 1 StPO einfache Erkundigungen und Vernehmungen zulässig sein sollen[1569], dürfte sich in diesem Zusammenhang aus der nach § 136 StPO zu beachtenden Pflicht zur Belehrung des Beschuldigten ergeben, dass eine erhöhte Intensität bei verdeckten Maßnahmen besteht.[1570] Denn einfache Erkundigungen von Personen können nach § 161 Abs. 1 S. 1 StPO nur zulässig sein, soweit gegen die hiervon betroffene Person noch kein Anfangsverdacht besteht. Sobald ein solcher Verdacht besteht, ist der Beschuldigte nach § 136 StPO entsprechend über die Tatvorwürfe zu belehren. Hieraus ergibt sich insoweit, dass eine erhöhte Intensität besteht, soweit die staatliche Maßnahme gegenüber dem Betroffenen nicht offengelegt wird.[1571]

c) Einsatz von V-Leuten, Scheinkäufern und nicht offen ermittelnden Polizeibeamten

In diesem Zusammenhang ist insbesondere auch auf die bereits kurz angesprochene[1572] Zulässigkeit des Einsatzes von V-Leuten und Scheinkäufern nach §§ 161, 163 StPO in Abgrenzung zum Einsatz von verdeckten Ermittlern nach §§ 110a ff. StPO einzugehen. Denn hieraus ergibt sich, ab wann eine derart erhöhte Eingriffsintensität besteht, dass sie besonderen gesetzlichen Anforderungen der §§ 110a StPO unterliegt.

1569 Gercke/Julius/Temming/Zöller/*Zöller,* § 161 Rn. 20.
1570 Vgl. *Hefendehl*, StV 2001, 700 (703).
1571 Vgl. *Hefendehl*, StV 2001, 700 (703).
1572 Siehe hierzu bereits oben unter Kap. 5, B.VIII.

Hierzu ist zunächst zwischen den unterschiedlichen Begriffen von V-Leuten, Scheinkäufern, nicht offen ermittelnden Polizeibeamten und verdeckten Ermittlern zu differenzieren:

V-Leute sind als sog. Vertrauenspersonen zu verstehen.[1573] Sie sind selbst keine Polizeibeamten, gehören in der Regel einem kriminellen Milieu an und liefern den Strafverfolgungsbehörden über einen längeren Zeitraum vertrauliche Informationen zum Zwecke der Strafverfolgung.[1574] Begrifflich hiervon abgegrenzt werden außerdem sog. Informanten, die lediglich einzelfallbezogen oder für einen kurzen Zeitraum den Strafverfolgungsbehörden Informationen zur Strafverfolgung mitteilen.[1575]

Dem entgegen handelt es sich bei den nicht offen ermittelnden Polizeibeamten (nachfolgend als „noeP" bezeichnet) zunächst um Polizeibeamte, die ihre Funktion als Polizeibeamte nicht offenlegen. Sie treten jedoch nur kurzfristig oder einzelfallbezogen – etwa als Scheinkäufer von Betäubungsmitteln – auf.[1576]

Um einen Verdeckten Ermittler handelt es sich dagegen, wenn ein Polizeibeamter unter einer auf Dauer angelegten, veränderten Identität (=Legende) auftritt und so insbesondere im Bereich der organisierten Kriminalität ermittelt.[1577]

Nach der herrschenden Literaturauffassung und Rechtsprechung soll der Einsatz von V-Leuten, Informanten und noeP nach den §§ 161, 163 StPO zulässig sein.[1578] Zwar gab es auch in diesem Zusammenhang schon intensive Diskussionen um die spezialgesetzliche Regelung des Einsatzes von V-Leuten und Informanten, bisher wurden diese aber noch nicht umgesetzt.[1579] Nur für den Einsatz verdeckter Ermittler gelten also die speziellen Anforderungen der §§ 110a ff. StPO.

Insoweit ist insbesondere die Abgrenzung zwischen noeP und verdeckten Ermittlern relevant.

1573 *Gercke*, StV 2017, 615 (615).

1574 BeckOK-StPO/*Hegmann,* § 110a Rn. 7; *Gercke*, StV 2017, 615 (615) mit Verweis auf Abschnitt I.2.2 des Anhangs D der RiStBV; *Soiné*, NStZ 2014, 248 (251).

1575 *Soiné*, NStZ 2014, 248 (251).

1576 KK-StPO/*Bruns,* § 110a Rn. 5; *Weisser*, NZWiSt 2018, 59 (59); *Schneider*, NStZ 2004, 359 (359).

1577 BGHSt 41, 64 (65); KK-StPO/*Bruns,* § 110a Rn. 5; *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, S. 421.

1578 BVerfG NJW 2012, 833 (840); *Weisser*, NZWiSt 2018, 59 (61) m.w.N.; *Schneider*, NStZ 2004, 359 (359).

1579 *Gercke*, StV 2017, 615 (617) m.w.N.

Nach ständiger Rechtsprechung des BGH kommt es für diese Abgrenzung darauf an,

> *„ob unter Würdigung der gesamten Umstände sein Ermittlungsauftrag über wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, ob die Täuschung einer unbestimmten Vielzahl von Personen (über die Identität des Beamten) erforderlich werden wird und ob sich von vornherein absehen lässt, dass der Schutz des Beamten seine Geheimhaltung auch für die Zukunft erfordert, mit der Folge, dass er im Strafverfahren nicht oder nur eingeschränkt als Zeuge zur Verfügung stehen wird. Dabei ist darauf abzustellen, ob der allgemeine Rechtsverkehr oder die Beschuldigtenrechte in künftigen Strafverfahren eine mehr als nur unerhebliche Beeinträchtigung durch den Einsatz des verdeckt operierenden Polizeibeamten erfahren können"*[1580].

Insoweit soll der lediglich einmalig oder wenige Male auftretende Scheinkäufer, der nicht in die Ermittlungen eingebunden wird, als noeP einzuordnen sein, dessen Einsatz nicht an die strengeren Voraussetzungen der §§ 110a ff. StPO geknüpft ist.[1581]

Dementsprechend hängt die Abgrenzung zwischen noeP und verdecktem Ermittler in der Regel davon ab, ob der Polizeibeamte auf Dauer unter einer falschen Identität auftritt und die hiervon betroffenen Personen insbesondere auch unter Ausnutzung etwaigen persönlichen Vertrauens über seine wahre Identität täuscht.

Aus dem Vergleich des nach §§ 161, 163 StPO zulässigen Einsatzes von noeP zum nach §§ 110a ff. StPO zulässigen Einsatz von verdeckten Ermittlern ergibt sich insoweit, dass sich jedenfalls die dauerhafte und auf persönlichem Vertrauen beruhende Täuschung des Betroffenen derart intensitätssteigernd auswirkt, dass zusätzliche Anforderungen erfüllt sein müssen. Darüber hinaus lässt sich wiederum die Streubreite als intensitätssteigernden Aspekt ableiten, da ja gerade die Häufigkeit des Auftretens unter der falschen Identität die Einordnung als verdeckten Ermittler zur Folge hat.[1582]

1580 BGH NStZ 1995, 516 (516) ; BGH, NStZ 1997, 448 (448); *Weisser*, NZWiSt 2018, 59 (60). In der Literatur wird darüber hinaus auch die Auffassung vertreten, dass die Abgrenzung anhand des Merkmals der Dauer des Einsatzes vorzunehmen ist, vgl. *Weisser*, NZWiSt 2018, 59 (6) mit Verweis auf *Schneider*, NStZ 2004, 359 (361).

1581 *Schneider*, NStZ 2004, 359 (360).

1582 Vgl. *Schneider*, NStZ 2004, 359 (361, 367). Dagegen ergibt sich aus diesem Vergleich noch nicht, dass auch die Heimlichkeit von Ermittlungsmaßnahmen intensitätssteigernd sind, da sowohl der Einsatz von noeP als auch der Einsatz von

d) Insbesondere: Online-Ermittlungen

Besonders hervorzuheben ist außerdem, dass die sog. Online-Ermittlungen bzw. Ermittlungen im Internet wohl nach herrschender Meinung zulässigerweise auf § 161 Abs. 1 StPO gestützt werden können.[1583] Begrifflich soll die Online-Ermittlung den Abruf und die Kenntnisnahme von allgemein zugänglichen Daten im Internet zum Zwecke der Strafverfolgung betreffen. Insoweit besteht eine Ähnlichkeit der Online-Ermittlung zu den hier gegenständlichen Auswertungsmethoden, da in beiden Fällen auf Daten zugegriffen wird, die allgemein zugänglich sind.[1584]

Zunächst ist zu bestimmen, welche konkreten Ermittlungshandlungen vom Begriff der Online-Ermittlung erfasst sind und welche dieser Ermittlungshandlungen auf § 161 Abs. 1 StPO gestützt werden können (hierzu unter (1)). Nachfolgend soll darauf eingegangen werden, ob es spezielle Ermittlungsbefugnisse gibt, die Ähnlichkeiten zu der Online-Ermittlung aufweisen und welcher Rückschluss aus dem Vergleich mit diesen speziellen Ermittlungsbefugnissen gezogen werden kann (hierzu unter (2)) Schließlich wird auf eine erste Bestimmung der Grenzen der Zulässigkeit solcher Online-Ermittlungen im Rahmen der Ermittlungsgeneralklauseln eingegangen (hierzu unter (3)).

(1) Gegenstand der Online-Ermittlung

In der Kommentarliteratur erfasst die Online-Ermittlung zunächst den Abruf und die Kenntnisnahme von allgemein zugänglichen Inhalten im Internet.[1585] Dies betrifft etwa den Aufruf allgemein zugänglicher Internetseiten. Hiervon erfasst soll darüber hinaus auch der Aufruf von nicht

verdeckten Ermittlern heimlich erfolgt. Zwar ließe sich hieraus ableiten, dass jedenfalls die längerfristige Heimlichkeit intensitätssteigernd sein kann, aber die unmittelbare Intensitätssteigerung aus der Heimlichkeit selbst, ergibt sich hieraus noch nicht.

1583 BeckOK-StPO/*Sackreuther,* § 161 Rn. 11; MüKo-StPO/*Kölbel,* § 161 Rn. 11; KMR-StPO/*Notensmeier-von Osten,* § 161 Rn. 21; Löwe-Rosenberg/*Erb,* § 161 Rn. 5; vgl. ausführlich hierzu *Rückert*, ZStW 129 (2017), 302 (302ff.).

1584 Siehe zur allgemeinen Zugänglichkeit der von den Auswertungsmethoden ausgewerteten Daten bereits oben unter Kap. 2, A.IV., Kap. 4, B.II.2.c).

1585 BVerfGE 120, 274 (344f.); BeckOK-StPO/*Sackreuther,* § 161 Rn. 11; KK-StPO/*Griesbaum,* § 161 Rn. 12a; SK-StPO/*Weßlau/Deiters,* § 161 Rn. 14; *Soiné*, NStZ 2014, 248 (248); *Soiné*, NStZ 2010, 596 (602); *Rosengarten/Römer*, NJW 2012, 1764 (1765).

zugangsgesicherten Chat-Foren oder das Abonnieren von Mailing-Listen erfasst sein.[1586]

So nimmt etwa *Griesbaum* an, dass „[d]ie Online-Streife in allgemein zugänglichen Bereichen ohne gezielte Datenerhebung [...] ohne weiteres zulässig"[1587] ist, da hierdurch kein Eingriff in das RiS vorliege.[1588] So soll etwa auch der Aufruf einer Profilseite in einem sozialen Netzwerk zulässig sein, soweit diese Seite für alle Teilnehmer des sozialen Netzwerkes sichtbar ist.[1589] Konkret kann insoweit nach *Griesbaum* etwa die Facebook-Profil-Seite eines Einzelnen ohne Weiteres aufgerufen werden und die dort allgemein zugänglichen Daten abgerufen werden, soweit dies keine gezielte Suche nach Informationen über eine Person darstellt.[1590] Dagegen soll nach *Griesbaum* aber dann ein Grundrechtseingriff vorliegen, der aber wohl durch § 161 Abs. 1 StPO gerechtfertigt sein soll, wenn hierbei gezielt nach Informationen über Personen gesucht wird.[1591]

Darüber hinaus sollen in diesem Rahmen etwa auch die Teilnahme und das Aufzeichnen von Kommunikation in Chat-Foren zulässig sein, soweit für die Teilnahme keine Legitimierung erforderlich ist.[1592]

Weiterhin sind im Rahmen von Online-Ermittlungen aber noch weitergehende systematische Erhebungen und Auswertungen von öffentlich zugänglichen Daten möglich.[1593] Ob diese aber noch im Rahmen der §§ 161, 163 StPO zulässig sind, thematisiert die bisherige Kommentarliteratur allerdings noch nicht in Einzelheiten[1594] (hierzu nachfolgend im Einzelnen unter (3)).

1586 BVerfGE 120, 274 (344f.); *Rosengarten/Römer*, NJW 2012, 1764 (1765).

1587 KK-StPO/*Griesbaum,* § 161 Rn. 12a. Vgl. zur Einordnung als Grundrechtseingriffe bei der Kenntnisnahme öffentlich verfügbarer Daten bereits oben unter Kap. 4, B.II.2.b).

1588 KK-StPO/*Griesbaum,* § 161 Rn. 12a.

1589 KK-StPO/*Griesbaum,* § 161 Rn. 12a.

1590 Vgl. KK-StPO/*Griesbaum,* § 161 Rn. 12a.

1591 KK-StPO/*Griesbaum,* § 161 Rn. 12a.

1592 KMR-StPO/*Noltensmeier-von Osten,* § 161 Rn. 21; SK-StPO/*Weßlau/Deiters,* § 161 Rn. 17; Gercke/Julius/Temming/Zöller/*Zöller,* § 163 Rn. 12; *Soiné*, NStZ 2014, 248 (248); *Klesczewski*, ZStW 123 (2011), 737 (739f.); *Rosengarten/Römer*, NJW 2012, 1764 (1765).

1593 Siehe hierzu insbesondere *Rückert*, ZStW 129 (2017), 302 (306ff.); vgl. auch KMR-StPO/*Notensmeier-von Osten,* § 163 Rn. 17, der unter Verweis auf *Rückert*, ZStW 129 (2017), 302 (306ff.), zu dem Ergebnis kommt, dass derartige, systematische Datenauswertungen nicht nach §§ 161, 163 StPO zulässig sind.

1594 Vgl. hierzu bisher lediglich aus der Kommentarliteratur KMR-StPO/*Notensmeier-von Osten,* § 163 Rn. 17.

Nach der bisherigen herrschenden Literaturauffassung liegen die Grenzen der Zulässigkeit dieser Online-Ermittlungen nach § 161 Abs. 1 StPO allerdings jedenfalls dort, wo entweder Zugangsbeschränkungen hinsichtlich der ausgewerteten Internetkommunikation überwunden werden bzw. werden müssen[1595] oder dort, wo schutzwürdiges Vertrauen der Betroffenen ausgenutzt wird[1596].

(2) Ähnliche, spezielle Ermittlungsbefugnisse

Insoweit verläuft die Grenze der Zulässigkeit der Online-Ermittlung nach § 161 Abs. 1 StPO dort, wo insbesondere spezielle Ermittlungsbefugnisse einschlägig sind.

Denn, soweit etwa Zugangsbeschränkungen überwunden werden, soll etwa ein Eingriff in das Fernmeldegeheimnis vorliegen, für den eine entsprechende Rechtfertigung in Form einer gesetzlichen Befugnis erforderlich ist.[1597]

Dies ergibt sich insbesondere auch aus dem Vergleich mit den Ermittlungsbefugnissen der §§ 100a, 100b StPO. Denn diese ermöglichen – anders als bei den zuvor dargestellten Online-Ermittlungen nach §§ 161, 163 StPO – auch den Zugriff auf (Kommunikations-)Inhalte, die nicht im Internet allgemein zugänglich sind.[1598]

Nach § 100a StPO kann auch „ohne Wissen der Betroffenen […] die Telekommunikation überwacht und aufgezeichnet werden"[1599]. Klassischerweise betrifft § 100a StPO damit den Zugriff auf Telekommunikation, die vom Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG erfasst ist – der Schutzbereich des Art. 10 Abs. 1 GG und die Reichweite des nach § 100a StPO zulässigen Zugriffs sind aber nicht deckungsgleich.[1600] Nach § 100a Abs. 1 S. 2 StPO ist aber auch der Zugriff auf informationstechnisches Sys-

1595 Gercke/Julius/Temming/Zöller/*Zöller,* § 163 Rn. 12; *Klesczewski*, ZStW 123 (2013), 737 (739ff.).

1596 Vgl. *Soiné*, NStZ 2014, 248 (249); *Rosengarten/Römer*, NJW 2012, 1764 (1766f.) mit Verweis auf BVerfGE 120, 274 (345).

1597 *Klesczewski*, ZStW 123 (2013), 737 (739).

1598 Vgl. *Safferling/Rückert,* MMR 2015, 788 (793).

1599 Wortlaut des § 100a Abs. 1 S. 1 StPO.

1600 Siehe zur umstrittenen Frage, ob Schutzbereich des Art. 10 GG und Anwendungsbereich des § 100a StPO deckungsgleich sind, bereits ausführlich oben unter Kap. 5, B.IV.

tem zur Überwachung der damit geführten Telekommunikation möglich (sog. Quellen-TKÜ).[1601] Jedenfalls betrifft § 100a StPO aber die nicht öffentlich geführte Telekommunikation – öffentlich geführte Telekommunikation ist dagegen vom Anwendungsbereich des § 100a StPO nicht erfasst.[1602]

Von der Ermittlungsbefugnis des § 100b StPO ist darüber hinaus die sog. Online-Durchsuchung erfasst.[1603] Denn nach § 100b StPO kann auf informationstechnische Systeme ohne Wissen des Betroffenen zugegriffen werden und die dort gespeicherten Daten erhoben werden. § 100b StPO ermöglicht damit einen Eingriff in das IT-Grundrecht und damit den Zugriff auf informationstechnische Systeme auf einem technischen Weg, der dafür nicht vorgesehen ist und damit den Zugriff unter Überwindung von berechtigten Vertraulichkeitserwartungen des Betroffenen.[1604]

Aus dem Vergleich der nach §§ 100a, 100b StPO zulässigen Ermittlungsbefugnisse mit den nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen ergibt sich daher insoweit, dass einerseits ein intensitätserhöhender Faktor vorliegt, wenn unter Überwindung von Zugangsbeschränkungen und berechtigten Vertraulichkeitserwartungen auf Kommunikation zugegriffen wird. Im Umkehrschluss ergibt sich daraus andererseits, dass dann ein intensitätsverringernder Faktor vorliegt, wenn es gerade keine Zugangsbeschränkungen oder berechtigte Vertraulichkeitserwartungen gibt. Insoweit ergibt sich hieraus auch, dass eine geringere Grundrechtsintensität vorliegt, wenn nur solche Informationen ausgewertet werden, die allgemein zugänglich sind.

(3) Exkurs – Grenze der nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen

Erste Grenzen der Zulässigkeit von Online-Ermittlungen nach §§ 161, 163 StPO hat *Rückert* entwickelt:

So arbeitet *Rückert* zunächst heraus, dass die bloße öffentliche Verfügbarkeit von Informationen noch nicht insgesamt dazu führe, dass auch die Ermittlungsgeneralklauseln als Rechtfertigung für den Grundrechtsein-

1601 Vgl. BeckOK-StPO/*Graf,* § 100a Rn. 113f.
1602 *Rückert*, ZStW 129 (2017), 302 (316); vgl. *Safferling/Rückert,* MMR 2015, 788 (793).
1603 BeckOK-StPO/*Graf,* § 100b.
1604 Siehe hierzu bereits oben unter Kap. 5, B.V.

griff ausreichten.[1605] Hierzu zieht *Rückert* insbesondere einen Vergleich mit speziellen Ermittlungsbefugnissen in der analogen Welt heran, die sich ebenfalls auf Informationen aus dem öffentlichen Raum beziehen.[1606]

Ferner arbeitet *Rückert* heraus, dass insbesondere die automatisierte und die manuelle Auswertung von Informationen eine unterschiedliche Grundrechtsintensität aufweisen, sodass eine spezielle Ermächtigungsgrundlage erforderlich sein kann.[1607] Dabei stellt *Rückert* für die Frage der Grenzziehung darauf ab, ob von einer technikgestützten Auswertung die Gefahr für das allgemeine Persönlichkeitsrecht besteht, dass umfassende Persönlichkeits- und Bewegungsprofile erstellt werden könnten.[1608]

So kommt *Rückert* zu dem Ergebnis, dass die manuelle Erhebung und Auswertung von öffentlich verfügbaren Informationen im Internet wohl auf die Ermittlungsgeneralklauseln gestützt werden könne, da die Gefahr der Persönlichkeitsrechtsgefährdung gerade durch die beschränkten Möglichkeiten von manuellen Auswertungen begrenzt sei.[1609] Hinsichtlich einer „automatisierten Suche, Erhebung und Verarbeitung öffentlich zugänglicher Daten"[1610] kommt *Rückert* dagegen zu dem Ergebnis, dass zunächst danach zu differenzieren sei, ob derartige Ermittlungsinstrumente gegen konkret Tatverdächtige eingesetzt werden oder zum Zweck der Rasterdatenerhebung eingesetzt werden.[1611] Denn beim Einsatz zur Gewinnung von Beweisdaten würden Daten von unverdächtigen Personen nur erhoben, wenn dies unvermeidbar sei, wohingegen beim Einsatz zur Rasterdatenerhebung auch eine unüberschaubare Vielzahl nichtverdächtiger Personen betroffen sein könnte.[1612] Auf die Ermittlungsgeneralklauseln könnten automatisierte Ermittlungsmethoden nach *Rückert* allenfalls dann gestützt werden, wenn sie zur Gewinnung von Beweisdaten eingesetzt werden – *Rück-*

1605 *Rückert,* ZStW 129 (2017), 302 (325).
1606 *Rückert,* ZStW 129 (2017), 302 (325), der etwa auf die nur nach § 100h StPO zulässige Anfertigung von Bildaufnahmen im öffentlichen Bereich abstellt.
1607 *Rückert,* ZStW 129 (2017), 302 (326).
1608 *Rückert,* ZStW 129 (2017), 302 (326). Alternativ bestünde auch die Möglichkeit einer rein technischen Grenzziehung, die aber angesichts der vielfach bereits bei der einfachen Google-Suche eingesetzten Software nicht praktikabel ist, vgl. *Rückert,* ZStW 129 (2017), 302 (326). Vgl. zur Nutzung netzwerkinterner Suchfilter *Bauer*, Soziale Netzwerke, S. 145f. mit Verweis auf *Oermann/Staben*, Der Staat 2013, 630 (646).
1609 *Rückert,* ZStW 129 (2017), 302 (328).
1610 *Rückert,* ZStW 129 (2017), 302 (329).
1611 *Rückert,* ZStW 129 (2017), 302 (329).
1612 *Rückert,* ZStW 129 (2017), 302 (329).

ert empfiehlt jedoch auch für diesen Bereich eine gesetzliche Regelung, der sich an §§ 163e, 163f StPO orientieren solle.[1613] Dagegen sei nach *Rückert* die Grenze der Ermittlungsgeneralklauseln beim Einsatz zum Zweck der Rasterdatenerhebung überschritten, da hierdurch „zahlreiche[…] Daten von Nicht-Verdächtigen"[1614] einbezogen würden und insoweit eine große Vergleichbarkeit mit §§ 163d StPO und § 111 StPO bestünde.[1615]

(4) Zwischenergebnis

Aus dem Vorstehenden ergibt sich, dass nach § 161 Abs. 1 StPO jedenfalls der Aufruf und die Kenntnisnahme von öffentlich zugänglichen Inhalten im Internet zulässig ist, auch, wenn diese gezielt eingesetzt werden, um Informationen über Einzelpersonen zu ermitteln.[1616] Grenzen dieser nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen liegen dort, wo Zugangsbeschränkungen überwunden werden und berechtigte Vertraulichkeitserwartungen des Betroffenen bestehen.[1617] Hieraus ergibt sich, dass ein derartiger Zugriff wesentlich intensitätssteigernd ist.[1618] Eine weitere Grenze könnte auf Grund der Gefährdung des Persönlichkeitsrechts in der technikgestützten Auswertung öffentlich verfügbarer Inhalte liegen.[1619] Wann diese Grenze überschritten ist, dürfte maßgeblich davon abhängen, ob eine große Streubreite der Maßnahme vorliegt.[1620]

e) Abfragen von Kontoinformationen im Rahmen Europäischer Rechtshilfe

Schließlich können auch § 91c Abs. 2 Nr. 2 lit. b), lit. c) lit. aa) IRG und dessen Gesetzesbegründung als Vergleichsmaßstab herangezogen werden.

Die Vorschriften wurden zur Umsetzung der sog. Europäischen Ermittlungsanordnung (nachfolgend als „EEA" bezeichnet) eingeführt. Die EEA

1613 *Rückert,* ZStW 129 (2017), 302 (331).
1614 *Rückert,* ZStW 129 (2017), 302 (331).
1615 *Rückert,* ZStW 129 (2017), 302 (331f.).
1616 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(1).
1617 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(2)ii.
1618 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(2)ii.
1619 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(3)iii.
1620 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(3)iii.

beruht auf der RL (EU) 2014/41 (nachfolgend als „RL EEA" bezeichnet).[1621] Eines der Ziele der EEA ist es, die grenzüberschreitende Beweiserhebung innerhalb der EU zu vereinfachen und zu beschleunigen.[1622] Im Zusammenhang mit Ermittlungen bei Bankkonten enthält die RL EEA unter anderem die folgenden Vorgaben an die Mitgliedstaaten:

Art. 27 RL EEA enthält die Befugnis zur Ermittlung von „Informationen über Bank- und sonstige Finanzgeschäfte"[1623]. Nach Art. 27 Abs. 1 RL EEA soll eine EEA erlassen werden können, „um Angaben über bestimmte Bankkonten sowie über Bankgeschäfte zu erlangen, die während eines bestimmten Zeitraums über ein oder mehrere in der EEA angegebenes/angegebene Bankkonto/Bankkonten getätigt wurde, einschließlich der Angaben über sämtliche Überweisungs- und Empfängerkonten."[1624]

Darüber hinaus sieht Art. 28 Abs. 1 lit. a) RL EEA grundsätzlich die Möglichkeit einer fortlaufenden Überwachung von Bank- oder sonstigen Finanzgeschäften über einen bestimmten Zeitraum vor.[1625]

Zur Umsetzung der RL EEA hat der deutsche Gesetzgeber unter anderem einen zweiten Abschnitt des 10. Teils des IRG geschaffen und hierin Regelungen für die Umsetzung der EEA geschaffen.[1626] Hierin ist eine ergänzende Zulässigkeitsvoraussetzung[1627] für bestimmte Formen der Rechtshilfe in § 91c IRG enthalten.[1628] Ziel von § 91c IRG ist die Umsetzung der besonderen Zurückweisungsgründe der Art. 22ff. RL EEA.[1629] Dabei enthält § 91c Abs. 2 IRG eine „vollumfängliche Anwendung von § 59 Abs. 3 IRG"[1630]. § 59 Abs. 3 IRG regelt den Grundsatz, dass Rechtshilfe nur geleistet werden darf, „wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten."[1631] Hieraus ergibt sich, dass die Rechtshilfe nicht zulässig ist, „wenn die erbetene Ermittlungsmaßnahme in einem vergleich-

1621 BT-Drs. 18/9757, S. 17.
1622 BT-Drs. 18/9757, S. 19.
1623 So die amtliche Überschrift des Art. 27 RL (EU) 2014/41.
1624 So der Wortlaut des Art. 27 Abs. 1 RL (EU) 2014/41.
1625 *Leonhardt,* Die Europäische Ermittlungsanordnung in Strafsachen, S. 86.
1626 Vgl. BT-Drs. 18/9757, S. 17ff., S. 54f.
1627 Die grundsätzliche Zulässigkeit der sonstigen Rechtshilfe innerhalb der Europäischen Union richtet sich nach §§ 91a, 91b IRG, vgl. BT-Drs. 18/9757, S. 55, 57ff.
1628 BT-Drs. 18/9757, S. 62.
1629 BT-Drs. 18/9757, S. 62.
1630 BT-Drs. 18/9757, S, 62.
1631 So der Wortlaut des § 59 Abs. 3 IRG.

baren innerstaatlichen Fall nicht zulässig wäre"[1632]. Dies ist etwa für die Kontoüberwachung in Echtzeit der Fall, die das deutsche Strafprozessrecht nicht kennt.[1633]

Für die hier gegenständliche Untersuchung sind dabei insbesondere die besonderen Zulässigkeitsvoraussetzungen für die Abfrage von Kontoinformationen in § 91c Abs. 2 Nr. 2 lit. b), lit. c) lit. aa) IRG und die jeweilige Gesetzesbegründung relevant.

§ 91c Abs. 2 Nr. 2 lit. b) IRG enthält dabei die besondere Zulässigkeitsvoraussetzung, dass Rechtshilfeersuchen zurückgewiesen werden können, wenn die „Abfrage von bestimmten Kontenbewegungen […] [als] Ermittlungsmaßname in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde[1634]. Hiermit soll der besondere Zurückweisungsgrund des Art. 27 Abs. 5 S. 3 RL EEA umgesetzt werden.[1635] In der Gesetzesbegründung verweist der Gesetzgeber zur Erhebung von Kontoinformationen auf die gängige Ermittlungspraxis, nach den „§§ 160, 161a StPO eine Auskunft von der betroffenen Bank"[1636] zu verlangen. Sollte die jeweilige Bank diesem Ersuchen nicht nachkommen, sei eine zeugenschaftliche Vorladung nach §§ 161a Abs. 2, 51, 70 StPO oder die Durchsuchung und Beschlagnahme nach §§ 98, 102, 103 StPO in Betracht zu ziehen.[1637]

§ 91c Abs. 2 Nr. 2 lit. c) lit. aa) IRG enthält darüber hinaus die besondere Zulässigkeitsvoraussetzung für sog. Echtzeitmaßnahmen und setzt damit den besonderen Zurückweisungsgrund aus Art. 28 Abs. 1 RL EEA um.[1638] Denn nach Art. 28 Abs. 1 RL EEA ist es grundsätzlich möglich, eine EEA zu erlassen, „um Beweismittel in Echtzeit, fortlaufend oder über einen bestimmten Zeitraum zu erheben."[1639] In Art. 28 Abs. 1 Hs. 2 RL EEA ist aber auch der besondere Zurückweisungsgrund enthalten, dass die „Vollstreckung [auch] versagt werden [kann], wenn die Durchführung der betreffenden Ermittlungsmaßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde."[1640] Dies ist insoweit relevant, als dass der Gesetzgeber in der Gesetzesbegründung darauf verweist, dass nach „der StPO

1632 BT-Drs. 18/9757, S, 62.
1633 BT-Drs. 18/9757, S, 62. Vgl. insoweit § 91c Abs. 2 Nr. 2 lit. c) lit. aa) IRG.
1634 BT-Drs. 18/9757, S. 63.
1635 BT-Drs. 18/9757, S. 63.
1636 BT-Drs. 18/9757, S. 40.
1637 BT-Drs. 18/9757, S. 40.
1638 BT-Drs. 18/9757, S. 64.
1639 BT-Drs. 18/9757, S. 40.
1640 So der Wortlaut des Art. 28 Abs. 1 Hs. 2 RL EEA.

[…] in die Zukunft gerichtete Kontoüberwachungen in Echtzeit nicht zugelassen"[1641] sind.[1642] Nach der StPO seien allenfalls „periodische Auskunftsersuchen, durch die in gewissen Zeitabständen rückwirkende Kontoabfragen durch die Strafverfolgungsbehörden erfolgen"[1643], möglich.[1644]

Für die hier gegenständliche Untersuchung ergibt sich hieraus, dass nach Ermittlungsbefugnissen der §§ 161, 163 StPO weder Unterlagen herausverlangt werden können noch Konten fortlaufend überwacht werden können. Für ein Herausgabeverlangen von Unterlagen sind nur die Vorschriften zur Herausgabe und Beschlagnahme (§§ 94, 95, 98, 102, 103 StPO) einschlägig.[1645] Für eine fortlaufende Überwachung von Konten besteht in der StPO dagegen keine Ermächtigungsgrundlage.[1646]

Aus diesem Vergleich ergibt sich insoweit, dass kein geringfügiger Grundrechtseingriff mehr vorliegt, wenn Beweismittel (gegen den Willen des Berechtigten) sichergestellt werden oder eine fortlaufende Überwachung stattfindet. Insoweit besteht hier eine Parallele zur der bereits dargestellten Abgrenzung von kurz- und längerfristigen Observationen.[1647] Dementsprechend ergibt sich auch aus diesem Vergleich, dass bei umfangreicheren Informationserhebungen, sowie einer erhöhten Streubreite[1648] ein nicht mehr nur geringfügiger Grundrechtseingriff vorliegt.

f) Zwischenergebnis

Aus den vorstehenden Vergleichen der nach § 161 Abs. 1 StPO bisher als zulässig angesehenen Ermittlungsmaßnahmen mit den speziell geregelten Ermittlungsbefugnissen ergibt sich, dass für die Grundrechtsintensität von

1641 BT-Drs. 18/9757, S. 64.
1642 BT-Drs. 18/9757, S. 64.
1643 BT-Drs. 18/9757, S. 64.
1644 BT-Drs. 18/9757, S. 64.
1645 BT-Drs. 18/9757, S. 40; vgl. KK-StPO/*Griesbaum,* § 161 Rn. 8. Zu beachten ist insoweit, dass die freiwillige Herausgabe von potenziellen Beweismitteln nach § 94 Abs. 1 StPO ebenfalls nur ein Anfangsverdacht erforderlich ist. Lediglich die Beschlagnahme gegen den Willen des Berechtigten bedürfen den zusätzlichen Anforderungen der Beschlagnahme nach §§ 97, 98 StPO. Vgl. insoweit hierzu bereits ausführlich oben unter Kap. 5, B.I.1.
1646 BT-Drs. 18/9757, S. 64.
1647 Siehe hierzu bereits oben unter Kap. 5, D. II.1.a)(3).
1648 Denn auch bei der fortlaufenden Überwachung von Bankkonten dürfte eine größere Anzahl von Personen anlasslos von der Maßnahme betroffen werden.

Ermittlungsmaßnahmen unter anderem die folgenden Faktoren und Kriterien relevant sind:

Zunächst wirkt sich der Umfang der erhobenen Informationen auf die Grundrechtsintensität aus. So liegt jedenfalls eine gesteigerte Grundrechtsintensität bei umfangreicheren Datensätzen vor, eine geringe Grundrechtsrelevanz grundsätzlich, wenn nur einzelne Informationen erhoben werden.

Außerdem hängt die Grundrechtsintensität vom Inhalt und der Art der Erhebung der jeweiligen Information ab. So liegt insbesondere dann eine erhöhte Grundrechtsintensität vor, wenn bei der Erhebung berechtigte Vertraulichkeitserwartungen oder Zugangsbeschränkungen überwunden werden. So liegt etwa bereits bei der verdeckten Erhebung von Informationen grundsätzlich eine erhöhte Grundrechtsintensität vor. Besonders grundrechtsintensiv sind darüber hinaus Erhebungen, die unter Überwindung von grundrechtlich geschützten Vertraulichkeitserwartungen vorgenommen werden. Dagegen liegt eine deutlich geringere Grundrechtsintensität vor, wenn lediglich Informationen erhoben werden, die allgemein zugänglich sind und bei denen insoweit keine Vertraulichkeitserwartungen bestehen.

Darüber hinaus steht im engen Zusammenhang mit dem Inhalt und der Art der Erhebung auch die Art und Weise der Auswertung der Informationen, die sich ebenfalls intensitätssteigernd auswirken kann. So ist hier insbesondere die technikgestützte Auswertung von Informationen durch maschinelle Datenabgleiche in den Blick zu nehmen, bei der eine hohe Intensitätssteigerung vorliegt. Denn hierdurch können einerseits auch einzelne Informationen mit geringem Informationsgehalt derart miteinander verknüpft werden, dass sich hieraus sensible Informationen ergeben können. Andererseits können bei der technikgestützten Auswertung gerade auch viele Personen betroffen sein, die durch ihr Verhalten keinen Anlass gegeben haben, von einer staatlichen Ermittlungsmaßnahme betroffen zu sein (Streubreite).

Dabei ist die Streubreite insgesamt ein wesentlicher Faktor der Grundrechtsintensität von Ermittlungsmaßnahmen – sowohl bei der Auswertung von Informationen als auch bei der Erhebung der ausgewerteten Informationen. So besteht eine wesentlich erhöhte Grundrechtsintensität, wenn eine Vielzahl unbeteiligter Personen von staatlichen Ermittlungsmaßnahmen betroffen ist. Darüber hinaus ist hierbei die Grundrechtsintensität der Streubreite außerdem danach abzustufen, ob es überhaupt einen Anlass dafür gegeben hat, dass der Einzelne von der Maßnahme betroffen ist und in welcher Intensität und Form dieser Anlass bestanden hat.

2. Rechtsprechung des BVerfG zu Kriterien und Bewertung der Grundrechtsintensität

Zu diesen Kriterien für die Bewertung der Grundrechtsintensität kommt auch die Rechtsprechung des BVerfG weitgehend.

So nimmt das BVerfG an, dass die Grundrechtsintensität „insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten beeinflusst wird"[1649]. So sind hier grundsätzlich vier verschiedene Kriterien zu unterscheiden, die sich allerdings in ihren Einzelheiten teilweise wieder überschneiden. Trotzdem soll nachfolgend versucht werden, diese Kriterien jeweils im Einzelnen darzustellen.[1650]

a) Art der erfassten Informationen

Grundsätzlich ist nach dem BVerfG zunächst für die Beurteilung der Grundrechtsintensität relevant, welche Persönlichkeitsrelevanz die jeweiligen Informationen haben.[1651] Insoweit wirkt sich etwa intensitätsverringernd aus, wenn die Daten anonym sind[1652] oder der Personenbezug erst durch Zusatzwissen hergestellt werden kann.[1653] Eine absolute Grenze der Intensität ist dagegen der Kernbereich privater Lebensgestaltung.[1654] Zu

1649 BVerfGE 120, 378 (Ls. 2).

1650 Nachfolgend wird insbesondere auch auf Rechtsprechung des BVerfG eingegangen, die sich zur Grundrechtsintensität bei Eingriffen in Art. 10, Art. 13 GG äußert. Nach BVerfGE 115, 320 (347) finden die in diesem Zusammenhang festgestellten Grundsätze aber auch für Eingriffe in das RiS Anwendung.

1651 BVerfGE 115, 320 (347); BVerfGE 118, 168 (196f.); vgl. außerdem BVerfGE 100, 313 (376); 109, 279 (353), 113, 348 (382) deren Maßstäbe zur Bewertung der Grundrechtsintensität bei Eingriffen in das Fernmeldegeheimnis, nach BVerfGE 115, 320 (347) grundsätzlich anwendbar sind.

1652 BVerfGE 65, 1 (45); BVerfGE 100, 313 (376); BVerfGE 115, 320 (347). Unklar ist allerdings, inwieweit bei anonymen Daten überhaupt ein Grundrechtseingriff vorliegen soll (vgl. hierzu ausführlich oben unter Kap. 4, B.I.b)). Grund hierfür könnte etwa sein, dass das BVerfG für die Bewertung der Grundrechtsintensität wechselseitig auf die jeweiligen Maßstäbe der Bewertung der Grundrechtsintensität bei Eingriffen in Art. 10, Art. 13 GG und das RiS nimmt, vgl. *Buermeyer,* Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug, S. 165f. Hieraus lässt sich aber der Rückschluss ziehen, dass die Grundrechtsintensität jedenfalls verringert ist, wenn kein unmittelbarer Personenbezug besteht.

1653 BVerfGE 128, 1 (53).

1654 BVerfGE 109, 279 (313).

diesem Kernbereich privater Lebensgestaltung „gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen."[1655]

Bei der Bewertung der Persönlichkeitsrelevanz der erfassten Information ist außerdem nicht nur die jeweilige Einzelinformation maßgeblich, sondern auch welche Informationen durch eine weitergehende Verarbeitung und Verknüpfung gewonnen werden können und sollen.[1656] Denn je nach Verarbeitungs- und Verknüpfungsmöglichkeit durch Informationstechnologie können auch belanglose Daten einen neuen Stellenwert bekommen.[1657] So können insbesondere etwa auch lediglich technische Nebenprodukte, wie die Verbindungsdaten von Telekommunikation gerade in ihrer Verknüpfung eine besondere Persönlichkeitsrelevanz haben, da sie Rückschlüsse auf das soziale Umfeld des Betroffenen und die jeweiligen Kontakte zulassen.[1658]

In diesem Zusammenhang ist daher auch zu berücksichtigen, dass sich die Vielzahl der erhebbaren Daten intensitätssteigernd auswirkt,[1659] denn je umfangreicher die erhobenen bzw. erhebbaren Daten sind, desto mehr und genauere Informationen können auch durch ihre Verknüpfung erlangt werden.

b) Anlass und Umstände der Erhebung

Im Zusammenhang mit der Vielzahl der erhebbaren und erhobenen Daten ist außerdem relevant, ob und welcher Anlass für die Datenerhebung bestanden hat und unter welchen Umständen die Datenerhebung erfolgt ist.

So soll sich zunächst insbesondere die Streubreite der jeweiligen Maßnahme erheblich intensitätssteigernd auswirken. Insoweit soll für die Intensitätssteigerung maßgeblich sein, ob der Betroffene einen Anlass für die Erhebung der Daten gegeben hat „oder ob sie anlasslos erfolgt und damit

1655 BVerfGE 109, 279 (313).
1656 BVerfGE 65, 1 (45f.); BVerfGE 107, 299 (320); BVerfGE 115, 320 (348).
1657 BVerfGE 65, 1 (45).
1658 BVerfGE 107, 299 (319f.).
1659 BVerfGE 113, 348 (365).

praktisch jeden treffen kann."[1660] Dies ist insbesondere dann intensitätserhöhend, wenn eine Vielzahl der Daten verfahrensunerheblich ist.[1661]

Dabei ist außerdem maßgeblich für die Intensität, ob und welche Nachteile dem Betroffenen durch die Maßnahme drohen und ob diese nicht ohne Grund befürchtet werden.[1662] Dementsprechend ist allerdings auch intensitätsverringernd, wenn die Betroffenen selbst einen Anlass dafür gegeben haben, von der jeweiligen Maßnahmen betroffen zu sein.[1663]

Hintergrund dieser hohen Intensität ist, dass Einschüchterungseffekte entstehen können, wenn eine große Anzahl Personen, die keinen Erhebungsanlass gegeben haben, von der Maßnahmen betroffen sind.[1664] Denn Sinn und Zweck des RiS ist es auch der Schutz der allgemeinen Verhaltensfreiheit des Einzelnen, die auch dann eingeschränkt sein kann, wenn der Einzelne nicht weiß, welche Informationen über ihn erhoben werden und er insoweit die Entscheidungen über sein Handeln möglicherweise anpasst und damit nicht mehr frei treffen kann.[1665]

Insoweit ist insgesamt relevant, welcher Personenkreis von der Maßnahme betroffen ist.[1666]

Darüber hinaus ist für die Grundrechtsintensität außerdem relevant unter welchen Umständen die Datenerhebung stattfindet.[1667]

Intensitätserhöhend wirkt sich dabei insbesondere die Heimlichkeit der Erhebung aus.[1668] Denn einerseits befindet sich der Betroffene in einer vermeintlich vertraulichen Situation, wenn die Datenerhebung heimlich stattfindet.[1669] Andererseits kann er die Maßnahme auf Grund der fehlenden Kenntnis nicht selbst beeinflussen und kann sich allenfalls nach dem Abschluss der Maßnahme und damit erst, wenn der Eingriff bereits vollzogen ist, rechtlich gegen die Maßnahme wehren.[1670]

1660 BVerfGE 120, 378 (402) mit Verweis auf BVerfGE 100, 313 (376, 392); BVerfGE 107, 299 (320f.); BVerfGE 109, 279 (353); BVerfGE 113, 29 (53); BVerfGE 113, 348 (383); BVerfGE 115, 320 (354).

1661 BVerfGE 113, 29 (53) zur Beschlagnahme von Datenträgern einer Anwaltskanzlei.

1662 BVerfGE 100, 313 (376).

1663 BVerfGE 128, 1 (53).

1664 BVerfGE 120, 378 (402) mit Verweis auf BVerfGE 65, 1 (42); BVerfGE 113, 29 (46).

1665 BVerfGE 65, 1 (43). Siehe hierzu bereits im Einzelnen oben unter Kap. 4, B.II.1.a).

1666 BVerfGE 120, 378 (Ls. 2). Siehe hierzu auch die eingängliche Formulierung unter Kap. 5, C.II.2.b)

1667 BVerfGE 120, 378 (Ls. 2).

1668 BVerfGE 107, 299 (321); BVerfGE 115, 166 (194); BVerfGE 115, 320 (353).

1669 BVerfGE 107, 299 (321) mit Verweis auf BVerfGE 34, 238 (247).

1670 BVerfGE 107, 299 (321).

Darüber hinaus wirkt sich besonders intensitätssteigernd aus, wenn bei der Datenerhebung Vertraulichkeitserwartungen verletzt werden, die einen besonderen grundrechtlichen Schutz genießen.[1671]

(1) Intensitätsverringerung bei öffentlich verfügbaren Daten?

Intensitätsverringernd könnte sich dagegen der Umstand auswirken, wenn Daten erhoben werden, die allgemein zugänglich bzw. öffentlich verfügbar[1672] sind. Zu einer Intensitätsverringerung wegen der allgemeinen Zugänglichkeit von personenbezogenen Informationen hat sich das BVerfG etwa in seinen Entscheidungen zu automatisierten Kfz-Kennzeichenerfassungen[1673] geäußert. Das BVerfG stellte im Rahmen der Bewertung der Grundrechtsintensität zwar fest, dass die automatisierten Kfz-Kennzeichenkontrollen insgesamt einen Eingriff „von erheblichem Gewicht"[1674] darstellten. Allerdings sei der Bewertung des „Eingriffsgewicht[s] mindernd einzustellen, dass die Kennzeichenkontrolle im öffentlichen Verkehrsraum stattfinde[…]. Sowohl die Kraftfahrzeugkennzeichen als auch das erfasste Bewegungsverhalten [sei] ohne weiteres für alle erkennbar."[1675]

Fraglich ist, ob dies auch für die Erhebung von öffentlich zugänglichen Daten im Internet gelten kann.

Gegen eine derartige Anwendbarkeit ließe sich nämlich anführen, dass das BVerfG in seiner Entscheidung zum VSG NRW[1676] eindeutig die Grenze eines Eingriffs für die Erhebung öffentlich verfügbarer Daten festgelegt

1671 BVerfGE 109, 279 (313f., 325, 327f.); BVerfGE 113, 348 (364f., 383, 392); BVerfGE 115, 320 (348); BVerfGE 130, 1 (36). Abweichend von BVerfGE 115, 320 (348) vertritt Richterin *Haas* in ihrem Sondervotum zum Beschluss des Ersten Senats vom 04. April 2006 – 1 BvR 518/02 –, dass bei heimlichen Maßnahmen die Intensitätssteigerung der Streubreite von Maßnahmen im Widerspruch zur intensitätssteigernden Heimlichkeit der Maßnahme stünden. Denn es sei widersprüchlich, dass einerseits ein Einschüchterungseffekt intensitätssteigernd sei und andererseits die Heimlichkeit und damit die Unkenntnis des Betroffenen von der konkreten Maßnahme intensitätssteigernd sei, vgl. BVerfGE 115, 320 (372).

1672 Siehe zur Begriffsbestimmung öffentlich verfügbarer Daten bereits oben unter Kap. 4, B.II.1.d)

1673 BVerfGE 120, 378 (404) BVerfGE 150, 244ff.; siehe hierzu im Einzelnen bereits oben unter Kap. 4, B.II.2.b)iii., iv.

1674 BVerfGE 150, 244 (283).

1675 BVerfGE 150, 244 (283); vgl. BVerfGE 120, 378 (404).

1676 BVerfGE 120, 274ff; siehe hierzu bereits im Einzelnen oben unter Kap. 4, B.II.2.b)(1)i.

hat. Diese Grenze ist überschritten, wenn Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt."[1677] Wenn insoweit die Grenze des Eingriffs bei einer bestimmten Form der Erhebung (vereinfacht: dem gezielten Zusammentragen der Daten) überschritten ist, könnte man annehmen, dass hierin schon ein Umstand der Erhebung vorliegt. Wenn aber dieser bestimmte Umstand der Erhebung gerade die Grenze zum Vorliegen eines Eingriffs darstellt, wirkt es auf den ersten Blick widersprüchlich, gerade diesen Umstand dann wiederum als intensitätsverringernd zu berücksichtigen. Allerdings muss hierbei beachtet werden, dass hier bei der Festlegung der Grenze eines Eingriffs auf eine bestimmte Form des Zugriffs auf öffentlich verfügbare Daten und damit auf die Art und Weise der Erhebung – nämlich das gezielte Zusammentragen – abgestellt wird. Dagegen ist die öffentliche Verfügbarkeit ein Umstand der Daten selbst und deren Erhebbarkeit. Es ist daher nicht widersprüchlich, einerseits die Grenze eines Eingriffs von der Art und Weise der Erhebung abhängig zu machen und andererseits eine Intensitätsverringerung grundsätzlich auf Grund einer einfachen Erhebbarkeit und damit auf Grund der einfachen Verfügbarkeit von Daten anzunehmen. Hierzu passt etwa auch, dass das BVerfG in einer Entscheidung zum Gentechnikgesetz[1678] angibt, es wirke sich mildernd auf den Eingriff aus, wenn „der mit der Datenerhebung verbundene Aufwand verhältnismäßig gering"[1679] sei.

Allerdings ließe sich gegen eine Intensitätsverringerung von öffentlich verfügbaren Daten anführen, dass das BVerfG insbesondere in seiner grundlegenden Entscheidung zum RiS – dem Volkszählungsurteil[1680] – bestimmt hat, dass es im Rahmen des RiS gerade kein ‚belangloses' Datum mehr"[1681] gebe. Hieraus ließe sich wiederum auf den ersten Blick ein Widerspruch zur Intensitätsverringerung bei öffentlich verfügbaren Daten

1677 BVerfGE 120, 274 (345); siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.

1678 BVerfGE 128, 1 ff.; vgl. hierzu bereits oben unter Kap. 4, B.II.1.b)(1).

1679 BVerfGE 128, 1 (53). Allerdings stellt das BVerfG hier vorrangig darauf ab, dass es für denjenigen, der Angaben gegenüber der zuständigen Behörde abgeben muss, ein verhältnismäßig geringer Aufwand ist, diese Angaben zu machen. Dies ändert aber nichts daran, dass das BVerfG in diesem Zusammenhang insgesamt auf einen geringen Aufwand der Datenerhebung abstellt.

1680 BVerfGE 65, 1 ff.

1681 BVerfGE 65, 1 (45).

ableiten, da insoweit entgegen der grundlegenden Feststellung des BVerfG bei bestimmten Daten eine Abstufung vorgenommen werden würde. Dem steht allerdings entgegen, dass das BVerfG bei seiner Feststellung, dass es im Rahmen des RiS keine belanglosen Daten gebe, „auf die Art der Angaben [abstellt]“[1682]. Die öffentliche Verfügbarkeit von Daten ist dementgegen keine Art der Daten, sondern wiederum nur ein Umstand der Erhebbarkeit der Daten. Dass die Daten öffentlich verfügbar sind, hat keinerlei Auswirkung auf die Frage, welcher Art die Daten sind und welchen Inhalt sie haben.

Schließlich spricht für eine verringerte Intensität bei öffentlicher Verfügbarkeit ein umgekehrter Gleichlauf mit der besonderen Intensitätssteigerung, die dann vorliegt, wenn Daten erhoben werden, bei deren Erhebung grundrechtlich geschützte Vertraulichkeitserwartungen verletzt werden. Denn umgekehrt bestehen bei öffentlich verfügbaren Daten gerade keine Vertraulichkeitserwartungen, da der Betroffene hierbei nicht davon ausgehen kann, dass diese Daten nicht von Dritten zur Kenntnis genommen werden können.[1683] Problematisch hieran ist jedoch, dass das BVerfG bestimmt, „die Eingriffsintensität [sei] hoch, wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG“[1684]. Aus dem ersten Halbsatz dieser Bestimmung lässt sich daher grundsätzlich ableiten, dass die Eingriffsintensität insgesamt bei der Verletzung von Vertraulichkeitserwartungen hoch sei. Der zweite Halbsatz lässt dagegen den Rückschluss zu, dass sich die Verletzung von Vertraulichkeitserwartungen in besonderem Maße intensitätserhöhend auswirkt, wenn die Vertraulichkeitserwartungen auf einem grundrechtlichen Schutz beruhen. Problematisch ist daher die Frage, wie öffentlich verfügbare Daten in diesen Kontext einzuordnen sind. Denn bei öffentlich verfügbaren Daten können keine derartigen Vertraulichkeitserwartungen bestehen.[1685] Allerdings bestimmt das BVerfG in seiner Entscheidung zur polizeilichen Rasterfahndung[1686], dass sich bereits Vertraulichkeitserwartungen intensitätserhöhend auswir-

1682 BVerfGE 65, 1 (45).
1683 Vgl. BVerfGE 120, 351 (361).
1684 BVerfGE 115, 320 (348) mit Verweis auf BVerfGE 109, 279 (313f., 325, 327f.); BVerfGE 113, 348 (364f., 383, 391).
1685 Vgl. BVerfGE 120, 351 (361).
1686 BVerfGE 115, 320 ff.

ken – unabhängig davon, ob diese auf einem grundrechtlichen Schutz beruhen. Vertraulichkeitserwartungen, die nicht auf einem grundrechtlichen Schutz beruhen können etwa berufliche Schweigepflichten sein. Dies lässt insoweit den Rückschluss zu, dass der Ausgangspunkt des Schutzniveaus in diesem Zusammenhang bei Daten liegt, bei denen keinerlei Vertraulichkeitserwartungen bestehen. Das könnte insoweit bedeuten, dass das grundlegende Schutzniveau des RiS bereits bei öffentlich verfügbaren Daten besteht, sodass sich die öffentliche Verfügbarkeit nicht intensitätsverringernd auswirken kann.

In diesem Zusammenhang könnte jedoch zu berücksichtigen sein, dass das Nichtbestehen von Vertraulichkeitserwartungen nicht unbedingt mit der öffentlichen Verfügbarkeit von Daten gleichzusetzen ist. Denn, soweit der Betroffene Kenntnis von der öffentlichen Verfügbarkeit der Daten hat, muss er sich darüber bewusst sein, dass diese ungehindert von jedem Dritten zur Kenntnis genommen werden können. Dagegen ist die Stoßrichtung beim Nichtbestehen von Vertraulichkeitserwartungen eine andere. Denn der Betroffene muss nicht wie bei öffentlich verfügbaren Daten positiv davon ausgehen, dass jeder Dritte die Daten zur Kenntnis nehmen kann, sondern kann nur negativ nicht darauf vertrauen, dass diese nicht vertraulich sind, sondern möglicherweise auch von Dritten zur Kenntnis genommen werden können.

Insoweit lässt sich darauf abstellen, dass das grundlegende Schutzniveau bei Daten vorliegt, bei deren Erhebung keine Vertraulichkeitserwartungen bestehen. Erhöht ist die Intensität dagegen, wenn Vertraulichkeitserwartungen verletzt werden. Verringert ist die Intensität dagegen, wenn die erhobenen Daten öffentlich verfügbar sind.

(2) Zwischenergebnis

Insoweit lässt sich die Rechtsprechung des BVerfG insgesamt dahingehend verstehen, dass es sich intensitätsverringernd auswirkt, wenn die erhobenen Daten öffentlich verfügbar sind.

c) Art der Verwertung der erhobenen Daten

Auf die Intensität des Grundrechtseingriffs wirkt sich außerdem die Art und Weise der Verwertung der Daten aus.[1687] Dabei ist zunächst zu berücksichtigen, dass das RiS zwar vor dem Hintergrund der Gefahren von informationstechnologischen Datenverarbeitungen entwickelt wurde[1688], sein Schutz aber nicht hierauf beschränkt ist.[1689] So schützt das RiS „generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten"[1690]. Dementsprechend können sich bestimmte Arten der Verwendungs- und Verarbeitungsmöglichkeiten intensitätssteigernd auswirken.[1691]

So ist die Intensität erhöht, wenn mit der Nutzung die Möglichkeit besteht, dass die Informationen für Folgeeingriffe genutzt werden, sowie, wenn die erhobenen Daten auch zu anderen Zwecken genutzt werden können.[1692]

Außerdem wirkt sich bei der elektronischen Datenverarbeitung auch die Menge der erheb- und verwertbaren Daten auf die Intensität aus, sodass etwa bei einer großen Menge an erheb- und verwertbaren Daten eine erhöhte Intensität vorliegt.[1693]

So kommt dem Grundrechtseingriff auch dann erhebliches Gewicht zu, wenn zwar die Einzelinformationen in ihrer Intensität hinter der Intensität der Schutzbereiche der Art. 10, Art. 13 GG zurückbleiben, sich aber durch ihre Zusammenführung und Verknüpfungsmöglichkeiten vielfältige neue Informationen ergeben können, die nach Art und Inhalt eine besonders starke Persönlichkeitsrelevanz haben können.[1694] Denn aus der „Zusammenführung und Kombination […] der […] Datenbestände und ihrem wechselseitigen Abgleich"[1695] lassen sich vielfältige neue Informationen ge-

1687 BVerfGE 120, 378 (Ls. 2).
1688 BVerfGE 65, 1 (41f.); vgl. Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Rn. 176.
1689 BVerfGE 78, 77 (84).
1690 BVerfGE 78, 77 (84).
1691 Vgl. BVerfGE 120, 378 (Ls. 2).
1692 BVerfGE 113, 348 (365).
1693 So insbesondere BVerfGE 113, 348 (365), wonach „[d]ie Vielzahl der im Rahmen der modernen Telekommunikation erfassbaren Daten […] zu einer besonderen Intensität" führt. Vgl. BVerfGE 65, 1 (42, 45); BVerfGE 113, 29 (45f.); BVerfGE 115, 320 (348), wonach etwa der Abgleich mehrerer Datensätze miteinander intensitätserhöhend wirkt.
1694 BVerfGE 115, 320 (347f.) mit Verweis auf BVerfGE 100, 313 (376); BVerfGE 107, 299 (319f.); BVerfGE 109, 279 (353).
1695 BVerfGE 115, 320 (349).

winnen, die ebenfalls eine besondere Persönlichkeitsrelevanz haben können.[1696] Da das RiS aber gerade einen umfassenden Schutz der Privatheit und Verhaltensfreiheit ermöglichen soll, müssen insoweit im Rahmen der Intensität des Grundrechtseingriffs auch die Verarbeitungs- und Verknüpfungsmöglichkeiten von Datenberücksichtigt werden.[1697]

Zu berücksichtigen ist allerdings darüber hinaus, dass sich der besondere Schutzgehalt bei bestimmten Datenerhebungsmaßnahmen – etwa solche, die in den Schutzbereich der Art. 13, Art. 10 GG fallen – auch auf die sich daran anschließenden Datenverarbeitungsmaßnahmen erstrecken.[1698]

Dementsprechend müsste es sich umgekehrt allerdings auch intensitätsverringernd auswirken, wenn die Intensität der Datenerhebungsmaßnahme dadurch verringert ist, dass öffentlich verfügbare Daten erhoben werden.[1699]

Ferner müssen beim Einsatz von modernen Ermittlungsmethoden[1700] auch die Gefährdungen durch sog. additive Grundrechtseingriffe beachtet werden.[1701] Insoweit ergibt sich auch eine Intensitätssteigerung durch das Zusammenwirken verschiedener Überwachungsmaßnahmen.[1702]

d) Zwischenergebnis

Aus diesen Kriterien der Rechtsprechung lassen sich insoweit zwei maßgebliche, sozusagen übergeordnete Kriterien zur Bewertung der Grundrechtsintensität ableiten[1703]: einerseits die Persönlichkeitsrelevanz der jeweiligen Informationen und andererseits die Gefährdung der freien Entfaltung der Persönlichkeit insbesondere mit Blick auf die Verhaltensfreiheit[1704] – sowohl auf individueller als auch auf gesellschaftlicher Ebene.

1696 BVerfGE 115, 320 (349); BVerfG BeckRS 2020, 34607 (Rn. 110).
1697 Vgl. BVerfGE 65, 1 (44); BVerfGE 115, 320 (349).
1698 BVerfGE 109, 279 (325f.); BVerfGE 113, 348 (365). Vgl. zu den intensitätssteigernden Umständen von Datenerhebungen bereits soeben unter Kap. 5, C.II.2.b)(2).
1699 Siehe hierzu bereits soeben unter Kap. 5, C.II.2.b)(2)i.
1700 Insbesondere, wenn diese dem Betroffenen verborgen bleiben.
1701 BVerfGE 112, 304 (Ls. 2; 319f.); BVerfGE 141, 220 (280).
1702 BVerfGE 141, 220 (280) mit Verweis auf BVerfGE 112, 304 (319f.); vgl. hierzu bereits BVerfGE 112, 304 (319f.).
1703 Diese sind allerdings wiederum nicht trennscharf voneinander abzugrenzen, sondern bedingen sich wiederum gegenseitig.
1704 Vgl. insoweit die Begründung des Grundrechts auf informationelle Selbstbestimmung BVerfGE 65, 1 (43), wonach es sich insbesondere auch auf die Verhaltens-

So ist für die Grundrechtsintensität zunächst die Persönlichkeitsrelevanz der jeweiligen Einzelinformationen relevant. Dabei ist darüber hinaus aber auch die Persönlichkeitsrelevanz der Informationen, die sich aus der Verknüpfung der Einzelinformationen ergeben können, relevant. Insoweit ist etwa auch die Menge der erhobenen und erhebbaren Daten relevant, sowie die technischen Möglichkeiten der Verknüpfung.

Sowohl im Zusammenhang mit der Persönlichkeitsrelevanz der Informationen als auch mit der Gefährdung der Persönlichkeitsentfaltung und Verhaltensfreiheit sind Anlass und Umstände der Erhebung zu berücksichtigen. Dabei wirken sich insbesondere anlasslose, heimliche und solche Datenerhebungen, bei denen (grundrechtlich) geschützte Vertraulichkeitserwartungen verletzt werden, intensitätssteigernd aus. Intensitätsverringernd wirkt es sich dagegen aus, wenn öffentlich verfügbare Daten erhoben werden. Dabei schlägt sich diese Intensitätssteigerung und -verringerung auch auf die anschließende Datenverarbeitung durch. Zu berücksichtigen sind dabei außerdem, die Gefahren, die für die Persönlichkeitsentfaltung durch mehrere miteinander verbundene Grundrechtseingriffe entstehen, die zu einem Gefühl dauerhafter Überwachung führen können.

3. Bewertung der Grundrechtsintensität der hier gegenständlichen Maßnahmen

Nach den vorstehend herausgearbeiteten Kriterien zur Bewertung der Grundrechtsintensität stellt sich nun die Frage, wie die Grundrechtsintensität der hier gegenständlichen Auswertungsmethoden anhand dieser Kriterien zu bewerten ist.

a) Entitätsclustering

Beim sog. *Entitäts-Clustering* ist das Ziel, mehrere *Bitcoin-Adressen* einer einzelnen *Entität* zuzuordnen – sie insoweit zu gruppieren.[1705] Hierzu werden die in der jeweiligen Blockchain enthaltenen Daten systematisch dahingehend analysiert, ob und welche *Bitcoin-Adressen* bei mehreren

weisen des Einzelnen auswirkt, wenn er nicht weiß, welche Daten und Informationen über ihn verfügbar sind.

1705 Siehe hierzu bereits oben unter Kap. 3, A.I.

Transaktionen in unterschiedlichen Kombinationen genutzt werden.[1706] Datengrundlage dieser Auswertungsmethode sind damit die unmittelbaren Blockchain-Daten.[1707]

Technisch und in der Ermittlungspraxis dürften hierbei zwei unterschiedliche Einsatzmöglichkeiten bestehen, die wohl auch eine unterschiedliche Grundrechtsintensität nach sich ziehen: einerseits lässt sich das *Entitäts-Clustering* auf die gesamten Blockchain-Daten anwenden, um so alle dort genutzten und vorhandenen *Bitcoin-Adressen* insgesamt zu *Entitäten* zuzuordnen.[1708] Andererseits wäre es technisch wohl auch möglich, die gesamten Blockchain-Daten nur nach den *Bitcoin-Adressen* einer einzelnen[1709] *Entität* zu durchsuchen.

Nachfolgend wird zunächst auf die Grundrechtsintensität eingegangen, die beiden Einsatzmöglichkeiten gemeinsam ist (hierzu unter (1)), um im Anschluss auf die Unterschiede der Grundrechtsintensität bei diesen Einsatzmöglichkeiten einzugehen (hierzu unter (2)) und abschließend die Grundrechtsintensität des *Entitäts-Clusterings* bewerten zu können (hierzu unter (3)).

(1) Grundrechtsintensität, die bei beiden Einsatzmöglichkeiten vorliegt

Intensitätssteigernd wirkt sich jedenfalls der Umfang der erhobenen Daten in Form der Blockchain-Daten aus. Denn die Blockchain-Daten enthalten umfassend die Transaktionsdaten einer jeweiligen Kryptowährung. Die Erhebung geht insoweit weit über die Erhebung von lediglich einzelnen Informationen hinaus. Es ist außerdem nicht möglich, die Erhebung und Auswertung auf einzelne Daten der Blockchain zu beschränken. Denn einerseits dürfte dies rein technisch schon Schwierigkeiten aufwerfen, da beim Verwenden eines jeweiligen *full-clients* in der Regel die gesamten Blockchain-Daten heruntergeladen werden. Andererseits könnte ohne die gesamten Blockchain-Daten auch nicht die Funktionsfähigkeit der Auswer-

1706 Siehe hierzu im Einzelnen und zu den verschiedenen Möglichkeiten des *Entitäts-Clusterings* ausführlich oben unter Kap. 3, A.I.

1707 Siehe hierzu bereits oben unter Kap. 3, A.I.

1708 Siehe zur Frage, ob in diesem Anwendungsfall überhaupt ein ausreichender Anfangsverdacht vorliegt, bereits oben unter Kap. 5, D.I.2. Hier muss insoweit für die Bewertung der Grundrechtsintensität unterstellt werden, dass ein ausreichender Anfangsverdacht besteht.

1709 Oder auch mehreren, bestimmten.

tungsmethode gewährleistet werden. Denn eine gesamte *Entität* kann ja gerade nur dadurch zuverlässig, wirksam und vor allem umfassend ermittelt werden, dass die gesamten Blockchain-Daten nach entsprechenden Transaktionsdaten durchsucht werden, die im Zusammenhang mit einer oder mehreren, bestimmten *Bitcoin-Adressen* stehen.[1710] Wenn nur Teile der Transaktionsdaten erhoben und ausgewertet würden, könnten eben nicht alle *Bitcoin-Adressen* einer entsprechenden *Entität* zugeordnet werden.

Zu berücksichtigen ist jedoch zunächst, dass nach der hier vertretenen Auffassung die bloße Erhebung der Blockchain-Daten noch keinen Eingriff in das RiS darstellt, sondern ein Grundrechtseingriff erst bei dem systematischen Datenabgleich der Blockchain-Daten vorliegt.[1711] Da aber auch der Datenabgleich, durch den ein Eingriff in das RiS vorliegt[1712], die gesamten Blockchain-Daten zum Gegenstand hat, wirkt sich jedenfalls in dieser Hinsicht der Umfang der Daten hier intensitätssteigernd aus.

In Bezug auf die Datengrundlage des Abgleichs könnte jedoch intensitätsverringernd zu berücksichtigen sein, dass beim *Entitäts-Clusterings* nur ein einzelner Datenbestand – die Transaktionsdaten der jeweiligen Blockchain – ausgewertet wird und nicht mehrerer Datenbestände miteinander abgeglichen werden.[1713] Nach hier vertretener Auffassung kommt es für die Persönlichkeitsrelevanz und der Gefahr, dass umfassende Persönlichkeitsbilder erstellt werden, jedoch nicht darauf an, ob mehrere verschiedene Datenbestände miteinander zum Abgleich gebracht werden, sondern auf die möglichen Inhalte, die sich aus der Auswertung des jeweiligen Datenbestandes ergeben können.[1714] Da auch nach der Rechtsprechung des BVerfG aus Kontoinformationen erhebliche Rückschlüsse auf das jeweilige Sozialverhalten der Betroffenen abgeleitet werden können[1715], kann daher hier nicht von einer verringerten Grundrechtsintensität ausgegangen werden, nur weil lediglich die Blockchain-Daten ausgewertet werden. Insoweit wirkt es sich nicht intensitätsverringernd aus, dass beim *Entitäts-Clustering* lediglich die jeweiligen Blockchain-Daten ausgewertet werden.

1710 Siehe zur Funktionsweise der *Entitäts-Clustering*-Verfahren im Einzelnen oben unter Kap. 3, A.I.
1711 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c).
1712 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c).
1713 Vgl. insoweit zur geringeren Grundrechtsintensität bei der Abfrage von nur einer einzelnen Datenquelle BVerfG NJW 2009, 1405 (1407).
1714 Siehe hierzu ausführlich oben unter Kap. 5, B.II.3.
1715 BVerfGE 118, 168 (185f.).

Intensitätsverringernd ist mit Blick auf die Art und den Inhalt der Informationen allerdings zu berücksichtigen, dass die Blockchain-Daten selbst keinen unmittelbaren Rückschluss auf die hinter den *Bitcoin-Adressen* stehenden Personen zulassen.[1716] Zwar dürfte die Ermittlung der jeweiligen Identitäten gerade auch eines der Ziele der Ermittlungsbehörden sein, die Daten selbst sind aber zunächst jedenfalls pseudonymisiert[1717], sodass die Grundrechtsintensität daher verringert ist.

Mit Blick auf die Art und Weise der Anwendung des *Entitäts-Clusterings* ist dagegen intensitätssteigernd zu berücksichtigen, dass das *Entitäts-Clustering* heimlich – also ohne Kenntnis der Betroffenen – stattfindet. Dabei ist insbesondere zu berücksichtigen, dass es auf Grund der vorwiegenden Pseudonymität der Blockchain-Daten nach Abschluss der Auswertung in der Regel überhaupt nicht möglich ist, die von der Auswertung betroffenen Personen hierüber zu informieren, sodass die betroffenen Personen die Rechtmäßigkeit der Maßnahme gerichtlich überprüfen lassen könnten. Dies ist insoweit intensitätssteigernd zu berücksichtigen, als dass der Schutz des RiS gerade auch vor dem Hintergrund der Gefährdung der Persönlichkeitsentfaltung und der Verhaltensfreiheit besteht, die dadurch entstehen können, dass der Einzelne nicht weiß, wer wann was über ihn weiß.[1718] Insoweit kann auf Grund der Heimlichkeit der hier gegenständlichen Auswertungsmethode ein diffuses Überwachungsgefühl bei den einzelnen Nutzern von Blockchain-Technologien entstehen, das insbesondere auch zu einer Verhaltensanpassung führen kann.[1719]

In diesem Zusammenhang ist jedoch wesentlich intensitätsverringernd zu berücksichtigen, dass die ausgewerteten Daten öffentlich verfügbar sind und insoweit die Betroffenen davon ausgehen konnten und wohl auch mussten, dass die Daten von Dritten zur Kenntnis genommen werden. Technisch ist die dezentrale Verwaltung durch die Blockchain-Technologien ja gerade darauf angelegt, dass andere Nutzer die jeweiligen Transaktionen zur Kenntnis nehmen und sie auf Richtigkeit überprüfen und anschlie-

1716 Siehe hierzu bereits ausführlich oben unter Kap. 2, A.II.2. und Kap. 4, B.II.1.c).

1717 So *Finck*, Blockchain and the GDPR, S. 26f. Die in der Blockchain enthaltenen Daten sind pseudonym, da es grundsätzlich durch Zusatzwissen möglich ist, einen Personenbezug herzustellen, *Spindler/Bille,* WM 2014, 1357 (1359); vgl. *Boehm/Pesch*, MMR 2014, 75 (75f.); *Kaulartz,* CR 2016, 474 (480);

1718 BVerfGE 65, 1 (43).

1719 Siehe hierzu insbesondere die bereits entwickelten Möglichkeiten sog. *Mixing-Services,* hierzu bereits ausführlich oben unter Kap. 3, A.I.4.

ßend bestätigen.[1720] Insoweit kann auch kein Vertrauen darauf bestehen, dass staatliche Stellen die jeweiligen Daten nicht zur Kenntnis nehmen.[1721]

Intensitätssteigernd zu berücksichtigen ist dagegen, dass die Auswertung technikgestützt stattfindet und daher weit mehr Verarbeitungs- und Verknüpfungsmöglichkeiten bestehen als bei einer händischen Auswertung. Zwar ließe sich anführen, dass die technische Unterstützung, die bei den *Clustering*-Verfahren eingesetzt wird, grundsätzlich keine umfangreichen Verknüpfungen ermöglichen, sondern weitgehend nur eine erweiterte Suchfunktion darstellt. Denn das *Entitäts-Clustering* beschränkt sich in seiner technischen Umsetzung grundsätzlich darauf, dass die gesamten Blockchain-Transaktionsdaten nach Transaktionen durchsucht werden, bei denen die *Bitcoin-Adresse,* deren *Entität* gesucht wird, ebenfalls genutzt wurde, um zu ermitteln, ob und in welchem Zusammenhang diese *Bitcoin-Adresse* mit anderen *Bitcoin-Adressen* verwendet wurde. Dementsprechend stellt das *Entitäts-Clustering* in seiner Grundfunktion nur eine Suchfunktion nach bestimmten Inhalten dar. Allerdings muss berücksichtigt werden, dass ein derartig umfangreicher Datensatz wie etwa die Bitcoin-Blockchain wohl händisch gar nicht hiernach durchsucht werden könnte. So waren etwa in der Bitcoin-Blockchain am 20. Dezember 2021 mehr als 696 Millionen Transaktionen enthalten.[1722] Diese Transaktionen händisch nach der Verwendung von einer bestimmten *Bitcoin-Adresse* zu durchsuchen dürfte praktisch fast unmöglich sein. Außerdem kann durch ein *Clustering* Verfahren automatisch nicht nur nach Transaktionen einer bestimmten, einzelnen *Bitcoin-Adresse* gesucht werden, sondern darüber hinaus können, wenn bereits eine weitere *Bitcoin-Adresse* einer *Entität* zugeordnet wurde, die Transaktionsdaten der Blockchain nach dieser weiteren *Bitcoin-Adresse* automatisch auch durchsucht werden. Insoweit ist das *Entitäts-Clustering* zwar eines der einfachsten technischen Auswertungsmöglichkeiten, die hier betrachtet werden, im Vergleich zu einer händischen Auswertung, sind die Verknüpfungs- und Verarbeitungsmöglichkeiten durch das *Entitäts-Clustering* jedoch weit erhöht, sodass hiermit auch eine entsprechende Intensitätssteigerung einhergeht.

1720 Siehe zur technischen Funktionsweise des Überprüfungsmechanismus in Blockchain-Systemen bereits ausführlich oben unter Kap. 2, A.II.7.c), III.1.c).

1721 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).

1722 https://www.blockchain.com/charts/n-transactions-total (letzter Abruf: 20. Dezember 2021).

(2) Unterschiedliche Grundrechtsintensität

Unterschiedlich ist die Grundrechtsintensität beider Einsatzmöglichkeiten dagegen hinsichtlich der Streubreite und der damit verbundenen Anlasslosigkeit von Grundrechtseingriffen zu bewerten.

So liegt eine erhebliche Streubreite vor, wenn alle *Bitcoin-Adressen,* die in der Blockchain insgesamt vorkommen, zu *Entitäten geclustert* werden. Denn hiervon sind insoweit alle Nutzer der jeweiligen Blockchain betroffen, unabhängig davon, ob sie einen Anlass dafür gegeben haben, der über das bloße Nutzen einer Blockchain hinausgeht. Mit einer derartigen Anwendung des *Entitäts-Clusterings* ginge daher auch eine erhebliche Gefahr mit einher, dass die Nutzer von Blockchains ihr Verhalten entsprechend anpassen.

Dass die Nutzer ihr Transaktionsverhalten bereits entsprechend angepasst haben, zeigt sich bereits daran, dass es mittlerweile die bereits erwähnten *Mixing-Services* gibt, die eingesetzt werden, um ein *Entitäts-Clustering* jedenfalls zu erschweren.[1723]

Insoweit liegt eine erhebliche Intensitätssteigerung vor, wenn die *Entitäts-Clustering*-Verfahren eingesetzt werden, um alle *Bitcoin-Adressen* einer Blockchain zu *Entitäten* zu *clustern.*

Nicht so eindeutig kann dagegen die Frage beantwortet werden, wie die Grundrechtsintensität zu bewerten ist, wenn nur die *Entitäten* bestimmter *Bitcoin-Adressen,* bei denen etwa der Verdacht einer Straftat besteht, ermittelt werden. Problematisch ist nämlich, dass einerseits keine *Entitäts-Cluster* von unbeteiligten Dritten erstellt werden, andererseits stellt sich die Frage, ob nicht die anderen Nutzer, deren *Entitäten* zwar nicht ermittelt werden, deren Transaktionsdaten aber trotzdem abgeglichen werden müssen, um als sog. Nicht-Treffer auszuscheiden, trotzdem in ihren Grundrechten betroffen sind. Insoweit stellt sich hier die Frage, ob auch hier die als Nichttreffer ausgeschiedenen Personen bzw. Daten in ihren Grundrechten betroffen sind. Denn dann läge auch in diesem Anwendungsfall eine erhöhte Streubreite vor, da auch hier anlasslos in die Grundrechte Unbeteiligter eingegriffen werden würde.

1723 Siehe hierzu bereits ausführlich oben unter Kap. 3, A.I.4. Ob dies allerdings am staatlichen Einsatz derartiger *Entitäts-Clustering*-Verfahren oder etwa an einem entsprechenden privaten Einsatz liegt, ist unklar.

Zur Beantwortung dieser Frage muss nochmals die Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung[1724] herangezogen werden. Denn grundsätzlich liegt auch nach dieser neuen Rechtsprechung des BVerfG dann kein Grundrechtseingriff vor, wenn Daten lediglich technikbedingt miterhoben werden und im Anschluss unmittelbar und spurenlos wieder ausgeschieden werden.[1725] Allerdings hat das BVerfG seine Rechtsprechung mit seiner zweiten Entscheidung zur automatisierten Kfz-Kennzeichenkontrolle im Jahr 2018 dahingehend konkretisiert, dass dann kein lediglich technikbedingtes Miterheben vorliegt, wenn sich an den ausscheidenden Daten bereits ein spezifisches Interesse verdichtet hat.[1726] Das BVerfG hat für die automatisierte Kfz-Kennzeichenkontrolle mittlerweile festgestellt, dass hierbei auch ein derartiges spezifisches Interesse an den Nichttreffern bestünde, da die Maßnahme nur dann wirkungsvoll sei, wenn auch die Nichttreffer zunächst miterhoben würden, um so die Treffer zu ermitteln. Insoweit bestünde bei der automatisierten Kfz-Kennzeichenkontrolle ein spezifisches Interesse an den gesamten Daten, da nur so die Maßnahme wirksam sei, sodass auch bei den sog. Nichttreffern ein Grundrechtseingriff vorläge.[1727]

Insoweit stellt sich die Frage, ob und inwieweit die Grundsätze dieser Rechtsprechung bei dem hier gegenständlichen *Entitäts-Clustering,* das zwar nur in Bezug auf bestimmte, einzelne *Bitcoin-Adressen* eingesetzt wird, aber trotzdem die gesamte Blockchain-Daten nach Treffern und eben auch Nichttreffern durchsucht, Anwendung finden können. Sollte nach der Anwendung dieser Grundsätze auch hier ein Grundrechtseingriff für die Nichttreffer vorliegen, läge auch dann eine hohe Streubreite des *Entitäts-Clusterings* vor, wenn dieses nur eingesetzt würde, um die *Entitäten* einzelner *Bitcoin-Adressen* zu ermitteln. Daher stellt sich die Frage, ob hier in vergleichbarer Weise ein großer Datensatz lediglich mit dem Ziel, diesen zu verkleinern, erhoben wurde und insoweit auch ein spezifisches Interesse an den als Nichttreffer ausgeschiedenen Daten besteht.

Dies könnte auf den ersten Blick insoweit der Fall sein, da ja gerade die gesamten Blockchain-Daten nach Treffern einer oder mehrerer bestimmter *Bitcoin-Adressen* abgeglichen werden. Zwar dürfte es auch möglich sein,

1724 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.
1725 BVerfGE 100, 313 (366).
1726 BVerfGE 150, 244 (266). vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.
1727 BVerfGE 150, 244 (266); vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.

nur einzelne Teilbereiche der Blockchain-Daten nach entsprechenden Treffern zu durchsuchen – etwa die Transaktionsdaten des vergangenen Jahres – das Ziel des *Entitäts-Clusterings* dürfte es aber in der Regel sein, alle *Bitcoin-Adressen* zu ermitteln, die zu einer bestimmten *Entität* gehören. Dieses Ziel kann aber nur dann erreicht werden, wenn auch die gesamten Transaktionsdaten der jeweiligen Blockchain hiernach durchsucht und analysiert werden. Insoweit besteht grundsätzlich zunächst auch ein spezifisches Interesse an den gesamten Blockchain-Daten.

Allerdings muss berücksichtigt werden, dass – anders als bei der automatisierten Erhebung von Kfz-Kennzeichen – in der Erhebung der Blockchain-Daten noch kein Grundrechtseingriff vorliegt, da diese ohnehin öffentlich verfügbar sind.[1728] Insoweit liegt beim *Entitäts-Clustering* noch kein Eingriff dadurch vor, dass die Daten erhoben werden. Sondern der Eingriff liegt erst darin, dass die Daten systematisch ausgewertet werden.[1729] Insoweit liegt auch bei der Erhebung der Blockchain-Daten noch kein Grundrechtseingriff vor, selbst, wenn zum Zwecke des *Entitäts-Clusterings* ein spezifisches Interesse an dem gesamten Datensatz besteht. Dass die Erhebung der Blockchain-Daten selbst keinen Grundrechtseingriff darstellen, während die Erhebung der ebenfalls im öffentlichen Verkehrsraum verfügbaren Kfz-Kennzeichen bereits einen Eingriff darstellen, hat den technischen Hintergrund, dass für die Erhebung der Blockchain-Daten lediglich die Teilnahme an dem jeweiligen Blockchain-Netzwerk erforderlich ist und die gesamten Blockchain-Daten bereits als einheitlicher Datensatz vorhanden sind, wohingegen für die automatisierte Erfassung der Kfz-Kennzeichen zunächst entsprechende technische Anlagen eingerichtet werden müssen und die Kfz-Kennzeichen hiermit erst erfasst werden müssen.[1730] Die Erhebung der für das *Entitäts-Clustering* erforderlichen Daten stellt daher – anders als bei der automatisierten Kfz-Kennzeichenkontrolle – keinen Grundrechtseingriff dar.

Insoweit kann für die Frage der Streubreite nur darauf abgestellt werden, ob im Rahmen des unmittelbaren Datenabgleichs des *Entitäts-Clusterings* ein Grundrechtseingriff hinsichtlich der ausscheidenden Personen vorliegt. Da hierbei aber nur nach Treffern der gesuchten *Bitcoin-Adressen* gesucht

1728 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).
1729 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).
1730 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).

wird, lässt sich annehmen, dass die Nichttreffer insoweit spurenlos und unmittelbar technisch ausgeschieden werden.[1731]

Daher liegt hier beim *Entitäts-Clustering* kein Grundrechtseingriff für die ausgeschiedenen Nichttreffer vor. Ein Grundrechtseingriff liegt nur für die ermittelten Treffer vor.

Soweit das *Entitäts-Clustering* etwa eingesetzt wird, um lediglich die *Entität* einer *Bitcoin-Adresse,* die mutmaßlich im Zusammenhang mit einer Straftat steht, zu ermitteln, erfolgt dieser Grundrechtseingriff daher nicht anlasslos.

Insoweit besteht beim Einsatz des *Entitäts-Clusterings* lediglich zur Ermittlung des *Clusters* einer oder mehrerer bestimmter *Bitcoin-Adressen,* bei denen ein Anlass für die Ermittlung besteht, keine erhöhte Streubreite, da jeweils nur ein anlassbezogener Grundrechtseingriff vorliegt und keine Vielzahl von Grundrechtsträgern ohne Anlass betroffen sind.

Festzuhalten bleibt daher, dass die Ermittlung aller *Entitäten* einer jeweiligen Blockchain eine erhebliche Streubreite aufweist und insoweit auch eine erheblich erhöhte Grundrechtsintensität vorliegt.

An dieser erhöhten Grundrechtsintensität fehlt es dagegen, wenn lediglich die *Entität* von einzelnen, bestimmten *Bitcoin-Adressen* ermittelt wird und ein Anlass dieser Ermittlung besteht.

(3) Abschließende Bewertung der Grundrechtsintensität

Vor diesem Hintergrund ergibt sich, dass nur dann ein lediglich geringfügiger Grundrechtseingriff vorliegt, wenn *Entitäts-Clustering*-Verfahren nur in Bezug auf bestimmte, einzelne *Bitcoin-Adressen* eingesetzt werden, bei denen ein Anlass für die Ermittlung besteht. Die Grenze der nach § 161 Abs. 1 StPO zulässigen Grundrechtsintensität ist dagegen überschritten, wenn die *Entitäts-Clustering*-Verfahren eingesetzt werden, um Blockchain-Daten insgesamt nach *Entitäts-Clustern* auszuwerten.

Grund für diese Bewertung ist, dass sich wesentlich intensitätsverringernd die grundsätzliche Pseudonymität der ausgewerteten Daten und die öffentliche Verfügbarkeit auswirken. Dem steht lediglich die geringfügige

1731 Vgl. zum Nichtvorliegen eines Grundrechtseingriffs, wenn Daten technisch spurenlos unmittelbar ausgeschieden werden BVerfGE 100, 313 (366); BVerfGE 150, 244 (266). Vorteilhaft wäre es, wenn technisch tatsächlich abgesichert würde, dass die Nichttreffer ohne irgendwelche weitere Erkenntnismöglichkeiten ausgeschieden werden.

Intensitätssteigerung durch den Umfang der ausgewerteten Daten und deren möglicher Persönlichkeitsrelevanz sowie die Heimlichkeit der Ermittlung und die technikgestützte Auswertung entgegen, die aber insgesamt nicht zu einer Einordnung als grundrechtsintensive Ermittlungsmaßnahme führen. Anders ist dies zu beurteilen, wenn eine erhöhte Streubreite dadurch vorliegt, dass anlasslos eine große Vielzahl von Personen ebenfalls von der Maßnahme betroffen sind.

b) Aufdecken von auffälligem Transaktionsverhalten

Bei dem in Kap. 3, A.II. dargestellten Aufdecken von auffälligem Transaktionsverhalten wird durch die systematische Analyse der Transaktionsdaten, die in der Blockchain enthalten sind, ermittelt, ob und welche Transaktionen von dem durchschnittlichen bzw. typischem Transaktionsverhalten abweichen.[1732] Technisch müssen hierzu zunächst die gesamten Transaktionsdaten der Blockchain analysiert werden, um so zu ermitteln, welches Transaktionsverhalten typisch ist und welches Transaktionsverhalten hiervon abweicht.[1733]

In der Ermittlungspraxis kann diese Auswertungsmethode nur in Bezug auf konkrete einzelne Transaktionen oder *Bitcoin-Adressen* eingesetzt werden. Nur, wenn bei einzelnen Transaktionen oder *Bitcoin-Adressen* bereits aus anderen Gründen der Anfangsverdacht einer Straftat besteht, kann die Auswertungsmethode eingesetzt werden und so der Anfangsverdacht etwa dadurch erhärtet werden, dass die Transaktion oder *Bitcoin-Adresse* tatsächlich auffällig ist. Grund hierfür ist das Erfordernis eines konkreten Anfangsverdachts nach § 161 Abs. 1 StPO.[1734] Insoweit stellt sich die Frage, wie sich dies auf die Grundrechtsintensität des Einsatzes dieser Auswertungsmethode auswirkt.

Hinsichtlich der Datengrundlage – der ausgewerteten Blockchain-Daten – gelten die Ausführungen zur Grundrechtsintensität des *Entitäts-Clusterings*[1735] hier entsprechend. Zusammenfassend soll daher nur kurz festge-

1732 Siehe hierzu im Einzelnen oben unter Kap. 3, A.II.
1733 Siehe hierzu im Einzelnen oben unter Kap. 3, A.II m.w.N.
1734 Siehe zu den Anforderungen des Anfangsverdachts und den daraus resultierenden Folgen für den Einsatz der Auswertungsmethoden ausführlich oben unter Kap. 5, D.I.
1735 Siehe hierzu im Einzelnen oben unter Kap. 5, D.II.3.a)(1).

halten werden, dass sich der Umfang der erhobenen Daten, sowie deren mögliche Persönlichkeitsrelevanz auf Grund der Nähe zu Kontoinformationen, sowie die heimliche Erhebung und die technikgestützte Auswertung[1736] intensitätssteigernd auswirken. Wesentlich intensitätsverringernd wirken sich dagegen die Pseudonymität der Daten, sowie deren öffentliche Verfügbarkeit aus. Aus diesen Faktoren ergibt sich, dass grundsätzlich ein geringfügiger Grundrechtseingriff bei Erhebung und Auswertung[1737] von Blockchain-Daten vorliegt.

Fraglich ist allerdings, wie in diesem Zusammenhang die Streubreite der Maßnahme zu bewerten ist. Hierbei muss beachtet werden, dass die Auswertungsmethoden einerseits nur in Bezug auf eine konkrete Transaktion oder *Bitcoin-Adresse* vorgenommen wird, sodass insoweit jedenfalls keine große Anzahl Unbeteiligter anlasslos betroffen ist. Andererseits muss beachtet werden, dass um zu diesem Ergebnis, ob eine konkrete Transaktion auffällig ist oder nicht, zunächst ermittelt werden muss, wodurch sich auffälliges bzw. typisches Verhalten auszeichnet. Auch diese vorgelagerte Ermittlung von typischem und auffälligem Transaktionsverhalten ist Teil der hier gegenständlichen Auswertungsmethode.

Insoweit stellt sich die Frage, ob dadurch, dass zunächst der Vergleichsmaßstab, welche Transkationen typisch und welche auffällig sind, eine hohe Streubreite dieser Auswertungsmethode vorliegt.

Da grundsätzlich auch der Datenabgleich einen eigenständigen Grundrechtseingriff darstellt[1738], ließe sich insoweit annehmen, dass auch in der systematischen Analyse nach typischem und untypischem Transaktionsverhalten ein Grundrechtseingriff vorliegt. Insoweit läge hierin auch eine erhöhte Streubreite, die zu einer erhöhten Grundrechtsintensität führen könnte.

Dem ließe sich allerdings entgegenhalten, dass hier zwar grundsätzlich ein Datenabgleich vorliegt, dieser aber gerade nicht mit dem Ziel erfolgt, durch Verknüpfung von Einzelinformationen weitere Informationen über

1736 Zwar liegt hier eine andere Variante der technischen Auswertung vor – nämlich das Ermitteln eines typischen bzw. durchschnittlichen Transaktionsverhaltens in einem ersten Schritt und dann der Vergleich von Transaktionen mit diesem Durchschnitt, dies ändert aber nicht an der Bewertung der Intensität, da auch hier durch den Einsatz von Technik eine Auswertung ermöglicht wird, die so nicht händisch möglich wäre.

1737 Zur Grundrechtsintensität der hier gegenständlichen Auswertungsmethode sogleich im Einzelnen.

1738 Vgl. BVerfGE 150, 244 (266).

eine oder mehrere einzelne Transaktionen zu erhalten, sondern das Ziel darin liegt, abstrakt einen Vergleichsmaßstab zu erhalten.

Das trifft jedoch nur im ersten Schritt – der Ermittlung des abstrakten Vergleichsmaßstabes – zu. Denn der Vergleichsmaßstab dient ja gerade dazu, einzelne Transkationen mit ihm zu vergleichen und so eine weitere Einzelinformation über die jeweils verfahrensgegenständliche Transaktion zu erhalten – entspricht sie dem typischen Transaktionsverhalten oder nicht.

Daher muss hier grundsätzlich auf Grund der hohen Streubreite auch eine entsprechende Intensitätssteigerung angenommen werden. Auf Grund dieser Intensitätssteigerung liegt hierin grundsätzlich auch kein lediglich geringfügiger Grundrechtseingriff mehr vor.

Um diese erhöhte Grundrechtsintensität zu vermeiden, könnte es in der Ermittlungspraxis aber möglich sein, die Auswertung in einer anderen Art vorzunehmen: So ließe sich die Auswertung technisch etwa auch in Form eines „Treffer-/Nichttreffer-Modells" anwenden, wobei die Auswertung nur im Hintergrund stattfinden würde und lediglich die Transaktion, bei der aus einem anderen Grund ein Verdacht besteht, mit typischem Transaktionsverhalten verglichen wird.[1739] Die Ermittlungsbehörden könnten insoweit selbst nicht auf das Ergebnis der Auswertung, was eine typische Transaktion ist, zugreifen, sondern würden nur das Ergebnis erhalten, ob eine oder mehrere bestimmte Transaktionen typisch oder auffällig sind. Dabei müsste aber technisch und praktisch gewährleistet werden, dass die Ermittlungsbehörden keinen Zugriff auf Inhalt und Ergebnisse dieser Auswertungen im Hintergrund haben. Hierdurch könnte nämlich die Intensität des Grundrechtseingriffs der Auswertungsmethode verringert werden. Denn für die Bewertung der Intensität ist auch maßgeblich, ob die betroffenen Personen anonym bleiben und ob und welche Nachteile die Betroffenen befürchten müssen oder sie nicht ohne Grund befürchten.[1740] Durch die Einsatzmöglichkeit eines „Treffer-/Nichttreffer-Modells" sind zwar auch al-

1739 Ein vergleichbares „Treffer-/Nichttreffer-Modell" wird insbesondere auch beim grenzüberschreitenden Austausch von DNA-Profilen vorgenommen, vgl. insoweit den Beschluss 2008/616/JI des Rates vom 23. Juni 2008.
zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität. Siehe zu diesem Verfahren und dem hieraus resultierenden Grundrechtsschutz außerdem ausführlich *Böse*, Grundsatz der Verfügbarkeit von Informationen, S. 142ff., S. 147.

1740 Vgl. BVerfGE 100, 313 (376); BVerfGE 107, 299 (320).

le anderen Nutzer der jeweiligen Blockchain von der Auswertungsmethode zunächst betroffen, sie müssen aber keinerlei Nachteile befürchten, wenn die Ergebnisse der systematischen Analyse von typischen Transaktionsverhalten nur in der Weise verwendet werden können, dass einzelne Transaktionen mit dem typischen Transaktionsverhalten verglichen werden können. Außerdem könnte so sichergestellt werden, dass die Personen anonym bleiben. Insoweit ließe sich durch diese Art des Einsatzes der Auswertungsmethode die Intensität der Beeinträchtigung für die Betroffenen verringern, die anlasslos von der Maßnahme betroffen sind.

In dieser Form ließe sich das Aufdecken bzw. in diesem Fall das Ermitteln von auffälligem Transaktionsverhalten noch zulässigerweise als geringfügigen Grundrechtseingriff auf § 161 Abs. 1 StPO stützen.

c) Vergleich mit bekanntem Transaktionsverhalten

Die in Kap. 3, A.III. dargestellten Auswertungsmethoden weisen bestimmte Ähnlichkeiten zu den soeben bereits bewerteten Auswertungsmethoden auf, gehen teilweise aber auch über sie hinaus.[1741] Denn bei den Auswertungsmethoden mit dem Oberbegriff des „Vergleichs mit bekanntem Transaktionsverhalten" werden im Grundsatz wiederum die in der Blockchain enthaltenen Daten systematisch analysiert, in diesem Fall aber noch – vereinfacht gesprochen – mit Zusatzwissen kombiniert, um so genauere Informationen etwa über die Hintergründe der Transaktionen zu erhalten.[1742]

So können etwa durch das in Kap. 3, A.III.1. dargestellte Verfahren Transaktionen bzw. *Entitäten* ermittelt werden, die mutmaßlich im Zusammenhang mit Betrug stehen. Hierzu wird in einem ersten Schritt durch einen *Classifier* das typische Transaktionsmuster ermittelt, das bei Transaktionen besteht, die im Zusammenhang mit Betrug stehen. Durch die so abstrahierten Merkmale von Betrugstransaktionen kann dann die Blockchain nach ähnlichen Transaktionsmustern durchsucht werden.

Vergleichbar ist die in Kap. 3, A.III.2. dargestellte Auswertungsmethode, bei der ebenfalls in einem ersten Schritt Transaktionen analysiert wurden, die im Zusammenhang mit Schneeballsystemen auf der Ethereum-Blockchain standen. Durch das ebenfalls so abstrahierte Transaktionsmuster

1741 Siehe zu diesen Auswertungsmethoden im Einzelnen oben unter Kap. 3, A.III.
1742 Vgl. hierzu bereits oben unter Kap. 3, A.III.

konnte anschließend die Ethereum-Blockchain nach vergleichbaren Transaktionsmustern durchsucht werden.

Ähnlich, aber noch etwas weitgehender bzw. breiter angelegt, ist die in Kap. 3, A.III.3. darstellte Auswertungsmethode der sog. *Labelling*-Verfahren. Hierbei wurde wiederum eine bestimmte Datengrundlage mittels *Classifier* analysiert, um so die abstrakten Transaktionsmuster bestimmter Anwendungsmöglichkeiten von *Bitcoin-Adressen* zu erhalten und anschließend die Blockchain-Daten nach dem Vorliegen vergleichbarer Transaktionsmuster zu durchsuchen. Die *Labelling*-Verfahren gehen insoweit über den Vergleich mit Betrugs- und Schneeballtransaktionen hinaus, als dass hierbei einerseits in einem vorgelagerten Schritt zunächst die in der Blockchain enthaltenen *Bitcoin-Adressen* zu *Entitäten* gruppiert werden. Andererseits wird zwar ebenfalls ein *Classifier* eingesetzt, um abstrakt Transaktionsmuster zu ermitteln, hierbei werden aber nicht nur ein einzelnes Transaktionsmuster – wie das von Betrugs- oder Schneeballtransaktionen – ermittelt, sondern Ziel war etwa die Ermittlung von insgesamt sechs verschiedenen *Labels,* u.a. *Exchange-* und *Mixing-Services*.[1743]

Gemeinsam ist diesen Auswertungsmethoden insoweit, dass sie auf Grund von bestimmtem Hintergrundwissen zunächst auf einer abstrakten Ebene in einem sog. Trainingsschritt die typischen Transaktionsmuster von bestimmten Anwendungsbereichen ermitteln, um im Anschluss nach weiteren Transaktionen zu suchen, die diesem Muster ähnlich sind.

Auf Grund des erforderlichen Anfangsverdachts[1744] können diese Auswertungsmethoden in der Ermittlungspraxis nur eingesetzt werden, um weitere Hintergründe zu einer bestimmten, bereits aus einem anderen Grund als verdächtig eingestuften Transaktion zu ermitteln. So könnte etwa die Identität einer bestimmten Person, die über eine oder mehrere bestimmte *Bitcoin-Adressen* verfügt, dadurch ermittelt werden, dass die Transaktionen dieser *Bitcoin-Adresse* nachverfolgt werden und sobald sie bei einem *Exchange-Service* angelangt sind, die Identität des Kunden abgefragt wird, die die entsprechende *Bitcoin-Adresse* verwendet hat.[1745] Dabei ist zu

1743 Siehe hierzu im Einzelnen bereits oben unter Kap. 3, A.III.3.

1744 Siehe insoweit zu der weiteren Variante des Einsatzes, bei der die Blockchain-Daten unmittelbar nach Transaktionsmustern durchsucht werden, die auf bestimmte Straftaten hindeuten und dem hierbei fehlenden Anfangsverdacht oben unter Kap. 5, D.I.2.c)

1745 Vgl. zur Pflicht der Kundenidentifizierung im Rahmen der Geldwäscheprävention bereits oben unter Kap. 4, B.II.1.c)(1). Die Strafverfolgungsbehörden sind nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG berechtigt, im Fall des

berücksichtigen, dass eine unmittelbare Abfrage der Identitätsdaten der bestimmten *Bitcoin-Adresse* beim Anbieter eines *Exchange-Services* nur dann möglich ist, wenn eine unmittelbare Transaktion zwischen der „verdächtigen" *Bitcoin-Adresse* und der *Bitcoin-Adresse* des *Exchange-Services* stattgefunden hat. Da wohl insbesondere diejenigen, die ihre *Bitcoin-Adressen* zum Zwecke illegaler Aktivitäten verwenden, keinen unmittelbaren Kontakt zu *Exchange-Services* haben, die im Rahmen Geldwäscherechtlicher Präventionspflichten zur Kundenidentifizierung verpflichtet sind, dürften die Auszahlungen in Fiat-Geld wohl in der Regel über mindestens eine weitere *Bitcoin-Adresse* stattfinden. Für die Strafverfolgungsbehörden dürfte es aber möglich sein, dass auch die Identitäten dieser noch unverdächtigen *Bitcoin-Adresse* abgefragt werden, um anschließend, bei der so ermittelten Person eventuell weitere Anhaltspunkte für die Identitätsermittlung der unmittelbar verdächtigen *Bitcoin-Adresse* zu erhalten.

Hinsichtlich der Grundrechtsintensität dieser Auswertungsmethoden ist wiederum auf die gegenständliche Datengrundlage der Blockchain-Daten und deren Erhebung zu verweisen[1746]: intensitätssteigernd wirken sich der Umfang und die Heimlichkeit der erhobenen und ausgewerteten Daten der Blockchain aus, sowie deren Persönlichkeitsrelevanz auf Grund der Nähe zu Kontoinformationen. Intensitätsverringernd wirken sich dagegen Pseudonymität und öffentliche Verfügbarkeit der ausgewerteten Daten aus.

Darüber hinaus muss bei der hier gegenständlichen Auswertungsmethode die umfangreiche technische Unterstützung intensitätssteigernd berücksichtigt werden. Denn, wenn bei den *Entitäts-Clustering*-Verfahren noch darauf abgestellt wurde, dass diese vergleichsweise technisch simpel seien, ist dies insbesondere bei den hier gegenständlichen *Labelling*-Verfahren anders zu beurteilen. Bei den *Labelling*-Verfahren wird nämlich ein *Clustering*-Verfahren für die gesamten Blockchain-Daten vorgeschaltet. Darüber hinaus werden die Transaktionsdaten etwa dahingehend ausgewertet, welche Höhe eingehende und ausgehende Transaktionen haben, wie viele *Bit-*

Verdachts einer Straftat diese Daten bei den entsprechenden Anbietern abzufragen. Praktisch dürfte allerdings das Problem bestehen, dass selbst wenn bekannt ist, dass diese *Bitcoin-Adresse* von einem *Exchange-Service* verwendet wird, noch nicht klar ist, welcher *Exchange-Service* dies ist. Allerdings dürfte es wohl möglich sein, bei allen von der BaFin genehmigten Unternehmen, die derartige Services anbieten, eine entsprechende Abfrage zu machen, soweit die Informationen, welche *Bitcoin-Adresse* zu welchem *Exchange-Service* gehören nicht gespeichert werden, sondern nur zur Identifizierung der unmittelbar „verdächtigen" *Bitcoin-Adresse* verwendet werden.

1746 Siehe hierzu bereits oben unter Kap. 5, D.II.3.a)(1).

coin-Adressen für ein- und ausgehende Transaktionen verwendet werden und wie viele *Bitcoin-Adressen* nur für einzelne Transaktionen verwendet werden. Diese Auswertungen beziehen sich jeweils auf alle *Entitäten.* Dementsprechend gehen die technischen Möglichkeiten dieser Auswertungen weit über das händisch Mögliche hinaus und ermöglichen systematische Verknüpfungen von Einzelinformationen.

Außerdem muss ebenfalls intensitätssteigernd berücksichtigt werden, dass durch das Erstellen von Transaktionsmustern weitergehende Informationen über einzelne Transaktionen und *Entitäten* erhalten werden können. Dementsprechend ist die Persönlichkeitsrelevanz insoweit erhöht. Soweit es auf die Verknüpfung mehrerer Datenbestände ankommen sollte[1747], ergibt sich insoweit ebenfalls eine Intensitätssteigerung dadurch, dass die in der Blockchain enthaltenen Daten mit Zusatzinformationen zu einzelnen Hintergründen verknüpft werden.

Fraglich ist wiederum, wie in diesem Zusammenhang die Streubreite des Einsatzes dieser Auswertungsmethode zu bewerten ist.

Denn problematisch ist hier wiederum, dass die Auswertungsmethode wiederum mehrere Schritte der Datenverarbeitung voraussetzt. So muss in einem ersten Trainingsschritt anhand von Transaktionsdaten mit bekanntem Hintergrund das Transaktionsmuster von bestimmten Akteuren ermittelt werden. Dabei muss außerdem berücksichtigt werden, dass zur Ermittlung dieses einzelnen Transaktionsmusters auch alle weiteren, in der Blockchain enthaltenen Transaktionsdaten herangezogen werden müssen. Denn ein bestimmtes Transaktionsmuster kann nur durch den Vergleich mit anderen Transaktionsmustern ermittelt werden. Die besonderen Eigenschaften von Mustern ergeben sich insoweit nur aus dem Vergleich mit den Eigenschaften aller anderen Transaktionen. Erst nach diesem umfangreichen Trainingsschritt kann ermittelt werden, ob eine oder mehrere bestimmte Transaktionen Ähnlichkeiten mit diesem Transaktionsmuster aufweisen. Für den hier beschriebenen Einsatz der Auswertungsmethode in der Form, dass bei Transaktionen oder *Bitcoin-Adressen,* die bereits aus einem anderen Grund verdächtig sind, geprüft werden soll, ob sie etwa mit einem *Exchange-Anbieter* interagiert hat, muss also zunächst das Transaktionsmuster eines *Exchange-Anbieters* dadurch ermittelt werden, dass die Transaktionen von *Exchange-Anbietern* mit allen anderen in der Blockchain enthaltenen Transaktionen verglichen werden. Dementsprechend besteht hier zunächst

1747 Vgl. BVerfG NJW 2009, 1405 (1406f.).

eine hohe Streubreite, die zu einer erhöhten Grundrechtsintensität führt, die über das nach §§ 161, 163 StPO zulässige Maß hinausgeht.

In Betracht kommt aber auch hier, die Intensität wiederum durch eine Art „Treffer-/Nichttreffer-Modell" zu verringern. So könnte etwa bei einer verdächtigen *Bitcoin-Adresse* zunächst deren „naheliegenden" Transaktionen und *Bitcoin-Adressen* betrachtet werden. Naheliegend wären dann etwa die Transaktionen oder *Bitcoin-Adressen,* mit denen die verdächtige *Bitcoin-Adresse* unmittelbar oder maximal über 2-3 weitere Transaktionen interagiert hat. Bildlich gesprochen ergäbe sich so ein Kreis um die verdächtige *Bitcoin-Adresse* herum. In diesem umliegenden Kreis könnte dann geprüft werden, ob eine der *Bitcoin-Adressen* etwa einer *Entität* zuzuordnen ist, die Kundenidentifizierungspflichten unterliegt, um so Anhaltspunkte für die Identitätsermittlung der verdächtigen *Bitcoin-Adresse* zu erhalten.

Dabei müsste wiederum sichergestellt werden, dass die Ergebnisse der Auswertungsmethode – also das Transaktionsmuster bestimmter *Labells* – nicht zur Kenntnis genommen werden kann. Es dürfte von den Strafverfolgungsbehörden nur eingesehen werden, ob es in einem zu definierenden naheliegenden Umkreis um die verdächtige *Bitcoin-Adresse* eine *Entität* mit einem Transaktionsmuster, das auf eine Identifizierungspflicht hindeutet, gibt.

So würde wiederum die Anonymität aller anderen Nutzer der Blockchain gewahrt werden. Außerdem würde sichergestellt, dass Nutzer nur anlassbezogen betroffen wären. Für die identifizierungspflichtigen Dienstleister bestünde dieser Anlass zwar unabhängig von einem Verdacht einer Straftat. Allerdings wurde die Identifizierungspflicht bei Dienstleistern im Umfeld von Kryptowährungen gerade mit dem Ziel eingeführt, die Anonymität bei Kryptowährungen aufheben zu können.[1748]

(1) Exkurs – Grundrechtsintensität beim Einsatz zum Aufdecken von Transaktionsmustern, die auf bestimmte Straftaten hindeuten

Alternativ ließe sich diese Auswertungsmethode grundsätzlich auch einsetzen, um anhand von Transaktionsmustern, die auf bestimmte illegale Aktivitäten hindeuten, unmittelbar Transaktionen zu ermitteln, die mutmaßlich im Zusammenhang mit Straftaten stehen. Zwar ist dieser Einsatz nach

1748 So Erwägungsgrund Nr. 9, RL (EU) 2018/843, die mit der am 01.01.2020 in Kraft getretenen Änderung von KWG und GwG umgesetzt wurde, vgl. BT.-Drs. 19/13827.

§ 161 Abs. 1 StPO auf Grund des hierfür erforderlichen Anfangsverdachts nicht zulässig, seine Grundrechtsintensität soll hier jedoch trotzdem kurz dargestellt werden. Denn fraglich ist, ob eine durch ein „Treffer-/Nichttreffer-Modell" verringerte Grundrechtsintensität auch dann vorliegen kann, wenn die gesamten Blockchain-Daten nach Transaktionsmustern durchsucht werden, die unmittelbar auf bestimmte illegale Aktivitäten hindeuten.

Denn einerseits dürfte insoweit eine erhöhte Anzahl an Personen betroffen sein – nämlich alle, die dieses Transaktionsmuster tatsächlich aufweisen. Andererseits muss in diesem konkreten Anwendungsfall berücksichtigt werden, dass diese Personen ja nicht anlasslos betroffen werden. Sondern der Grund hierfür liegt darin, dass sie ein Transaktionsmuster aufweisen, das unmittelbar auf illegale Aktivitäten hindeutet.

So nimmt das BVerfG in seinem MIKADO-Beschluss vom 17.2.2009[1749] an, dass bei dem Abgleich „allgemeine[r] Merkmale […] regelmäßig auch zahlreiche unbeteiligte Personen"[1750] betroffen sind. Dies soll dagegen nicht der Fall sein, wenn im Rahmen der Abfrage von Kreditkartendaten, gezielt nach Personen gesucht werde, die mit hinreichender Wahrscheinlichkeit strafbare Handlungen vorgenommen haben.[1751] Da nur die Daten von Personen, bei denen auf Grund der bestimmten Kreditkartenbuchung eine hinreichende Wahrscheinlichkeit für das Vorliegen einer Straftat bestand, übermittelt wurden, wurden auch diejenigen Personen, bei denen die entsprechende Buchung nicht vorlag, nicht in ihren Grundrechten betroffen.

Hiernach wären von der Ermittlung bestimmter illegaler Transaktionsmuster auch nur diejenigen Personen in ihren Grundrechten betroffen, bei denen ein entsprechendes Transaktionsmuster vorliegt. Bei diesen bestünde aber auf Grund des Transaktionsmusters ein entsprechender Anlass, dass sie Gegenstand der Ermittlungsmaßnahme geworden sind, sodass keine Vielzahl Unbeteiligter Personen betroffen wäre.

Fraglich ist aber auch hier, ob diese vom BVerfG im MIKADO-Beschluss aufgestellten Grundsätze nach der zweiten Entscheidung zur automatisierten Kfz-Kennzeichen-Erfassung[1752] noch gelten können. Denn hierin hat das BVerfG festgelegt, das auch diejenigen, die auf Grund des Datenabgleichs mit dem Fahndungsbestand unmittelbar als „Nichttreffer" ausge-

1749 BVerfG NJW 2009, 1405 ff.
1750 BVerfG NJW 2009, 1405 (1406).
1751 BVerfG NJW 2009, 1405 (1407).
1752 BVerfGE 150, 244 ff. Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.

schieden wurden, durch die Erfassung und den Abgleich in ihrem RiS betroffen seien. Zu berücksichtigen ist jedoch, dass das BVerfG auch in seiner zweiten Entscheidung zur automatisierten Kfz-Kennzeichenerfassung bei dem Grundsatz verbleibt, dass weiterhin dann kein Grundrechtseingriff vorliegt, wenn die Daten lediglich technikbedingt miterhoben werden, und anschließend unmittelbar anonym und ohne weiteres Erkenntnisinteresse wieder ausgesondert werden. Das BVerfG formuliert insoweit von diesem Grundsatz nur eine Rückausnahme dahingehend, dass ein Eingriff jedoch dann vorliegen soll, wenn „die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung" sei.[1753] Ob in diesem Zusammenhang bei der Erhebung eines großen Datenbestandes ein Eingriff in das RiS vorliege, hänge maßgeblich davon ab, ob sich „bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet habe, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen"[1754] sei. Abweichend von diesen Grundsätzen ist bei dem hier gegenständlichen Einsatz der Auswertungsmethode zunächst zu berücksichtigen, dass die Erhebung der Blockchain-Daten zunächst noch keinen Eingriff in das RiS begründet.[1755] Darüber hinaus muss beachtet werden, dass zwar grundsätzlich das Ziel verfolgt wird, die „Treffer" von bestimmten, auf illegale Aktivitäten hindeutenden Transaktionsmuster zu ermitteln und insoweit auch das Ziel verfolgt wird, die erfassten Datenbestände zu verkleinern. Anders als bei der automatisierten Kfz-Kennzeichenerfassung ist dies aber nicht das einzig verfolgte Ziel der Erhebung der Blockchain-Daten. Denn diese müssen allein technikbedingt vollständig erhoben werden. Es besteht kein unmittelbares Interesse daran „alle Treffer" zu erhalten, sondern für die Strafverfolgung kann es bereits ausreichen, einige „Treffer" zu ermitteln. Insoweit lässt sich bei einer Gesamtbetrachtung nicht annehmen, dass sich ein spezifisches Interesse an den erhobenen Daten verdichtet hat, das einen Grundrechtseingriff begründen kann.

Dementsprechend können weiterhin die Grundsätze des MIKADO-Beschlusses hier Anwendung finden, sodass auch hier keine Vielzahl Unbeteiligter betroffen ist, wenn die Betroffenheit auf einer konkreten Grundlage

1753 BVerfGE 150, 244 (266).

1754 BVerfGE 150, 244 (266) mit Verweis auf BVerfGE 115, 320 (343) und BVerfGE 120, 378 (398).

1755 Siehe hierzu bereits oben ausführlich unter Kap. 4, B.II.2.c)(1).

beruht, die mit hinreichender Wahrscheinlichkeit auf ein strafbares Verhalten hindeutet. Insoweit hängt die Grundrechtsintensität dieses Einsatzes der Auswertungsmethode maßgeblich von der Zuverlässigkeit der Auswertungsmethode ab. Denn nur, wenn auf Grund eines bestimmten Transaktionsmusters tatsächlich eine hinreichende Wahrscheinlichkeit eines strafbaren Verhaltens vorliegt, wird hinreichend ausgeschlossen, dass Unbeteiligte in ihren Grundrechten betroffen sind.

(2) Zwischenergebnis

Bei der Auswertungsmethode des Vergleichs mit bekanntem Transaktionsverhalten liegt allenfalls ein noch geringfügiger Grundrechtseingriff, der nach § 161 Abs. 1 StPO zulässig wäre, vor, wenn in der beschriebenen Form eines „Treffer-/Nichttreffer-Modells" nur naheliegende Transaktionen und *Bitcoin-Adressen* auf einen bestimmten Hintergrund untersucht werden.

Hinsichtlich der Suche nach Transaktionsmustern, die unmittelbar auf strafbares Verhalten hindeuten, liegt zwar der für § 161 Abs. 1 StPO erforderliche Anfangsverdacht nicht vor[1756], die Maßnahme könnte jedoch auf Grund der Rechtsprechung des BVerfG im MIKADO-Beschluss[1757] noch als geringfügiger Grundrechtseingriff zu bewerten sein.

d) Auswertung des Netzwerkverhaltens und der Netzwerkverbindungen

Darüber hinaus muss die Grundrechtsintensität der in Kap. 3, B. dargestellten Auswertungsmethoden bewertet werden, bei denen maßgeblich das Netzwerkverhalten im Blockchain-Netzwerk ausgewertet wird, um so insbesondere die jeweiligen IP-Adressen den *Bitcoin-Adressen* zuordnen zu können.[1758]

Hierzu wird nachfolgend zunächst auf die grundlegende Möglichkeit der Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten eingegangen (hierzu unter (1)), um anschließend auf die zusätzlich möglichen Auswertungen im Zusammenhang mit dem *Tor-Netzwerk* einzugehen (hierzu unter (2), (3)). Abschließend wird die Grundrechtsintensität der sog. *Bloom-Filter-Attacks* bewertet (hierzu unter (4)).

1756 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.2.c).
1757 BVerfG NJW 2009, 1405ff.
1758 Siehe hierzu ausführlich oben unter Kap. 3, B.

(1) Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten

Zur Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten wurde eine Verbindung mit allen *Full-nodes* hergestellt, um so die Verbreitung von Transaktionsnachrichten im Bitcoin-Netzwerk nachverfolgen zu können und so die IP-Adresse des ersten Absenders der *Bitcoin-Adresse,* die Absender der Transaktionsnachricht war, zuordnen zu können.[1759]

Hinsichtlich der Grundrechtsintensität auf Grund des Umfangs der erhobenen Daten muss hier abweichend von den bereits bewerteten Auswertungsmethoden berücksichtigt werden, dass die Auswertung der Weiterleitung der Transaktionsnachrichten nicht auf der Grundlage aller Blockchain-Daten stattfindet. Dahingehend ist der Umfang der ausgewerteten Daten insoweit geringer als der Umfang der Blockchain-Daten. Allerdings geht der Umfang der ausgewerteten Daten in anderer Hinsicht weit über die Auswertung der Blockchain-Daten hinaus. Denn zur Auswertung des Netzwerkverhaltens muss neben den jeweiligen Transaktionsnachrichten auch erhoben werden, wie sich diese Transaktionsnachrichten jeweils im Netzwerk von allen *Full-nodes* verbreitet hat. Hierzu wurde zunächst eine unmittelbare Verbindung zu allen *Full-nodes* hergestellt, um so von jedem *Full-node* die von ihm weitergeleiteten Transaktionsnachrichten zu erheben und zu speichern. Auf Grund dieser umfangreichen Daten der Netzwerkverbindungen ist auch für die Auswertung des Netzwerkverhaltens eine Intensitätserhöhung auf Grund des Umfangs der erhobenen und ausgewerteten Daten anzunehmen.

Ein weiterer Unterschied zu den bereits bewerteten Auswertungsmethoden liegt darin, dass bei der Auswertung des Netzwerkverhaltens bereits in der Erhebung und Speicherung ein Eingriff in das RiS vorliegt – anders als bei der Erhebung der Blockchain-Daten.[1760] Denn insbesondere hier liegt bereits eine gezielte Speicherung der Verbindungsdaten vor.[1761]

Ebenfalls abweichend könnte zu berücksichtigen sein, dass bei der Auswertung des Netzwerkverhaltens zunächst einmal keine umfassenden Persönlichkeitsbilder erstellt werden können bzw. sollen, da das Ziel der Maßnahme ja darin liegt, *Bitcoin-Adressen* einer IP-Adresse zuzuordnen und nicht die Transaktionen selbst ausgewertet werden wie bei den vorstehend bewerteten Auswertungsmethoden. Insoweit sind zunächst nicht die

1759 Siehe hierzu im Einzelnen ausführlich unter Kap. 3, B.I.
1760 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c)(1).
1761 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c)(1).

mit Kontoinformationen vergleichbaren Transaktionsdaten der Blockchain Gegenstand der Auswertung, sondern nur das Weiterleitungsverhalten der *Full-nodes*. Allerdings muss auch beachtet werden, dass hiervon ja gerade auch die Transaktionsnachrichten beinhaltet sind – diese werden ja gerade weitergeleitet. Insoweit liegt das Ziel zwar nicht in dem Erstellen von Persönlichkeitsprofilen anhand von Daten, die mit Kontoinformationen vergleichbar sind, es ist aber anhand der Datengrundlage ebenso möglich – auch wenn der Umfang der Transaktionsdaten im Vergleich zu den umfangreichen Blockchain-Daten beschränkt ist. Daher ist auch hier die Gefahr, dass umfassende Persönlichkeitsbilder erstellt werden, intensitätssteigernd zu berücksichtigen. Soweit dagegen für die Intensitätssteigerung darauf abgestellt wird, dass Daten aus mehreren verschiedenen Quellen miteinander abgeglichen werden, ließe sich auf den ersten Blick zwar annehmen, dass hier eine einheitliche Datenquelle bestünde. Allerdings muss beachtet werden, dass bei der Auswertung des Netzwerkverhaltens gerade die Weiterleitungsdaten aller *Full-nodes* erhoben werden müssen. Insoweit liegen hier auch unzählig viele einzelne Datenquellen vor, die jeweils miteinander zum Abgleich gebracht werden.

Im Vergleich zu den zuvor bewerteten Auswertungsmethoden ist außerdem intensitätssteigernd zu berücksichtigen, dass hier die erhobenen und ausgewerteten Daten teilweise einen Rückschluss auf die dahinterstehenden Personen zulassen. Denn Ziel der Auswertung ist es ja gerade, eine *Bitcoin-Adresse* einer IP-Adresse zuordnen zu können, die jedenfalls einer natürlichen oder juristischen Person zugeordnet werden kann.[1762] Insoweit geht die Auswertung des Netzwerkverhaltens über die Auswertung der unmittelbaren Blockchain-Daten hinaus, da diese vorwiegend pseudonym waren. Die hier betrachteten Netzwerkverbindungsdaten sind aber gerade personenbeziehbar. Dies muss insbesondere gelten, wenn die Verschleierung von IP-Adressen über das *Tor-Netzwerk* aktiv im Rahmen der Auswertungsmethode verhindert werden.

Ebenfalls intensitätssteigernd wirkt sich hier aus, dass die Maßnahme wiederum heimlich erfolgt und es praktisch nicht möglich sein wird, alle Betroffenen hierüber zu informieren.

Dagegen ergibt sich keine weitergehende Intensitätssteigerung daraus, dass sich die Strafverfolgungsbehörden zur Erhebung der Daten mit den Betroffenen in eine Kommunikationsbeziehung begeben. Zwar kann sich

1762 Vgl. EuGH NJW 2016, 3579 Ls. 1.

eine dauerhafte Täuschung gegenüber einer Vielzahl Betroffener intensitätssteigernd auswirken[1763], zu berücksichtigen ist hier jedoch, dass ein Grundrechtseingriff nach dem BVerfG nur dann vorliegt, wenn „dabei ein schutzwürdiges Vertrauen in die Identität und die Motivation seines Kommunikationspartners" besteht[1764]. Bei den hier gegenständlichen Auswertungen des Netzwerkverhaltens liegt dagegen nur eine Kommunikationsbeziehung zu allen *Full-nodes* über das öffentlich zugängliche Blockchain-Netzwerk vor. Auf Grund der öffentlichen Zugänglichkeit des Netzwerkes kann daher kein schutzwürdiges Vertrauen in die jeweiligen Kommunikationspartner bestehen.[1765]

In diesem Zusammenhang ist jedoch die maßgebliche Intensitätsverringerung zu berücksichtigen, die sich gerade aus der öffentlichen Zugänglichkeit des Netzwerkes ergibt. Denn die hier gegenständlichen Daten werden eben aus dem öffentlich zugänglichen Blockchain-Netzwerk erhoben, so dass grundsätzlich kein Vertrauen der Betroffenen an deren Vertraulichkeit besteht.

Besonders intensitätssteigernd ist jedoch wiederum die technische Auswertung zu berücksichtigen. Denn wiederum wäre es sowohl bei der Masse der Transaktionsdaten als auch hier insbesondere bei den darüberhinausgehenden Daten über die Weiterleitung der Transaktionsnachrichten keinesfalls möglich, diese händisch auszuwerten. Eine solche Auswertung ist nur technikgestützt möglich. Dementsprechend kann die IP-Adresse einer *Bitcoin-Adresse* nur dadurch zugeordnet werden, dass hier eine technikgestützte Auswertung stattfindet.

Fraglich ist, wie wiederum die Streubreite dieser Auswertungsmethode zu bewerten ist und ob es die Möglichkeit gibt, die Auswertungsmethode mit einer geringen Streubreite einzusetzen.

Ursprünglich wurde die Auswertungsmethode in der Form eingesetzt, dass über einen längeren Zeitraum zunächst die Daten über die Weiterleitung von Transaktionsnachrichten von allen *Full-nodes* erhoben wurden und anschließend danach ausgewertet wurden, von welchem *Full-node* welche Transaktionsnachricht zuerst in das Blockchain-Netzwerk versandt wurde. Ziel war es insoweit, möglichst viele *Bitcoin-Adressen* einer IP-Adresse zuordnen zu können, unabhängig von einem konkreten Anlass. Insoweit besteht bei dieser Form des Einsatzes eine stark erhöhte Streubrei-

1763 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.II.1.c)
1764 BVerfGE 120, 274 (345).
1765 Vgl. BVerfGE 120, 274 (345f.).

te, die zu einer derart erhöhten Grundrechtsintensität führt, dass sie nicht mehr als geringfügig einzustufen ist.

In Betracht kommt jedoch, die Auswertung des Netzwerkverhaltens anlassbezogen vorzunehmen. So könnte etwa die Auswertungsmethode wiederum eingesetzt werden, wenn eine konkret verdächtige *Bitcoin-Adresse* vorliegt, um diese möglichst einer IP-Adresse zuzuordnen. In diesem Fall müssten dann wiederum die Daten über die Weiterleitung der Transaktionsnachricht von allen *Full-nodes* erhoben werden, um so zu ermitteln, ob die verdächtige *Bitcoin-Adresse* eine Transaktion getätigt hat und über die Auswertung der Verbreitung dieser Transaktionsnachricht die IP-Adresse ermittelt werden kann.

Insoweit würden grundsätzlich nur anlassbezogen die jeweiligen Daten über das Weiterleitungsverhalten erhoben und ausgewertet werden.

Problematisch ist in diesem Zusammenhang jedoch, dass anders, als bei der Auswertung der unmittelbaren Blockchain-Daten hier bereits in der Erhebung der Daten ein Eingriff in das RiS vorliegt.[1766] Zwar ließe sich zunächst anführen, dass auch diese Daten lediglich technikbedingt miterhoben würden und anschließend anonym und spurenlos wieder gelöscht würden, sodass in diesem Fall kein Grundrechtseingriff vorliegt.[1767] Allerdings muss auch hier wiederum die Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung beachtet werden, nach der jedoch ein Grundrechtseingriff vorliegt, wenn die Daten lediglich mit dem Ziel der Verkleinerung erhoben werden und sich insoweit ein spezifisches Interesse an den erhobenen Daten bereits verdichtet hat. Anders als bei den vorstehend bereits bewerteten Auswertungen der unmittelbaren Blockchain-Daten, muss hier berücksichtigt werden, dass die Auswertung des Netzwerkverhaltens in Bezug auf eine konkrete *Bitcoin-Adresse* nur dann wirksam ist, wenn die Daten der Weiterleitung aller Transaktionsnachrichten erhoben werden. Denn nur so kann gewährleistet werden, dass im Falle einer neuen Transaktion der verdächtigen *Bitcoin-Adresse* diese auch einer IP-Adresse zugeordnet werden kann. Dementsprechend liegt auch hier eine umfassende Datenerhebung mit dem Ziel der Verkleinerung vor, sodass hier auch die „Nichttreffer" in ihrem RiS betroffen sind und insofern eine große Anzahl an Personen in ihren Grundrechten betroffen ist, die keinen Anlass hierfür gegeben hat. Daher liegt auch dann, wenn die Daten des Netzwerkverhaltens nur im Falle einer verdächtigen *Bitcoin-Adresse*

1766 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(2).
1767 Vgl. BVerfGE 100, 313 (366).

ausgewertet werden, eine hohe Streubreite vor, die zu einer entsprechend hohen Grundrechtsintensität führt.

Aus diesem Grund liegt – unabhängig von der konkreten Einsatzmöglichkeit – eine erhöhte Streubreite und damit ein erhöhter Grundrechtseingriff vor, der nicht mehr nur geringfügig ist.

(2) Auswertung der Verbreitung von Transaktionsnachrichten, wenn zusätzlich eine Verbindung über das Tor-Netzwerk verhindert wird

Fraglich ist, ob sich hinsichtlich dieser Grundrechtsintensität etwas verändert, wenn zur Datenerhebung die Verbindung über das *Tor-Netzwerk* verhindert wird.

Insoweit könnte sich die Frage stellen, ob hier eine weitere Steigerung der Grundrechtsintensität dadurch vorliegt, dass berechtigte Vertraulichkeitserwartungen überwunden werden.[1768] Dies ist jedoch hier nicht der Fall, denn auch in dem Fall, dass die Verbindung über das *Tor-Netzwerk* verhindert wird, werden die maßgeblichen Daten über eine öffentlich zugängliche Verbindung mit dem Blockchain-Netzwerk erhoben. Insoweit wird nur verhindert, dass im Rahmen der Datenerhebung die IP-Adressen der Betroffenen verschleiert werden, an der Erhebung selbst ändert sich allerdings nichts. Deshalb ändert sich auch nichts an den nichtbestehenden Vertraulichkeitserwartungen bei der Datenerhebung, sodass auch hier insgesamt von einer gesteigerten Grundrechtsintensität ausgegangen werden muss, die nicht mehr als geringfügig einzustufen ist.

(3) Auswertung des Datenverkehrs des Tor-Netzwerks

Das Gleiche muss selbst dann gelten, wenn darüber hinaus die Daten ausgewertet werden, die dadurch erhoben werden, dass die Strafverfolgungsbehörden selbst *Tor-Exit-Relays* bereitstellen, um so die Kommunikation, die über das *Tor-Netzwerk* mit dem Blockchain-Netzwerk stattfindet, erheben und auswerten zu können. Denn insoweit muss wiederum gelten, dass in dieser Kommunikationsbeziehung kein berechtigtes und schutzwürdiges Vertrauen besteht.[1769] Soweit die so erhobenen Daten in vergleichba-

1768 Vgl. zu dieser Intensitätssteigerung bereits unter Kap. 5, C.II.2.b)(2).
1769 Siehe hierzu bereits Kap. 4, B.II.2.c)(2).

rer Weise ausgewertet werden, muss insoweit eine entsprechend erhöhte Grundrechtsintensität vorliegen, die ebenfalls als nicht mehr geringfügig anzusehen ist.

(4) Bloom-Filter-Attacks

Auch mit den in Kap. 3, B.III. dargestellten sog. *Bloom-Filter-Attacks* lassen sich IP-Adressen einzelnen *Bitcoin-Adressen* zuordnen.

Hierzu wird die Verwendung von sog. *Bloom-Filtern* bei den sog. *SPV-Clients* ausgenutzt.[1770] *SPV-Clients* werden zur Datenminimierung eingesetzt, damit Bitcoin auch über mobile Endgeräte genutzt werden kann. Hierzu hinterlegt der *SPV-Client* in einem *Bloom-Filter* bei einem *Full-node* die *Bitcoin-Adressen,* die für den Nutzer des *SPV-Clients* relevant sind – in der Regel *Bitcoin-Adressen,* über die der *SPV-Client* verfügt. Bei neuen Transaktionsnachrichten fragt dann der *Full-node* bei diesem *Bloom-Filter* ab, ob eine der *Bitcoin-Adressen* der neuen Transaktionsnachrichten im *Bloom-Filter* enthalten ist, um so nur die neuen Transaktionsnachrichten an den *SPV-Client* weiterzuleiten, die auch für den Nutzers des *SPV-Clients* relevant sind.

Bei der *Bloom-Filter-Attack* fragt nun der *Full-node,* bei dem der *Bloom-Filter* des *SPV-Clients* hinterlegt ist, alle bisher in der Blockchain verwendeten *Bitcoin-Adressen* und die dazugehörigen *public keys* ab, um so zu ermitteln, welche *Bitcoin-Adressen* zur *Wallet* des *SPV-Clients* gehören. Da zwischen *Full-node* und *SPV-Client* eine Netzwerkverbindung bestehen muss, kennt der *Full-node* die IP-Adresse des *SPV-Clients* und kann so die ermittelten *Bitcoin-Adressen* dessen IP-Adresse zuordnen.

Der Umfang der so ermittelten Daten und die damit einhergehenden Grundrechtsintensität hängen von der Art und Weise des Einsatzes der *Bloom-Filter-Attack* ab. So könnte sie grundsätzlich etwa nur in Bezug auf einen speziellen *SPV-Client* eingesetzt werden, um dessen *Bitcoin-Adressen* jeweils einer IP-Adresse zuzuordnen. Insoweit bestünde lediglich ein relativ geringer Umfang an erhobenen Daten.

Dies dürfte in der Ermittlungspraxis allerdings wenig zielführend sein. Denn ein vorrangiges Ziel der Ermittlungen liegt ja darin, die Identität hinter einer bestimmten *Bitcoin-Adresse* zu ermitteln.[1771] Bei der *Bloom-Filter-*

1770 Siehe hierzu im Einzelnen unter Kap. 3, B.III.
1771 Siehe hierzu bereits oben unter Kap. 5, B.II.

Attack ist aber vorher nicht bekannt, welche *Bitcoin-Adressen* der jeweilige *SPV-Client* verwaltet – dies soll ja gerade ermittelt werden. Insoweit wäre es ein Glückstreffer, wenn nur mit einer einzelnen *Bloom-Filter-Attack* bei einem *SPV-Client* die IP-Adresse einer bestimmten, verdächtigen *Bitcoin-Adresse* ermittelt werden könnte.

Daher ist es wahrscheinlicher, dass die *Bloom-Filter-Attack* in der Ermittlungspraxis eher in der Form eingesetzt wird, dass bei einer verdächtigen *Bitcoin-Adresse* die *Bloom-Filter-Attack* bei allen möglichen *SPV-Clients* eingesetzt wird, um so eventuell die IP-Adresse der verdächtigen *Bitcoin-Adresse* ermitteln zu können.

In diesem Fall ist die Grundrechtsintensität der Auswertungsmethode bereits auf Grund des Umfangs der erhobenen Daten jedenfalls erhöht. Denn hierbei müssen jedenfalls die gesamten Blockchain-Daten erhoben werden, um so alle bisher verwendeten *Bitcoin-Adressen* abgleichen zu können.

Ebenfalls stark erhöht ist die Grundrechtsintensität außerdem auf Grund der hohen Streubreite, die dieser Form des Einsatzes der *Bloom-Filter-Attack* einhergeht. Denn bei dieser Form des Einsatzes ist eine große Anzahl Unbeteiligter in ihren Grundrechten betroffen, da wohl auch alle abgefragten *SPV-Clients,* die nicht über die verdächtige *Bitcoin-Adresse* verfügen als „Nichttreffer" in ihrem RiS betroffen sind. Nach dem BVerfG liegt nämlich auch ein Eingriff in das RiS der Personen vor, die als „Nichttreffer" ausgeschieden werden, wenn „die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung"[1772] sei und sich bei einer Gesamtbetrachtung das behördliche Interesse an den erhobenen Daten bereits in einer einen Grundrechtseingriff auslösenden Weise verdichtet habe.[1773] Wenn also die *Bloom-Filter-Attack* bei allen verfügbaren *SPV-Clients* eingesetzt wird, um so die IP-Adresse einer bestimmten, verdächtigen *Bitcoin-Adresse* zu ermitteln, ist diese Maßnahme nur erfolgversprechend, wenn sie auch tatsächlich bei allen verfügbaren *SPV-Clients* eingesetzt wird. Daher hat sich beim Einsatz der *Bloom-Filter-Attack* bereits ein spezifisches Interesse an den anschließend ausscheidenden Daten verdichtet, sodass auch die „Nichttreffer" in ihrem RiS betroffen sind und demensprechend eine hohe Streubreite vorliegt.

Darüber hinaus muss intensitätssteigernd berücksichtigt werden, dass durch die *Bloom-Filter-Attacks* ein unmittelbarer Personenbezug möglich

1772 BVerfGE 150, 244 (266).
1773 BVerfGE 150, 244 (266).

gemacht wird und insoweit die Gefahr besteht, dass ein Persönlichkeitsprofil, das auf Grund der Blockchain-Daten erstellt wird, einer Person zugeordnet werden kann. Soweit nach anderer Auffassung auf die Verknüpfung unterschiedlicher Datenquellen abgestellt wird, liegt auch diese durch den Abgleich der *Bitcoin-Adressen,* die in der Blockchain gespeichert sind, mit den in den *Bloom-Filtern* hinterlegten *Bitcoin-Adressen* vor. Auch insoweit wäre die Grundrechtsintensität entsprechend erhöht.

Ferner ist wiederum die technische Unterstützung intensitätssteigernd zu berücksichtigen, da hieraus wiederum Rückschlüsse und Informationen gewonnen werden können, die durch einen händischen Abgleich nicht möglich wären.

Diesen intensitätssteigernden Aspekten steht wiederum maßgeblich die öffentliche Verfügbarkeit der erhobenen und ausgewerteten Daten gegenüber. Denn einerseits sind zunächst die in die Blockchain enthaltenen *Bitcoin-Adressen* öffentlich verfügbar. Andererseits beruht die Auswertung der *Bloom-Filter* darauf, dass sich die Strafverfolgungsbehörden in eine Telekommunikationsbeziehung mit den betroffenen *SPV-Clients* begeben, um so deren *Bloom-Filter* abgleichen zu können. Allerdings besteht kein schutzwürdiges Vertrauen der Nutzer, die die *SPV-Clients* verwenden, in die mit den *Full-nodes* geführte Telekommunikation.

Diese Faktoren – insbesondere die hohe Streubreite – führen insgesamt zu einer erhöhten Grundrechtsintensität des Einsatzes von *Bloom-Filter-Attacks,* die nicht mehr als geringfügig anzusehen sind.

Darüber hinaus könnte die *Bloom-Filter-Attack* auch unabhängig von einem bestehenden Verdacht eingesetzt werden, um so möglichst viele *Bitcoin-Adressen* einer IP-Adresse zuzuordnen, damit in einem Verdachtsfall auf diese Daten zurückgreifen zu können. Dieser Einsatz entspricht daher einer Datensammlung auf Vorrat. Insoweit würde sich jedoch die Streubreite nochmals erhöhen, sodass die Grundrechtsintensität auch hier jedenfalls nicht mehr als geringfügig einzuordnen ist.

(5) Zwischenergebnis

Bei allen Auswertungen des Netzwerkverhaltens und der Netzwerkverbindungen liegt auf Grund der erhöhten Streubreite ein nicht mehr nur geringfügiger Grundrechtseingriff vor.

e) Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten

Die Grundrechtsintensität der in Kap. 3, C. dargestellten Auswertungsmethoden durch eine Verknüpfung von anderweitig verfügbaren Daten hängt u.a. auch von deren konkretem Einsatz ab.

(1) Durchsuchen des Internets nach Bitcoin-Adressen

Wenn etwa das Internet nach *Bitcoin-Adressen* durchsucht wird, um so Anhaltspunkte für die dahinterstehende Identität zu erhalten[1774], dürfte insbesondere der bisher maßgebliche Faktor der Streubreite vom konkreten Einsatz abhängen.

Denn einerseits ist es möglich, in einem konkreten Verdachtsfall das Internet nach einer verdächtigen *Bitcoin-Adresse* zu durchsuchen – etwa einfach mit Google. In diesem Fall dürfte die Streubreite verhältnismäßig gering sein, denn soweit etwa über Foren-Beiträge oder Ähnlichem Anhaltspunkte für die Identität der verdächtigen *Bitcoin-Adresse* erhalten werden, erfolgt dies jedenfalls anlassbezogen. Außerdem wäre auch der Umfang der erhobenen Daten verhältnismäßig gering. Intensitätssteigernd wären allerdings sowohl die heimliche Erhebung, sowie die Gefahr, dass anschließend personenbezogene Persönlichkeitsprofile erstellt werden könnten[1775] zu berücksichtigen. Andererseits muss wiederum intensitätsverringernd berücksichtigt werden, dass sowohl die Blockchain-Daten als auch die durchsuchten Daten des Internets öffentlich verfügbar sind. Insoweit ließe sich im Fall dieses Einsatzes noch ein geringfügiger Grundrechtseingriff annehmen.

Andererseits ist es eben auch möglich, durch einen *Web-Crawler* das Internet systematisch nach der bestimmten Zeichenstruktur von *Bitcoin-Adressen* und *public keys* zu durchsuchen, um so möglichst viele Daten über möglichst viele *Bitcoin-Adressen* zu erhalten[1776], die dann im Fall eines konkreten Verdachts genutzt werden können. Der Einsatz würde insoweit anlasslos erfolgen und damit eine besonders hohe Streubreite aufweisen, sodass jedenfalls kein geringfügiger Grundrechtseingriff mehr vorliegt.

1774 Siehe hierzu im Einzelnen oben unter Kap. 3, C.I.
1775 Bzw., dass hier ein Abgleich mehrerer unterschiedlicher Datenquellen stattfindet.
1776 Siehe hierzu im Einzelnen oben unter Kap. 3, C.I.

(2) Auswertung von Dritt-Anbieter-Cookies

Bisher ist noch nicht eindeutig klar, wie konkret die Auswertung von Dritt-Anbieter-Cookies zum Zweck der Strafverfolgung eingesetzt werden kann. So stellt sich für die Bewertung der Grundrechtsintensität insbesondere die Frage danach, wie die von den Dritt-Anbieter-Cookies erhobenen Daten von den Strafverfolgungsbehörden erhoben werden können und ob diese nur in einem konkreten Verdachtsfall erhoben werden können, ohne dass die Daten von Dritten hiervon betroffen sind. Darüber hinaus dürfte die Grundrechtsintensität auch davon abhängen, welchen Umfang die erhobenen Daten haben. Dabei muss auch berücksichtigt werden, dass jedenfalls die Blockchain-Daten einen großen Umfang haben und durch die zusätzliche Auswertung von Dritt-Anbieter-Cookies weitergehende Rückschlüsse mit möglicher Persönlichkeitsrelevanz haben können[1777].

(3) Standortdaten-Ermittlung bei IoT-Blockchain-Anwendung

Ebenfalls bisher noch nicht klar ist, wie die von *Shahid et.al.*[1778] lediglich theoretisch dargestellte Auswertung von IoT-Blockchain-Anwendungen tatsächlich eingesetzt werden kann. Daher kann auch hier wiederum nur auf die Faktoren, die für die Bewertung der Grundrechtsintensität maßgeblich werden können, eingegangen werden.

So dürfte hier in einem besonderen Maße der Umfang der erhobenen Daten sowie deren mögliche Persönlichkeitsrelevanz zu beachten sein. Denn, wenn mittels der in der Blockchain enthaltenen Daten durch die Verknüpfung von Einzelinformationen konkrete Bewegungsprofile von einzelnen Personen erstellt werden können, erhöht dies die Grundrechtsintensität in besonderem Maße.

Darüber hinaus dürfte wiederum maßgeblich zu beachten sein, wie zielgerichtet wie Maßnahme eingesetzt werden kann und, ob eine hohe Anzahl Unbeteiligter hiervon betroffen sein kann.

1777 Bzw. es werden mehrere unterschiedliche Daten miteinander abgeglichen.

1778 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (116ff.).

f) Kombination von Auswertungsmethoden

Wenn schließlich in der Ermittlungspraxis die einzelnen Auswertungsmethoden miteinander kombiniert werden, erhöht sich die Grundrechtsintensität jeweils um die Intensität der jeweiligen Auswertungsmethode.

Insoweit muss etwa berücksichtigt werden, dass etwa bei der Kombination von *Labelling*-Verfahren und Auswertung des Weiterleitungsverhaltens der Transaktionsnachrichten zunächst jedenfalls die Streubreite nochmals erhöht ist. Darüber hinaus muss in diesem Zusammenhang in besonderem Maße auch die erhöhte Gefahr der Persönlichkeitsrelevanz berücksichtigt werden. Denn einerseits wird es insbesondere über die Zuordnung einer IP-Adresse zu einer *Bitcoin-Adresse* möglich, einen konkreten Personenbezug herzustellen. Andererseits ist es außerdem möglich, mittels der systematischen Auswertung der Transaktionsmuster weitergehende Rückschlüsse zu erhalten, die abhängig von den Daten der jeweiligen Trainingsgrundlage und auch besondere Persönlichkeitsrelevanz haben könnten.

Insoweit führt die Kombination mehrere Auswertungsmethoden zu einer erhöhten Grundrechtsintensität, die jedenfalls nicht mehr geringfügig ist.

g) Zwischenergebnis

Als noch geringfügiger Grundrechtseingriff zulässig ist das *Entitäts-Clustering,* soweit es nur in einem Verdachtsfall bezogen auf eine verdächtige *Bitcoin-Adresse* eingesetzt wird. Die Grenze der Geringfügigkeit wird allerdings auf Grund einer erhöhten Streubreite überschritten, wenn anlasslos alle in einer Blockchain enthaltenen *Bitcoin-Adressen* zu *Entitäten* gruppiert werden.

Bei dem Aufdecken von auffälligem Transaktionsverhalten besteht ebenfalls das Problem der erhöhten Streubreite, die zu einer erhöhten Grundrechtsintensität führt, da jedenfalls eine systematische Auswertung aller in der Blockchain enthaltenen Transaktionsdaten erforderlich ist. Insoweit ist allenfalls der Einsatz der Auswertungsmethode in Form eines „Treffer-/Nichttreffer-Modells“ als noch geringfügiger Grundrechtseingriff zulässig, da so vermieden werden kann, dass die Betroffenen, die keinen Anlass für die Ermittlung gegeben haben, Gegenstand strafrechtlicher Ermittlungen werden.

Ein ähnliches Problem stellt sich auch bei den als *Labelling*-Verfahren bezeichneten Auswertungsmethoden. Denn auch hier müssen jedenfalls

alle in der Blockchain enthaltenen Transaktionsdaten zunächst systematisch ausgewertet werden, damit ein Vergleichsmaßstab besteht. Auf Grund dieser hohen Streubreite ist daher wiederum allenfalls der Einsatz dieser Auswertungsmethode in vergleichbarer Form wie ein „Treffer-/Nichttreffer-Modell" als noch geringfügiger Grundrechtseingriff vorstellbar, um so zu vermeiden, dass Unbeteiligte Gegenstand strafrechtlicher Ermittlungen werden. Hinsichtlich des Einsatzes eines *Labelling*-Verfahrens zur Ermittlung von noch unbekannten Transaktionen, die auf Grund ihres Transaktionsmusters auf bestimmte illegale Aktivitäten hindeuten, hängt die Zulässigkeit als geringfügiger Grundrechtseingriff davon ab, wie zuverlässig die Ergebnisse dieser Auswertungsmethode sind.

Bei der Auswertung des Netzwerkverhaltens stellt sich die Bewertung der Grundrechtsintensität noch etwas anders dar, denn hier besteht bereits bei der Erhebung der jeweiligen Datengrundlage ein Eingriff in das RiS. Insoweit besteht etwa bereits bei der grundlegenden Auswertung der Daten über die Weiterleitung von Transaktionsnachrichten auch dann eine erhöhte Streubreite, wenn sie nur in Bezug auf eine konkret verdächtige *Bitcoin-Adresse* vorgenommen wird. Denn hierzu müssen grundsätzlich alle Weiterleitungsdaten mit dem Ziel, diese wiederum zu verkleinern, erhoben werden, sodass bereits in der Erhebung und Aussonderung der „Nichttreffer" ein Grundrechtseingriff vorliegt, der zu einer entsprechenden Streubreite und damit einhergehenden erhöhten Grundrechtsintensität führt. Gleiches gilt, soweit darüber hinaus die Verbindung über das *Tor-Netzwerk* verhindert wird und die über das *Tor-Netzwerk* übermittelten Daten in vergleichbarer Weise ausgewertet werden. Insoweit besteht hier jedenfalls keine geringfügige Grundrechtsintensität mehr.

Ähnlich gilt dies für die sog. *Bloom-Filter-Attacks.* Denn in der Ermittlungspraxis wird diese Auswertungsmethode so eingesetzt werden müssen, dass nicht nur ein einzelner *SPV-Client* abgefragt wird, sondern möglichst alle verfügbaren. Insoweit ergibt sich auch hier wiederum eine erhöhte Streubreite, da auch hier bereits auch für die „Nichttreffer" ein Grundrechtseingriff vorliegt, der sich daraus ergibt, dass die gesamten Daten mit dem Ziel der Verkleinerung erhoben werden. Dementsprechend ist auch der Einsatz der *Bloom-Filter-Attacks* wohl in der Regel auch als nicht mehr geringfügig einzustufen.

Anders stellt sich die Grundrechtsintensität dar, wenn lediglich das Internet anlassbezogen nach Anhaltspunkten zur Identitätsermittlung durchsucht wird – dann dürfte der Grundrechtseingriff noch geringfügig sein. Die Grenze der Geringfügigkeit ist jedoch überschritten, wenn anlassunab-

hängig mittels *Web-Crawler* die öffentlich verfügbaren Inhalte im Internet nach möglichst vielen Hintergrundinformationen durchsucht werden, um so hierauf im Verdachtsfall zurückgreifen zu können.

Hinsichtlich der Auswertung von Dritt-Anbieter-Cookies und IoT-Blockchain-Anwendungen hängt die jeweilige Grundrechtsintensität grundsätzlich von deren konkreter Umsetzung ab. Dabei dürfte insbesondere relevant werden, ob und welche Rückschlüsse auf die Persönlichkeit gezogen werden können und ob und wie viele Unbeteiligte von den Auswertungsmethoden betroffen werden.

Schließlich liegt auf Grund der erhöhten Streubreite und Gefahr der Persönlichkeitsrelevanz kein geringfügiger Grundrechtseingriff mehr vor, wenn die einzelnen Auswertungsmethoden miteinander kombiniert werden.

4. Zwischenergebnis

Ein lediglich geringfügiger Grundrechtseingriff liegt dann vor, wenn die in Kap. 3, A. dargestellten Auswertungsmethoden, die als Datengrundlage die unmittelbaren Blockchain-Daten nutzen, anlassbezogen eingesetzt werden und dabei sichergestellt wird, dass unbeteiligt Betroffene nicht Gegenstand eines Strafverfahrens werden können und deren personenbezogene Daten nur zu Vergleichszwecken betroffen werden. Ebenfalls nur geringfügig ist auch der Grundrechtseingriff, bei der anlassbezogenen Suche nach weiteren Anhaltspunkten im öffentlich zugänglichen Internet.

Der Einsatz aller weiteren Auswertungsmethoden ist als nicht mehr geringfügig anzusehen. Hintergrund dieser unterschiedlichen Einordnung ist maßgeblich, dass bei allen Auswertungsmethoden, die nicht nur die jeweiligen Blockchain-Daten als Grundlage nutzen, bereits in der gezielten Erhebung und Speicherung der jeweiligen Daten ein Grundrechtseingriff vorliegt, der eine entsprechend höhere Streubreite auslöst.

III. Zwischenergebnis

Dementsprechend können nur die Kap. 3, A., C.I. dargestellten Auswertungsmethoden zulässigerweise auf §§ 161, 163 StPO gestützt werden, wenn sie lediglich in Bezug zu einem konkreten Straftatverdacht eingesetzt werden. Eine darüber hinausgehende Anwendung der Auswertungsmethoden

ist dagegen nicht mehr durch die Ermittlungsgeneralklauseln der §§ 161, 163 StPO verfassungsrechtlich gerechtfertigt.

E. Zusammenfassung

Aus den vorstehenden Ausführungen ergibt sich zunächst, dass als Ermächtigungsgrundlage für den Einsatz der hier gegenständlichen Auswertungsmethoden des Kapitels 3 nur die Ermittlungsgeneralklauseln der §§ 161, 163 StPO einschlägig sein können.

Zwar ermächtigt insbesondere § 98a StPO zu einem maschinellen Datenabgleich und damit zu einem Eingriff in das RiS. Der Anwendungsbereich des § 98a StPO ist allerdings in mehrfacher Hinsicht eingeschränkt und besonders geprägt von der ursprünglichen Rasterfahndung. Dementsprechend ist § 98a StPO für die hier gegenständlichen Auswertungsmethoden selbst dann nicht einschlägig, wenn man der hier vertretenen Auffassung folgt, dass auch der Datenabgleich von nur einer Speicherstelle in den Anwendungsbereich des § 98a StPO fällt, wenn eine Datenabfrage und ein Datenabgleich mit dem Ziel, einen unbestimmten Personenkreis zu ermitteln, stattfindet. Denn die Datengrundlage des maschinellen Datenabgleichs des § 98a StPO ist auf Grund des begrenzten Wortlauts auf Daten, die entweder freiwillig herausgegeben wurden oder zuvor nach § 98a Abs. 2 StPO erhoben bzw. übermittelt wurden, beschränkt. Insoweit kann § 98a StPO nicht einschlägig sein, wenn – wie bei den hier gegenständlichen Auswertungsmethoden – zuvor Daten aus öffentlich zugänglichen Quellen von den Strafverfolgungsbehörden erhoben wurden.

Insoweit bestätigt sich das bereits eingangs erwähnte Problem, dass der Fokus der Ermittlungsbefugnisse der StPO auf der Erhebung von bestimmten Daten liegt und nicht auf bestimmten Datenverarbeitungsmaßnahmen.

Die hier einschlägigen Ermittlungsgeneralklauseln der §§ 161, 163 StPO genügen grundsätzlich den verfassungsrechtlichen Anforderungen an die Einschränkung des RiS.

Sie können allerdings nur eine verfassungsrechtliche Rechtfertigung für geringfügige Grundrechtseingriffe darstellen, da sie einerseits als Generalklauseln relativ unbestimmt sind und andererseits zur Ermittlung sämtlicher Straftaten einschlägig sind und insoweit nur bei geringfügigen Grundrechtseingriffen verhältnismäßig sind.

Ob ein geringfügiger Grundrechtseingriff bei den hier gegenständlichen Auswertungsmethoden vorliegt, hängt maßgeblich auch davon ab, ob hier

eine noch geringe Streubreite vorliegt. Dies hängt teilweise wiederum von dem konkreten Einsatz der Auswertungsmethoden ab.

Dementsprechend genügen die §§ 161, 163 StPO als verfassungsrechtliche Rechtfertigung für die hier gegenständlichen Auswertungsmethoden nur dann, wenn die unmittelbaren Blockchain-Daten nur im konkreten Verdachtsfall und auch nur in Bezug auf diesen konkreten Verdachtsfall ausgewertet werden und, wenn technisch sichergestellt wird, dass Daten, die nicht Gegenstand des konkreten Verdachts sind, ohne weitere Erkenntnisse ausgesondert werden. Darüber hinaus kann das öffentlich zugängliche Internet auch anlassbezogen nach weiteren Informationen durchsucht werden.

Dem entgegen besteht durch die §§ 161, 163 StPO keine ausreichende verfassungsrechtliche Rechtfertigung für die Auswertungsmethoden, die in Kap. 3, B. dargestellt wurden. Denn anders als bei der Auswertung der unmittelbaren Blockchain-Daten liegt bei den in Kap. 3, B. dargestellten Auswertungsmethoden in der Regel bereits durch die Datenerhebung ein Eingriff in das RiS vor, sodass sich die Streubreite entsprechend maßgeblich erhöht.

Außerdem bieten die Ermittlungsgeneralklauseln keine verfassungsrechtliche Rechtfertigung für den Einsatz der in Kap. 3, A. dargestellten Auswertungsmethoden, wenn diese in der Form eingesetzt werden, dass auch Erkenntnisse über Personen, die nicht Gegenstand des konkreten Verdachts sind, hieraus hervorgehen können.

Soweit darüber hinaus die Erkenntnisse der jeweiligen Auswertungsmethoden miteinander kombiniert werden, steigert sich die Grundrechtsintensität, sodass die §§ 161, 163 StPO keine ausreichende verfassungsrechtliche Rechtfertigung mehr bieten.

Dementsprechend kann eine Verletzung des RiS durch die Anwendung der hier gegenständlichen Auswertungsmethoden vorliegen.

F. Lösungsvorschlag – § 98a Abs. 2 S. 2 StPO-E

Da der Einsatz der hier gegenständlichen Auswertungsmethoden nur teilweise durch die §§ 161, 163 StPO verfassungsrechtlich gerechtfertigt ist, empfiehlt sich die Schaffung einer neuen, ausreichenden Rechtsgrundlage für den Einsatz der Auswertungsmethoden.

Dabei muss berücksichtigt werden, dass in § 98a StPO bereits eine verfassungsgemäße[1779] Ermächtigungsgrundlage besteht, die grundsätzlich zu einem Eingriff in das RiS in Form der Auswertung von personenbezogenen Daten ermächtigt, der eben auch eine Vielzahl an unbeteiligten Personen betrifft.[1780] Insoweit bietet § 98a StPO bereits eine ausreichend bestimmte[1781] und verhältnismäßige Ermächtigungsgrundlage für maschinelle Datenabgleiche, bei der technikgestützt eine große Menge personenbezogener Daten ausgewertet werden.

Es bietet sich daher an, § 98a Abs. 2 StPO um folgenden Satz 2 zu erweitern:

> *„Zu diesem Zweck sind die Strafverfolgungsbehörden außerdem ermächtigt, allgemein zugängliche Daten zu erheben und für den Abgleich zu verarbeiten.“*

Hierdurch könnte gewährleistet werden, dass auch die hier gegenständlichen Auswertungsmethoden in den Anwendungsbereich der Rasterfahndung nach § 98a StPO fallen würden. Denn, dass die hier gegenständlichen Auswertungsmethoden nicht vom Anwendungsbereich des § 98a StPO erfasst sind, beruht nach der hier vertretenen Auffassung nur darauf, dass die Datengrundlage des maschinellen Datenabgleichs in § 98a Abs. 1 StPO auf Grund des begrenzten Wortlauts auf freiwillig herausgegebene Daten oder zuvor nach § 98a Abs. 2 StPO erhobene Daten beschränkt ist. Wenn aber die Strafverfolgungsbehörden mit dem vorgeschlagenen S. 2 des § 98a Abs. 2 StPO selbst zur Erhebung öffentlich zugänglicher Daten ermächtigt wären, könnte auch die maschinelle Auswertung von derartigen Daten auf § 98a StPO gestützt werden.

Durch eine Erfassung der maschinellen Datenabgleiche der hier gegenständlichen Auswertungsmethoden in § 98a StPO könnte außerdem gewährleistet werden, dass die mit den Auswertungsmethoden verbundenen Grundrechtseingriffe in einem angemessenen Verhältnis zu den mit ihnen verfolgten Zwecken stehen würden. Denn anders als bei den Ermittlungsgeneralklauseln setzt § 98a Abs. 1 StPO das Vorliegen zureichender tatsächli-

1779 Löwe-Rosenberg/*Menges,* § 98a Rn. 14; vgl. BVerfGE 115, 320ff.

1780 Löwe-Rosenberg/*Menges,* § 98a Rn. 12ff.

1781 § 98a StPO genügt grundsätzlich den verfassungsrechtlichen Bestimmtheitsanforderungen, Löwe-Rosenberg/*Menges,* § 98a Rn. 12ff.; Siehe zur Problematik der Bestimmtheit des § 98a SK-StPO/*Wohlers/Greco,* § 98a Rn. 6 m.w.N., die allerdings auch zu dem Ergebnis kommen, dass § 98a StPO hinreichend bestimmt ist.

cher Anhaltspunkte für das Vorliegen einer Straftat von erheblicher Bedeutung aus dem Katalog der Nr. 1 – 6 voraus.[1782] Insoweit wäre die Zulässigkeit der Grundrechtseingriffe, die mit den hier gegenständlichen Auswertungsmethoden einhergehen, entsprechend begrenzt.

Weiterhin wäre durch die explizite Erfassung der Erhebung öffentlicher verfügbarer Daten zum Zweck von maschinellen Datenabgleichen das besonders im Rahmen des RiS zu beachtende Bestimmtheitsgebot gewahrt.[1783] So wäre für den Bürger einerseits klar ersichtlich, dass zu bestimmten Zwecken öffentlich verfügbare Daten maschinell abgeglichen werden dürfen und andererseits wäre hieraus im Umkehrschluss erkennbar, dass der Handabgleich von öffentlich verfügbaren Daten auf Grund der hierbei nicht gesteigerten Grundrechtsintensität nur den Anforderungen der §§ 161, 163 StPO unterliegen würde.

Außerdem würde der gesteigerten Grundrechtsintensität durch den in § 98b StPO enthaltenen Richtervorbehalt Rechnung getragen.

Bei einer Umsetzung der vorgeschlagenen Änderung müsste allerdings das Zitiergebot beachtet werden, da hierdurch neue Grundrechtsbeschränkungen möglich wären.[1784]

In der Kommentarliteratur wird angenommen, die Rasterfahndung sei bei der auch maschinellen Auswertung von öffentlich verfügbaren Daten nicht anwendbar, da hierin auf Grund der öffentlichen Verfügbarkeit entweder kein oder nur ein geringfügiger Grundrechtseingriff vorliege, der auch auf die §§ 161, 163 StPO gestützt werden könne.[1785] Dem sind die bereits dargestellten Ausführungen zur Grundrechtsintensität entgegenzuhalten.[1786] Insbesondere ist anzumerken, dass bereits in der zielgerichteten Erhebung von öffentlich verfügbaren Daten ein Eingriff in das RiS vor-

1782 Siehe hierzu bereits ausführlich unter Kap. 5, D.II.1.a)(1).

1783 Siehe zu den Bestimmtheitsanforderungen bereits ausführlich unter Kap. 5, C.IV.

1784 Vgl. BVerfGE 113, 348 (366), wonach das Zitiergebot auch bei Änderungen von bereits bestehenden Ermächtigungsgrundlagen zu beachten ist, die zu neuen Grundrechtsbeschränkungen führen.

1785 KK-StPO/*Greven,* § 98a Rn. 33; SK-StPO/*Wohlers/Greco,* § 98a Rn. 4; KMR-StPO/*Jäger,* § 98a Rn. 7, der allerdings unter Verweis auf *Rückert,* ZStW 129 (2017), 302 (332f.) angibt, dass möglicherweise ab einer automatisierten Erhebung und Auswertung von öffentlich zugänglichen Informationen eine mit §§ 111, 163d StPO vergleichbare Eingriffsintensität bestehen würde.

1786 Siehe hierzu ausführlich bereits unter Kap. 5, D.II.3.

liegt[1787], der bei den hier gegenständlichen Auswertungsmethoden teilweise auch einen gesteigerten Grundrechtseingriff darstellt.[1788]

Insoweit bietet die hier vorgeschlagenen Lösung einen hinreichenden Ausgleich zwischen dem Strafverfolgungsinteresse, dass weiterhin bei allen Straftaten grundsätzlich allgemein zugängliche Informationen im Internet – auch unter Verwendung von Suchmaschinen – genutzt werden können, der maschinelle Datenabgleich von allgemein zugänglichen Informationen aus dem Internet aber nur unter den zusätzlichen Voraussetzungen der §§ 98a, 98b StPO zulässig ist.

1787 Vgl. BVerfGE 120, 274 (345).
1788 Siehe hierzu ausführlich bereits unter Kap. 5, D.II.3.