Kapitel 4 – Grundrechtsrelevanz der Auswertungen von Blockchain-Systemen

Vorstehend wurden nun eingehend die technischen Funktionsweisen unterschiedlichster Ermittlungsmöglichkeiten im Zusammenhang mit Blockchains dargestellt.[434]

Nachfolgend wird nun die Frage untersucht, ob und in welche Grundrechte ein Eingriff durch diese Ermittlungsmöglichkeiten vorliegen könnte.

Hierzu wird zunächst einleitend kurz und beispielhaft dargestellt, wie Ermittlungen in der Praxis tatsächlich ablaufen könnten (hierzu unter A.), um anschließend bewerten zu können, welche Grundrechte hiervon betroffen wären (hierzu unter B.).

A. Blockchain-Ermittlungen in der Praxis

Im Bereich von Cybercrime-Ermittlungen dürfte in der Regel das Ziel bestehen, die Identität(en) der verdächtigen Person(en) festzustellen. Soweit etwa Kryptowährungen im Zusammenhang mit einer Straftat stehen, können die in Kap. 3 dargestellten Auswertungsmethoden angewendet werden, um über die jeweils verwendeten *public keys* Rückschlüsse oder Anhaltspunkte auf die Identitäten der Personen zu erhalten.

Wird etwa ein strafrechtliches Ermittlungsverfahren gegen Unbekannt wegen des Verdachts auf illegalen Drogenhandel eingeleitet, könnte eine in diesem Zusammenhang auf einem *Darknet-Handelsplatz* verwendete *Bitcoin-Adresse* als Anhaltspunkt für eine Identitätsermittlung genutzt werden.

So könnte etwa eine der in Kap. 3, B. dargestellten Auswertungsmethoden angewandt werden, um zu ermitteln, über welche IP-Adresse die *Bitcoin-Adresse* verwendet wird. Sollte dies für die konkrete *Bitcoin-Adresse* nicht möglich sein – etwa, weil sie nach der mutmaßlichen Straftat nicht mehr verwendet wird – könnte sie durch die in Kap. 3, A.I. dargestellten

434 Es wird bewusst nicht die Formulierung der „Auswertung von Blockchain-Inhalten verwendet", da die technischen Auswertungsmöglichkeiten nicht auf die Inhalte der Blockchain beschränkt sind, sondern sich insbesondere auch auf das Netzwerkverhalten bei Blockchain-Systemen beziehen.

Clustering-Methoden einer *Entität* zugeordnet werden, um so etwa die IP-Adresse zu ermitteln, mit der eine der anderen *Bitcoin-Adressen* der *Entität* genutzt wird. Anschließend könnte beim Internet-Access-Provider abgefragt werden, welcher Person diese IP-Adresse zugeordnet werden kann.[435]

Außerdem könnten etwa – ebenfalls unter Anwendung eines *Entitäts-Clustering*-Verfahrens –die Zahlungsströme der jeweiligen *Bitcoin-Adresse* bzw. der *Entität* nachverfolgt werden, um zu ermitteln, ob und wie ein Austausch der Bitcoin in Fiatgeld oder umgekehrt stattgefunden hat. Da die Zahlungsströme teilweise sehr komplex sind, ist es hier insbesondere möglich, diese graphisch darzustellen.[436] Diese (graphische) Nachverfolgung kann insbesondere durch die in Kap. 3, A.III.3. dargestellten auf künstlicher Intelligenz basierenden *Labelling*-Verfahren erweitert werden. Denn hierdurch könnte bestimmten, bisher unbekannten *Entitäten* etwa das Attribut eines *Exchange-Services* zugeschrieben werden, sodass einfacher erkennbar wird, an welcher Stelle die verdächtige *Bitcoin-Adresse* oder *Entität* Fiatgeld in Bitcoin oder umgekehrt umgetauscht hat. So wäre es für die Strafverfolgungsbehörden unter Umstände möglich, an die jeweiligen *Exchange-Anbieter* heranzutreten und die zugehörigen Kundendaten zu abzufragen, um die Identität zu ermitteln.[437]

Aus diesen Ermittlungsbeispielen ergibt sich, dass die in Kap. 3 dargestellten Auswertungsmethoden nicht getrennt voneinander betrachtet werden können, sondern 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.

---

435 Zur Zuordnung von (dynamischen) IP-Adressen zu natürlichen Personen nachfolgend ausführlich unter Kap. 4, B.I.b).

436 Siehe hierzu insbesondere das im Rahmen des EU-Forschungsprojektes TITANIUM entwickelte, bisher nur zu Forschungszwecken eingesetzte Ermittlungstool *GraphSense* (https://demo.graphsense.info letzter Abruf: 20. Dezember 2021), mit dem eine graphische Darstellung der Zahlungsströme insbesondere unter Anreicherung mit den aus anderen Verfahren gewonnen Erkenntnissen über bestimmte *Entitäten* möglich ist.

437 Dies setzt voraus, dass der jeweilige *Exchange-Service* in Deutschland bzw. in der EU ansässig ist. Hierauf und auf das nun für Kryptowährungsdienstleistungsanbieter geltende KYC-Prinzip (siehe hierzu das Gesetz zur Umsetzung der Änderungsrichtlinie der Vierten EU-Geldwäscherichtlinie, BGBl. 2602ff.) wird im Folgenden eingegangen.

B. Betroffene Grundrechte

Durch den Einsatz der soeben dargestellten Ermittlungsmöglichkeiten könnte ein Eingriff in verschiedene Grundrechte vorliegen. Da Gegenstand der Ermittlungsmöglichkeiten Daten aus Internetkommunikation sind, kommen insbesondere folgende Grundrechte in Betracht:

- Das Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) (hierzu unter I.),
- das Recht auf informationelle Selbstbestimmung (nachfolgend als „RiS" bezeichnet), abgeleitet aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[438] (hierzu unter II.),
- das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (nachfolgend als „IT-Grundrecht" bezeichnet), abgeleitet aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[439] (hierzu unter III.),

Außerdem kommen die speziellen und die allgemeine Verhaltensfreiheit(en) grundsätzlich in Betracht – je nachdem für welche Anwendung eine Blockchain konkret eingesetzt wird.[440] So wäre es beispielsweise grundsätzlich möglich, dass bei der Anwendung der Auswertungsmöglichkeiten bei einem blockchain-basierten sozialen Netzwerk[441] etwa auch ein Eingriff in die Meinungsfreiheit (Art. 5 Abs. 1 HS. 1 GG)[442] oder die allgemeine Verhaltensfreiheit vorliegt.

Bei der Anwendung der Auswertungsmethoden könnten daher, je nach Anwendungskontext der Blockchain, die Schutzbereiche folgender Verhaltensfreiheiten eröffnet sein:[443]

- Versammlungsfreiheit (Art. 8 GG)
- Berufsausübungsfreiheit (Art. 12 GG)
- Religionsfreiheit (Art. 4 GG)
- Meinungs-, Informations- und Kunstfreiheit (Art. 5 Abs. 1, Abs. 3 GG
- Allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG)

438 Siehe hierzu grundlegend BVerfGE 65, 1, 1ff.
439 Siehe hierzu grundlegend BVerfGE 120, 274, 302f.
440 Siehe hierzu etwa insbesondere die Ausführungen unter Kap. 2, C. zu weiteren Einsatzmöglichkeiten von Blockchains.
441 Siehe etwa das blockchain-basierte soziale Netzwerk *steemit* (https://steemit.com letzter Abruf: 20. Dezember 2021).
442 So etwa *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 176ff., 191ff.
443 Siehe ausführlich zur Eröffnung der Schutzbereiche bei sozialen Netzwerken *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 176ff., 191ff.

Fraglich ist allerdings, ob durch die Auswertung derartiger Inhalte ein Eingriff in diese Verhaltensfreiheiten vorliegen kann. Denn grundsätzlich wird die Möglichkeit der Nutzung – etwa von blockchain-basierten sozialen Netzwerken – nicht dadurch beeinträchtigt, dass eine staatliche Kenntnisnahme bzw. Auswertung stattfindet.[444] Das Ziel der dargestellten Auswertungsmethoden liegt eben nicht darin, die Nutzung von Blockchain-Systemen zu unterbinden, sondern darin, die in ihr enthaltenen Daten zur Kenntnis zu nehmen und auszuwerten. Insoweit stellt sich die Frage, ob eine derartige Kenntnisnahme bzw. Auswertung der Blockchain-Daten bereits einen Eingriff in die Verhaltensfreiheiten begründen kann.

Nach dem klassischen Eingriffsbegriff liegt ein Grundrechtseingriff vor bei einem Rechtsakt, „der unmittelbar und gezielt (final) durch ein vom Staat verfügtes, erforderlichenfalls zwangsweise durchzusetzendes Ge- oder Verbot, also imperativ, zu einer Verkürzung grundrechtlicher Freiheiten führt."[445] Die Anwendung der Auswertungsmethoden verfolgt aber weder das Ziel der Verkürzung der grundrechtlich geschützten Verhaltensfreiheiten noch wird der Staat hierbei durch ein Ge- oder Verbot tätig, sodass kein klassischer Eingriff in die Verhaltensfreiheiten vorliegt.[446]

Der mittlerweile vorherrschende moderne Eingriffsbegriff nimmt dagegen bereits einen Grundrechtseingriff bei jedem, dem Staat zurechenbaren Verhalten an, durch das grundrechtlich geschützte Positionen verkürzt werden.[447] Voraussetzungen eines Eingriffs sind dabei, dass ein grundrechtlich geschütztes Verhalten nicht mehr in vollem Umfang verwirklicht werden kann, diese Beeinträchtigungen dem Staat zurechenbar sind und eine gewisse Erheblichkeitsschwelle überschritten ist.[448]

Eine unmittelbare Verkürzung der aufgeführten Verhaltensfreiheiten liegt ebenfalls nicht durch die Anwendung der dargestellten Auswertungsmethoden vor, da die Blockchain-Systeme weiterhin in ihrer jeweiligen Anwendung genutzt werden können.[449]

444 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 237.
445 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 216 mit Verweis auf BVerfGE 105, 279 (300f.); *Oermann/Staben*, Der Staat 2013, 630 (637).
446 Siehe zur klassischen Eingriffswirkung bei der anlasslosen Internetaufklärung insbesondere *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 216; *Oermann/Staben*, Der Staat 2013, 630 (637).
447 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 216 m.w.N.
448 *Oermann/Staben*, Der Staat 2013, 630 (637) m.w.N.
449 Zur Eingriffsqualität von Online-Streifen *Oermann/Staben*, Der Staat 2013, 630 (640).

Insoweit kommt ein Eingriff in die Verhaltensfreiheiten allenfalls durch den mit der Anwendung der Auswertungsmethoden einhergehenden Abschreckungseffekt in Betracht.[450] Dass abschreckende Maßnahmen in gewisser Qualität einen Eingriff begründen können, ist von der Rechtsprechung anerkannt. Derartige abschreckende Maßnahmen sind dabei insbesondere das sog. „Gefährderschreiben", bei dem einem potenziell gewaltbereiten Fußballfan vor einem Fußballspiel, bei dem besondere Ausschreitungen zu erwarten sind, vorab in einem polizeilichen Schreiben mitgeteilt wird, dass er sich von der Veranstaltung fernhalten solle und andernfalls von der Polizei beobachtet werde.[451] Ähnliche Maßnahmen sind etwa die polizeiliche Begleitung einer Demonstration oder deren Übersichtsvideoüberwachung, sowie staatliche Warnungen.[452] Anerkannt ist insoweit, dass derartige, abschreckende Maßnahmen die vor der eigentlichen Verhaltensfreiheit vorgelagerte Willensentschließungsfreiheit betreffen und damit auch die jeweilige Verhaltensfreiheit.[453]

Daher stellt sich die Frage, ob durch die Anwendung der dargestellten Auswertungsmethoden eine derartig abschreckende Wirkung begründet wird, dass die vorgelagerte Willensentschließungsfreiheit in einer einen Eingriff begründenden Art und Weise betroffen ist.

Dem steht jedoch entgegen, dass bei der Anwendung der Auswertungsmethoden insoweit kein proaktives staatliches Handeln gegenüber dem Betroffenen stattfindet – die Blockchain-Inhalte werden lediglich passiv zur Kenntnis genommen, eine Aufforderung gegenüber dem Betroffenen wird dagegen nicht ausgesprochen. Ähnlich lässt sich einwenden, dass bei heimlichen bzw. verdeckten Maßnahmen, die der Betroffene nicht unmittelbar wahrnimmt, kein Abschreckungseffekt vorliegen kann.[454]

Dem Argument, dass ein Abschreckungseffekt nicht bestünde, wenn die Maßnahmen nicht wahrnehmbar seien, wird insbesondere entgegengehalten, dass bei verdeckten bzw. heimlichen Maßnahmen gerade ein sog. „panoptischer" Effekt erzeugt werde, der sich abschreckend auswirke.[455] Ein

450 Zur Eingriffsqualität von Abschreckungseffekten bei Online-Streifen *Oermann/Staben*, Der Staat 2013, 630 (640).
451 *Oermann/Staben*, Der Staat 2013, 630 (641f.) m.w.N.
452 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 218 m.w.N.
453 *Oermann/Staben*, Der Staat 2013, 630 (642f.).
454 *Oermann/Staben*, Der Staat 2013, 630 (644) mit Verweis auf das Sondervotum der Bundesverfassungsrichterin *Haas* zum Rasterfahndungsbeschluss BVerfGE 115, 320 (371f.).
455 *Oermann/Staben*, Der Staat 2013, 630 (644).

Abschreckungseffekt liege gerade darin, dass der Betroffene nicht wisse, ob und wann er beobachtet werde und daher sein Verhalten anpasse.[456]

Dem lässt sich für die Verhaltensfreiheiten im Bereich der Anwendung von Auswertungsmethoden bei Blockchain-Systemen insbesondere entgegenhalten, dass ein wesentlicher Bestandteil der Blockchain-Technologie die mittelbare öffentliche Verfügbarkeit aller verwalteten Transaktionsdaten ist. Insoweit muss derjenige, der aktiver Teilnehmer eines derartigen Blockchain-Systems sich darüber bewusst sein, dass all seine Aktivitäten von einer unbestimmten Anzahl weiterer Teilnehmer wahrgenommen werden können. Ein Abschreckungseffekt im Bereich der Verhaltensfreiheiten für den Einzelnen ergibt sich daher allenfalls aus der Technologie selbst und nicht aus der staatlichen Anwendung der Auswertungsmethoden.

Daher wäre auch die nachfolgend[457] ausführlich dargestellte Rechtsprechung des BVerfG im Volkszählungsurteil[458] widersprüchlich, wenn bereits durch die passive Kenntnisnahme die speziellen bzw. die allgemeine Verhaltensfreiheit(en) betroffen wären. Denn das BVerfG begründet die Notwendigkeit des Schutzes des RiS damit, dass zur freien Entfaltung der Persönlichkeit auch die Willensentschließungsfreiheit gehört und diese nur verwirklicht werden könne, wenn der Grundrechtsträger Kenntnis darüber hätte, welche Daten der Staat über ihn erhebt und verarbeitet. Plastisch ausgedrückt bedeutet dies, dass wenn bereits alle staatlichen Informationserhebungen mindestens die Willensentschließungsfreiheit als Teil der allgemeinen Handlungsfreiheit betreffen würden, der Schutz des RiS nicht notwendig wäre.

Aus diesen Gründen liegt durch die Anwendung der Auswertungsmethoden kein Eingriff in die speziellen oder die allgemeine Verhaltensfreiheit(en) vor.

I. Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG

Die in Kap. 3 dargestellten Auswertungsmethoden nutzen als Datengrundlage einerseits die Blockchain-Daten[459] und andererseits Informationen

456 *Oermann/Staben*, Der Staat 2013, 630 (644).
457 Siehe hierzu unter Kap. 4 B.II.1.
458 BVerfGE 65, 1ff.
459 Siehe hierzu Kap. 3 A.

über das Netzwerkverhalten der Beteiligten Nutzer[460], sowie Informationen, die aus anderweitigen, in der Regel allgemein zugänglichen, Quellen stammen.[461] Da diese Daten jeweils über das Internet übertragen und ausgetauscht werden, könnte durch die Auswertungsmethoden ein Eingriff in das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG vorliegen.[462]

Ob dies der Fall ist, wird nachfolgend dahingehend untersucht, dass zunächst der Schutzbereich des Telekommunikationsgeheimnis und die relevanten Schutzbereichsbegrenzungen dargestellt werden (hierzu unter 1.), um anschließend die Frage beantworten zu können, ob die ausgewerteten Daten von diesem Schutzbereich erfasst sind (hierzu unter 2.).

Dabei stellen sich folgende, wesentliche Probleme und Fragen:

- Wirkt es sich aus, dass in Blockchain-Systemen die Transaktionsnachrichten nach einem bestimmten, technischen Algorithmus automatisch weitergeleitet und so verbreitet werden?
- Liegt bei Blockchain-Inhalten eine fortlaufende oder bereits abgeschlossene Telekommunikation vor?
- Wie wirkt es sich aus, dass alle Transaktionen in Blockchain-Systemen öffentlich verfügbar sind?
- Kann das Verhindern eines bestimmten Telekommunikationsweges in den Schutzbereich des Telekommunikationsgeheimnisses fallen?

1. Schutzbereich

Art. 10 Abs. 1 GG schützt grundsätzlich die Vertraulichkeit der individuellen Kommunikation auf Distanz in den Ausprägungen des Brief-, Post- und Fernmeldegeheimnisses.[463]

Die grundrechtliche Gewährleistung des Fernmeldegeheimnisses, das in Literatur und Rechtsprechung auch als Telekommunikationsgeheimnis bezeichnet wird[464], schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsver-

460 Siehe hierzu Kap. 3 B.
461 Siehe hierzu Kap. 3 C.
462 Hierzu etwa ausführlich *Safferling/Rückert*, MMR 2015, 788 (792f.).
463 BVerfG NJW 2007, 351 (353); BeckOK-GG/*Ogorek* Art. 10 Rn. 13 ff; SSH-GG/*Guckelberger*, Art. 10 Rn. 5.
464 BeckOK-GG/*Ogorek* Art. 10 Rn. 35 mit Verweis auf BVerfGE 106, 28 (36).

kehrs.[465] Das Telekommunikationsgeheimnis soll Vertraulichkeit von Kommunikation auf Distanz gewährleisten, da die Beteiligten in der Regel auf Übermittler angewiesen sind und deshalb eine besonders hohe Gefahr des unberechtigten Zugriffs durch Dritte besteht.[466] Das Telekommunikationsgeheimnis soll insoweit die Privatsphäre auf Distanz ermöglichen[467] und nach Möglichkeit die Kommunikationsbeteiligten so stellen, als würden sie die Kommunikation in gegenseitiger Anwesenheit führen.[468] Dabei ist das Telekommunikationsgeheimnis für technikgestützte Telekommunikation entwicklungsoffen und erfasst auch neuartige Telekommunikationsmedien.[469] Insoweit ist auch die Fernkommunikation von informationstechnischen Systemen, die mit dem Internet verbunden sind, erfasst.[470]

Das Telekommunikationsgeheimnis soll die Abschirmung individueller Kommunikation gegenüber Dritten und dem Staat gewährleisten und dem Einzelnen insoweit eine „kommunikative[…] Privatheit"[471] ermöglichen.[472] Die individuelle Kommunikation des Einzelnen ist unter anderem Grundlage zur Entwicklung einer eigenen Persönlichkeit, sodass nach der Rechtsprechung des BVerfG durch das Telekommunikationsgeheimnis auch die freie Entfaltung der Persönlichkeit und damit auch die Würde des Menschen geschützt wird.[473]

Nicht nur aus den Kommunikations*inhalten,* sondern auch aus den Kommunikations*umständen* wie Art, Dauer, Kommunikationsbeteiligte und dem genutzten Kommunikationsmedium lassen sich Rückschlüsse auf das Privatleben und die Persönlichkeit des Betroffenen ziehen.[474] Insbesondere auf Grund der fortschreitenden, technischen Entwicklung, sind weit-

465 BVerfGE 67, 157 (172); BVerfGE 106, 28 (35f.); BVerfGE 115, 166, 182; BeckOK-GG/*Ogorek,* Art. 10 Rn. 36; SHH-GG/*Guckelberger,* Art. 10 Rn. 22; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 106.

466 BVerfGE 115, 166 (182); Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 69; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 196; *Bauer*, Soziale Netzwerke, S. 99f.

467 BVerfGE 115, 166 (182); *Bauer*, Soziale Netzwerke, S. 100.

468 BVerfGE 115, 166 (182); Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 59.

469 BVerfGE 115, 166 (182); BeckOK-GG/*Ogorek,* Art. 10 Rn. 37; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 64.

470 BVerfGE 120, 274 (307, 340).

471 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 58.

472 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 197.

473 BVerfGE 67, 157 (171); BVerfGE 115, 166 (182f.); *Bauer*, Soziale Netzwerke, S. 100; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 57.

474 BVerfGE 125, 260 (328); *Bauer*, Soziale Netzwerke, S. 100.

reichende Erkenntnisse aus den Daten der Telekommunikationsumstände möglich – wie etwa das Erstellen eines Bewegungsprofils durch die Auswertung der Standortdaten von Telekommunikation.[475] Auf Grund dieser weitreichenden Rückschlüsse sind auch die Kommunikations*umstände* eigenständiger Teilbereich des Schutzes von Art. 10 Abs. 1 GG.[476]

Das Telekommunikationsgeheimnis erstreckt sich außerdem unabhängig von der Qualität des Inhalts auf alle unkörperlichen Informationen, die mittels Telekommunikation übermittelt wurden und beim Empfänger reproduzierbar sind.[477]

Der Schutzbereich des Art. 10 Abs. 1 GG ist allerdings auf bestimmte Fernkommunikation bzw. deren Umstände begrenzt. Die für die Auswertungsmethoden relevanten Schutzbereichsbegrenzungen werden nachfolgend (hierzu unter a) – d)) dargestellt.

a) Schutzbereichsbegrenzung auf menschlich veranlasste Kommunikation

Der Schutzbereich des Art. 10 Abs. 1 GG ist nach dem BVerfG dahingehend eingeschränkt, dass Telekommunikation, die ausschließlich zwischen technischen Geräten stattfindet nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst ist.[478] Erforderlich ist nach dem BVerfG insoweit, dass ein menschlich veranlasster Informationsaustausch vorliegt, der sich auf Kommunikationsinhalte bezieht.[479]

Dieser Rechtsprechung des BVerfG lag die Frage nach dem Einsatz der sog. *IMSI-Catcher* zugrunde.[480] Mit deren Hilfe können Chip- und Gerätenummern von Mobiltelefonen ermittelt werden und darüber hinaus,

475 BVerfGE 125, 260 (328); *Bauer*, Soziale Netzwerke, S. 100.

476 So BVerfGE 125, 260 (328) mit der Begründung, dass „eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht [und deshalb] nicht ohne Weiteres davon ausgegangen werden [kann], dass der Rückgriff auf diese Daten grundsätzlich weniger wiegt als eine inhaltsbezogene Telekommunikationsüberwachung". BeckOK-GG/*Ogorek,* Art. 10 Rn. 38; *Bauer*, Soziale Netzwerke, S. 100.

477 *Bauer*, Soziale Netzwerke, S. 100 mit Verweis auf BVerfGE 106, 28 (36); BVerfG NJW 2000, 55 (56); BVerfGE 130, 151 (179); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 103.

478 BVerfG NJW 2007, 351 (353 Rn. 57); BVerfGE 130, 151 (179, 181); BVerfG NJW 2016, 3508 (3510 Rn. 38); SHH-GG/*Guckelberger,* Art. 10 Rn. 25.

479 BVerfG NJW 2007, 351 (353 Rn. 57); BeckOK-GG/*Ogorek,* Art. 10 Rn. 56f.

480 BVerfG NJW 2007, 351 (351).

Standortdaten von Mobilfunkgeräten.[481] Technisch wird hierzu eine virtuelle Funkzelle des Mobilfunkanbieters simuliert und nach einer sog. *IMEI* oder *IMSI-Gerätenummer*[482] durchsucht, um zu ermitteln, ob ein gesuchtes Gerät in einer bestimmten Funkzelle angemeldet ist.[483]

Das BVerfG hat dies nicht als Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG angesehen, da hier nur technische Geräte miteinander „kommunizieren" und deshalb nicht die für Art. 10 Abs. 1 GG erforderliche menschliche Kommunikation vorliege.[484]

Dieser Argumentation wird in der Literatur entgegengehalten, dass die Grundlage der Ermittlungsmöglichkeit gerade darin liegt, dass der Betroffene kommunikationsbereit sei.[485] Denn ein eingeschaltetes Handy verbindet sich grundsätzlich automatisch mit der nächstgelegenen Funkzelle und registriert sich dort entsprechend.[486] Um also von anderen potenziellen Kommunikationsteilnehmern erreicht werden zu können, muss der Betroffene zwangsläufig sein Handy einschalten, sich damit an einer Funkzelle anmelden und hierbei seine ungefähren Standortdaten übermitteln.[487]

Das BVerfG hält dem entgegen, dass das Aussenden der Daten aber unabhängig von konkreten Telekommunikationsvorgängen stattfinde und deshalb nur eine Sicherung der Betriebsbereitschaft vorliege und keine individuelle Kommunikation.[488] Weiterhin könne hierdurch aber das RiS betroffen sein, die Auswertung von vertraulicher Telekommunikation liege dagegen mangels konkreter Telekommunikationsvorgänge nicht vor.[489]

Da das Telekommunikationsgeheimnis seinem Schutzzweck nach vor dem Zugriff auf vertrauliche Telekommunikation von außen schützen

481 BVerfG NJW 2007, 351 (351); BeckOK-GG/*Ogorek,* Art. 10 Rn. 56; *Gercke*, MMR 2003, 453 (454f.).

482 Dies sind einmalig vergebene Gerätenummer mit denen sich Mobilfunkgeräte bei den Mobilfunkzellen des jeweiligen Anbieters anmelden, vgl. BVerfG NJW 2007, 351 (351ff.).

483 BVerfG NJW 2007, 351 (351f.); *Gercke*, MMR 2003, 453 (454f.); *Eisenberg/Singelnstein*, NStZ 2005, 62 (62f.).

484 BVerfG NJW 2007, 351 (351f.). Nach dem BVerfG soll allerdings hierdurch ein Eingriff in das RiS vorliegen, vgl. insoweit BVerfG NJW 2007, 351 (354f.).

485 *Nachbaur*, NJW 2007, 335 (336). Mit Kritik und weiteren Nachweisen hierzu aber im Ergebnis dem BVerfG zustimmend: Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 115; BeckOK-GG/*Ogorek,* Art. 10 Rn. 56.1.

486 BVerfG NJW 2007, 351 (351f.); *Gercke*, MMR 2003, 453 (454).

487 *Nachbaur*, NJW 2007, 335 (337).

488 BVerfG NJW 2007, 351 (353 Rn. 57).

489 BVerfG NJW 2007, 351 (354 Rn. 60).

soll[490], ist die einschränkende Rechtsprechung des BVerfG auf konkrete, menschlich veranlasste Telekommunikationsvorgänge konsequent und insoweit vorzugswürdig.

Dementsprechend ist für den Schutzbereich des Telekommunikationsgeheimnisses erforderlich, dass eine nicht nur zwischen technischen Geräten selbständig stattfindende Telekommunikation vorliegt, sondern mindestens, dass die Kommunikation auf einem menschlichen Veranlassen beruht.

b) Zeitliche Schutzbereichsbegrenzung – nur fortlaufende Telekommunikation

Außerdem ist der Schutzbereich des Telekommunikationsgeheimnisses auf fortlaufende Telekommunikation beschränkt.[491] Er ist nicht eröffnet, wenn die Telekommunikation bereits abgeschlossen ist und der Staat oder Dritte auf Inhalte abgeschlossener Telekommunikationsvorgänge zugreifen.[492] Hintergrund für diese Einschränkung ist, dass die Telekommunikationsteilnehmer für die Übermittlung der Telekommunikation in der Regel auf Dritte angewiesen sind und daher eine erhöhte Gefahr besteht, dass Dritte unberechtigt auf die Telekommunikation zugreifen (sog. spezifisches Übermittelungsrisiko). Gerade vor dieser Gefahr soll Art. 10 Abs. 1 GG schützen. Sie besteht aber in der Regel nicht mehr, wenn die Übermittlung bereits abgeschlossen ist.[493]

Nach der neueren Rechtsprechung des BVerfG besteht diese spezifische Übermittlungsgefahr allerdings weiterhin, wenn sich die Kommunikation außerhalb des Herrschaftsbereichs der Kommunikationsbeteiligten befindet.[494] Namentlich betraf dies im Urteil des BVerfG E-Mails, die auf dem Server eines E-Mail-Providers gespeichert waren.[495] Unerheblich sei nach dem BVerfG außerdem, ob die Kommunikation außerhalb des Herr-

490 BVerfGE 120, 274 (340f.).
491 BVerfGE 120, 274 (307f.); Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 124; Stern-Becker-GG/*Schenke,* Art. 10 Rn. 48.
492 BVerfGE 115, 166 (183ff.); BVerfGE 120, 274 (307f.); BeckOK-GG/*Ogorek,* Art. 10 Rn. 44.
493 BVerfGE 115, 166 (183ff.); BVerfGE 120, 274 (308); BeckOK-GG/*Ogorek,* Art. 10 Rn. 44.1.
494 BVerfG NJW 2009, 2431 (2432 Rn. 46); *Safferling/Rückert*, MMR 2015, 788 (792f.).
495 BVerfG NJW 2009, 2431 (2432 Rn. 46).

schaftsbereich der Betroffenen zwischen- oder endgespeichert werden.[496] Es komme somit maßgeblich darauf an, ob auf Grund der faktischen Herrschaftsverhältnisse über die Daten die Gefahr eines Zugriffs durch Dritte bestehe.[497]

Maßgeblich für die zeitliche Bewertung der fortlaufenden Telekommunikation ist außerdem nicht der Zeitpunkt des Zugriffs auf die Telekommunikation, sondern der Zeitpunkt des jeweiligen Datenanfalls.[498] Erforderlich ist insoweit nicht, dass ein staatlicher Zugriff auf laufende Kommunikation vorliegt, sondern ausreichend ist der Zugriff auf Daten, die durch eine laufende Kommunikation angefallen sind.[499] Zur Begründung hierzu führt *Durner* einen Vergleich mit dem Postgeheimnis an und legt dar, dass auch dann der Schutzbereich des Telekommunikationsgeheimnisses eröffnet ist, wenn der Staat einen Postboten nach Empfänger und Absender eines Briefs fragt, wenn der Brief schon zugestellt ist.[500]

Ähnlich kommt auch das BVerfG zu dem Ergebnis, dass etwa bei der Zuordnung einer dynamischen IP-Adresse zu einem Kunden eines Telekommunikationsanbieters ein Eingriff in Art. 10 Abs. 1 GG vorliegt, da hier konkrete Telekommunikationsverbindungen in einem Zwischenschritt gesichtet werden müssen, um eine dynamische IP-Adresse einem bestimmten Kunden zuzuordnen.[501] Diese Kommunikationsverbindungen sind zum Zeitpunkt der Abfrage in der Regel bereits abgeschlossen, die gesichteten Verbindungsdaten aber bei konkreten Telekommunikationsverbindungen angefallen.[502]

Zeitlich erstreckt sich der Schutzbereich des Art. 10 Abs. 1 GG darüber hinaus auch auf die im Anschluss an die Erhebung von geschützter Telekommunikation stattfindende Auswertung dieser Telekommunikation.[503] Insoweit erstreckt sich der Schutz des Telekommunikationsgeheimnisses

496 BVerfG NJW 2009, 2431 (2432 Rn. 46); *Safferling/Rückert*, MMR 2015, 788 (792f.).
497 BVerfG NJW 2009, 2431 (2432 Rn. 46). Ähnlich insoweit *Safferling/Rückert*, MMR 2015, 788 (793), die auf einen normativ geprägten Telekommunikationsbegriff abstellen, nach dem maßgeblich sei, ob die Daten außerhalb des Herrschaftsbereich eines Telekommunikationsteilnehmers gespeichert sind.
498 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 85 mit Verweis auf BVerfGE 120, 274 Ls. 4.
499 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 85.
500 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 85.
501 BVerfGE 130, 151 (181).
502 So die Begründung von Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 85.
503 BVerfG NJW 2000, 55 (Ls. 1, 57).

auch auf die an die Erhebung der Telekommunikationsdaten anschließenden Informations- und Datenverarbeitungsprozesse.[504]

c) Schutzbereichsbegrenzung auf Individualkommunikation

Der Schutzbereich des Telekommunikationsgeheimnisses ist außerdem dahingehend eingeschränkt, dass Telekommunikation, die sich an die Allgemeinheit richtet – also einen unbestimmten Adressatenkreis – nicht erfasst wird.[505] Hintergrund ist, dass Art. 10 Abs. 1 GG die Vertraulichkeit von Kommunikation schützen soll.[506] Bei Kommunikation, die sich an einen unbestimmten Adressatenkreis richtet, kann deren Vertraulichkeit dagegen nicht erwartet werden.[507] Insoweit wird der Schutzbereich des Telekommunikationsgeheimnisses auf individuelle Telekommunikation beschränkt und dadurch vom Schutzbereich anderer Kommunikationsgrundrechte abgegrenzt.[508] Vom Schutzbereich des Telekommunikationsgeheimnisses ist deshalb nur die Telekommunikation, die sich an einen *individuellen* Adressatenkreis richtet, erfasst, ausgenommen ist Telekommunikation, die sich an einen *nicht weiter abgrenzbaren* Adressatenkreis richtet.[509]

(1) Abgrenzungsschwierigkeiten bei Internetkommunikation als Massen- oder Individualkommunikation

Für Telekommunikation im Internet kann diese Abgrenzung problematisch sein, denn im Internet werden einerseits grundsätzlich immer individuelle Kommunikationsbeziehungen aufgebaut, andererseits kann mittels dieser individuellen Kommunikationsbeziehungen auch Telekommunikation

504 BVerfG NJW 2000, 55 (57).
505 BeckOK-GG/*Ogorek,* Art. 10 Rn. 40; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 70; Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43; *Bauer*, Soziale Netzwerke, S. 100.
506 SHH-GG/*Guckelberger,* Art. 10 Rn. 22; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 70.
507 SHH-GG/*Guckelberger,* Art. 10 Rn. 22.
508 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 70.
509 BeckOK-GG/*Ogorek,* Art. 10 Rn. 40.

übertragen werden, die sich an einen unbestimmten Adressatenkreis richtet.[510] Das verdeutlicht folgendes, technisch vereinfachtes Beispiel:

Wenn etwa ein Radiosender über das Internet „gestreamt" wird, baut der Nutzer, der das Radio „streamt", einerseits eine individuelle Kommunikationsbeziehung zum Server des Radioanbieters auf.[511] Hierzu dienen die grundsätzlich individuell vergebenen[512] IP-Adressen der mit dem Internet verbundenen Rechner – sie funktionieren ähnlich wie herkömmliche Postanschriften, sodass die Beteiligten einer Kommunikationsbeziehung wissen, an wen welche Daten zu versenden sind.[513] Der „streamende" Nutzer fragt also mit seiner IP-Adresse beim Server des Radioanbieters an, ob der Radioanbieter seine Inhalte an die IP-Adresse des „streamenden" Nutzers versenden kann. Der Server registriert diese Anfrage und sendet die angefragten Datenpakete (im konkreten Fall dann die Radioübertragung) an die IP-Adresse des Nutzers.[514] So entsteht eine individuelle Kommunikationsbeziehung zwischen „streamendem" Nutzer und Radioanbieter. Andererseits richtet sich das Rundfunkangebot des Radioanbieters natürlich an jeden Interessierten mit einem Internetzugang – also an einen nicht weiter abgrenzbaren Adressatenkreis – ähnlich wie beim herkömmlichen Rundfunk.[515] Der Radioanbieter baut insoweit zu jedem „Hörer" eine individuelle Kommunikationsbeziehung auf.[516]

510 *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104; *Bauer*, Soziale Netzwerke, S. 101; SHH-GG/*Guckelberger,* Art. 10 Rn. 22; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 120.

511 Vgl. *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104.

512 Dass IP-Adressen individuell vergeben werden, ist technisch stark vereinfacht. Sie ermöglichen aber u.a. einerseits die individuelle Adressierung beim Versand von Datenpakten in Rechnernetzwerken und andererseits die Identifizierung natürlicher Personen über die Abfrage bei Telekommunikationsanbietern. Vgl. hierzu die Ausführungen des BVerfG zur Einordnung von dynamischen IP-Adressen, BVerfG NJW 2012, 1419 (1420ff.).

513 Vgl. hierzu ausführlich *Meinel/Sack*, Digitale Kommunikation, S. 146ff. Ähnlich auch *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 44f, die ausführlich den Ablauf der Kommunikation in vernetzten Rechnersystemen darstellt.

514 Vgl. hierzu die ausführliche Darstellung von *Bauer*, Soziale Netzwerke, S. 41f., der sich außerdem insbesondere mit der technischen Architektur bei der Kommunikation mit und über soziale Netzwerke auseinandersetzt.

515 Allgemein hierzu *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104.

516 Entsprechend insbesondere auch *Bauer*, Soziale Netzwerke, S. 41f., 101; *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104.

Ähnliches gilt etwa auch für Kommunikationsbeziehungen in und mit sozialen Netzwerken[517]: einerseits wird durch das Aufrufen der Facebook-Seite eine individuelle Kommunikationsbeziehung zwischen dem Rechner eines Facebook-Nutzers und dem Facebook-Server hergestellt.[518] Andererseits kann der Nutzer aber mittels dieser Kommunikationsbeziehung auf Facebook etwa Urlaubsbilder veröffentlichen und sie so einem unbestimmten Adressatenkreis zugänglich machen, wenn er sie „öffentlich postet"[519]. Insoweit bestehen bereits beim einfachen „Posten" von Beiträgen in sozialen Netzwerken oder Diskussionsforen zwei voneinander zu unterscheidende Kommunikationsbeziehungen – einerseits die individuelle Kommunikationsbeziehung des Nutzers mit dem Facebook-Server und andererseits die Kommunikationsbeziehung mit einem unbestimmten Adressatenkreis, die durch das „Posten" von Beiträgen initiiert werden.[520]

Deshalb stellt sich die Frage, ob und welche Kommunikationsbeziehungen im Internet unter den Schutzbereich des Telekommunikationsgeheimnisses fallen. Hierzu werden die folgenden unterschiedlichen Ansichten vertreten.[521]

(2) Rechtsprechung des BVerfGE

i. BVerfGE 120, 274 ff. – Online-Durchsuchungsvorschriften des Verfassungsschutzgesetzes NRW (VSG NRW)

In seinem Urteil zu den Online-Durchsuchungsvorschriften des VSG NRW führt das BVerfG aus, das Telekommunikationsgeheimnis schütze auch die „mit einem an das Internet angeschlossenen informationstechnischen System geführte laufenden Fernkommunikation"[522]. Das Grundrecht aus Art. 10 Abs. 1 GG schütze aber nur davor, dass die Telekommunikation, die ein Einzelner über das Internet führe, nicht „von Dritten zur Kenntnis

517 *Bauer*, Soziale Netzwerke, S. 41f., 101.
518 *Bauer*, Soziale Netzwerke, S. 43ff. m.w.N.
519 *Bauer*, Soziale Netzwerke, S. 43ff. m.w.N.; Vgl. zu Funktionen und Ablauf von Kommunikation in sozialen Netzwerken ausführlich *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 97ff. m.w.N.
520 *Bauer*, Soziale Netzwerke, S. 43ff.
521 Ähnlich *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 103; *Bauer*, Soziale Netzwerke, S. 101.
522 BVerfGE 120, 274 (340).

genommen wird“[523] – das Telekommunikationsgeheimnis schütze dagegen nicht das „personengebundene Vertrauen“[524] der Kommunikationspartner zueinander und damit auch nicht davor, dass eine staatliche Stelle sich in eine Kommunikationsbeziehung zu einem Einzelnen begäbe.[525]

Maßgebliches Abgrenzungskriterium für einen Eingriff in Art. 10 Abs. 1 GG soll insoweit sein, ob der Staat „unautorisiert“ auf Telekommunikation zugreife.[526] So soll bei der staatlichen Kenntnisnahme von Telekommunikation nur dann ein Eingriff vorliegen, wenn der Staat die Kommunikation „von außen“ überwache, „ohne selbst Kommunikationsadressat zu sein“[527].

Der Zugriff auf Telekommunikation ist nach dem BVerfG zunächst „autorisiert“, wenn der Staat auf dem technisch dafür vorgesehenen Weg Kenntnis von allgemein zugänglichen Inhalten nimmt.[528] Denn bei allgemein zugänglichen Inhalten sei jedermann autorisiert, die Inhalte abzurufen.[529] Typische Beispiele für einen derartigen Zugriff sind der Aufruf von allgemein zugänglichen Internetseiten (etwa Google oder auch Diskussionsforen).[530]

Autorisiert sei eine staatliche Stelle ebenfalls, wenn auf dem technisch dafür vorgesehenen Weg auf Telekommunikation zugegriffen werde und die staatliche Stelle hierzu von einer von mehreren der Kommunikationsbeteiligten „autorisiert“ sei.[531] Erforderlich sei allerdings, dass der Kommunikationsteilnehmer die staatliche Stelle willentlich autorisiert habe.[532] Typisches Beispiel ist, dass einer der Teilnehmer eines passwortgeschützten Chat-Forums sein Passwort an eine staatliche Stelle weitergibt.[533] Das BVerfG begründet dies damit, dass Art. 10 Abs. 1 GG nur die Vertraulich-

523 BVerfGE 120, 274 (340).
524 BVerfGE 120, 274 (340) mit Verweis auf BVerfGE 106, 28 (37f.).
525 BVerfGE 120, 274 (341).
526 BVerfGE 120, 274 (340). Hierzu auch *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 106; *Bauer*, Soziale Netzwerke, S. 102f.
527 BVerfGE 120, 274 (341).
528 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
529 *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107, der noch auf den theoretischen Fall eingeht, dass der Staat einen allgemein zugänglichen Server mittels Online-Durchsuchung infiltriert und so ein Eingriff in Art. 10 Abs. 1 GG vorliegen würde, da in diesem Fall kein Zugriff „auf dem technisch dafür vorgesehenen Weg“ erfolgt.
530 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107. Beispielsweise: https://www.gutefrage.net (letzter Abruf: 20. Dezember 2021).
531 BVerfGE 120, 274 (341). *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
532 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
533 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.

keitserwartung in das Kommunikationsmedium schütze, nicht aber das „personengebundene Vertrauen“[534]. Wenn aber einer der Teilnehmer einer passwortgeschützten Telekommunikation sein Passwort herausgebe, werde eben das personengebundene Vertrauen und nicht das Vertrauen in das Kommunikationsmittel enttäuscht.[535]

Dagegen liegt nach dem BVerfG keine Autorisierung und damit ein Eingriff in Art. 10 Abs. 1 GG vor, wenn der Staat auf Inhalte oder Umstände von Internetkommunikation ohne oder gegen den Willen der Kommunikationsbeteiligten zugreift.[536] Maßgebliches Beispiel des BVerfG ist der Zugriff auf passwortgeschützte Telekommunikation durch ein mittels „Keylogging“[537] erhobenes Passwort.[538]

ii. BVerfG NJW 2016, 3508 ff. – Überwachung der Internetnutzung im Ermittlungsverfahren

Dementsprechend nimmt das BVerfG auch für die strafprozessuale Ermittlungsmaßnahme der Überwachung der Internetnutzung nach § 100a StPO – unter anderem also die Ermittlung, welche Internetseiten der Betroffene wann aufgerufen hat – an, dass in diesem Fall ein Eingriff in das nach Art. 10 Abs. 1 GG geschützte Telekommunikationsgeheimnis vorliege.[539] Nach dem BVerfG käme es maßgeblich darauf an, dass „Informationen körperlos befördert [würden] […] am Empfangsort wieder erzeugt werden“[540] könnten und diese körperlose Übermittlung an „einen individuellen Rezipienten“[541] erfolge. Bei einem „empfängergesteuerten Abruf von Informationen aus dem Netz“[542] seien diese Voraussetzungen erfüllt, wenn der Betroffene die Informationen „vertraulich wissen“[543] wolle.

534 BVerfGE 120, 274 (341).
535 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
536 BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
537 Keylogging ist eine Hard- oder Software, mit der es möglich ist, die Tastatureingaben an einem Computer zu protokolieren. BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.
538 BVerfGE 120, 274 (341).
539 BVerfG NJW 2016, 3508 (3510 Rn. 39).
540 BVerfG NJW 2016, 3508 (3510 Rn. 35).
541 BVerfG NJW 2016, 3508 (3510 Rn. 38).
542 BVerfG NJW 2016, 3508 (3510 Rn. 38) unter Verweis auf *Singelnstein*, NStZ 2012, 593 (594).
543 BVerfG NJW 2016, 3508 (3510 Rn. 37).

iii. Zwischenergebnis – Rechtsprechung des BVerfG zum Telekommunikationsgeheimnis

Für die oben[544] dargestellten Kommunikationsbeziehungen im Internet bedeutet die Rechtsprechung des BVerfG, dass immer dann ein Eingriff in den Schutzbereich des Telekommunikationsgeheimnis vorliegt, wenn Kommunikations*inhalte* oder *-umstände* von außen zur Kenntnis genommen werden, die nicht ohne Weiteres für jeden Dritten zur Kenntnis genommen werden können. Maßgeblich ist damit der Zugriff auf die Telekommunikation durch den Staat und nicht die Telekommunikationsbeziehung der Betroffenen.[545]

(3) Literatur-Ansichten

In der Literatur werden diese Ausführungen des BVerfG unterschiedlich bewertet bzw. gedeutet und teilweise abweichende Auffassungen vertreten.[546]

i. Zugangssicherungen als Indiz für Individualkommunikation

Durner vertritt etwa die Auffassung, das maßgebliche Abgrenzungskriterium für das Vorliegen von Individualkommunikation sei das Bestehen von „Zugangshindernisse[n]"[547]. Allerdings soll das Vorliegen eines Zugangshindernisses nur ein „Indiz"[548] für geschützte Individualkommunikation begründen, da auch zugangsgesicherte Kommunikationsformen bestehen können, die sich nicht zum Schutz von Geheimnissen eignen und deshalb „letztlich für die Allgemeinheit bestimmt [seien]"[549]. Insoweit muss nach *Durner* für den Schutzbereich des Art. 10 Abs. 1 GG eine ausreichende

544 Siehe hierzu unter Kap. 4 B.I.1.c).(1)
545 So insbesondere *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104, 110; *Bauer*, Soziale Netzwerke, S. 103f.
546 Siehe hierzu etwa *Bauer*, Soziale Netzwerke, S. 101, der die vertretenen Ansichten einerseits in ein Konzept der „Zugangssicherung" und andererseits ein „Autorisierungskonzept" gruppiert.
547 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 94 mit Verweis auf *Britz*, DÖV 2008, 411 (414). So auch BeckOK-GG/*Ogorek* GG Art. 10 Rn. 40 mit Verweis auf *Durner* (s.o.).
548 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 122.
549 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 122.

Zugangssicherung bestehen, um den Schutz von „Geheimnissen" zu gewährleisten.[550] Da also auch ein wertendes Kriterium (der hinreichende Geheimnisschutz) maßgeblich für die Abgrenzung ist, nimmt *Durner* außerdem an, dass bei Unsicherheiten im Einzelfall der Schutzbereich des Art. 10 Abs. 1 GG als eröffnet anzusehen sei.[551]

ii. Individuelle Adressierung der Nachricht

Eine ähnliche Ansicht, die ebenfalls auf die Art und Weise der geführten Telekommunikation abstellt, vertritt *Schenke* und grenzt Massen- von Individualkommunikation danach ab, ob „eine Nachricht individuell so adressiert wird, dass sie eigenständig in einen dem Empfänger zugeordneten Herrschaftsbereich gelangt"[552]. So kommt *Schenke* zu dem Ergebnis, dass jedenfalls der „E-Mail-Verkehr"[553] Individualkommunikation sei, „die Veröffentlichung von Daten auf einer Homepage im frei zugänglichen Internet"[554] dagegen nicht. Außerdem soll auch bei der Nutzung eines „Cloud-Dienstes zur Datensynchronisation"[555] keine Individualkommunikation vorliegen, da es an einem vom Nutzer zu unterscheidenden Adressaten der Telekommunikation fehle.[556]

iii. Inhalte, die für jedermann zugänglich sind

Dagegen stellt *Guckelberger,* ähnlich wie das BVerfG, nicht auf die Art und Weise der Telekommunikation ab, sondern darauf, wie und für wen diese

550 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 122.

551 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 123, der damit dem nachfolgenden Argument (hierzu unter (4)) entgegentreten will, dass ansonsten erst auf die Telekommunikation zugegriffen werden müsste, um zu ermitteln, ob ein Grundrechtseingriff vorliegt.

552 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43.

553 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43.

554 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43 mit Verweis auf BGHZ 208, 82 (109), in dem der BGH annimmt, dass sich ein Download-Angebot im frei zugänglichen Internet an einen unbestimmten Adressatenkreis richte und damit öffentlich sei.

555 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 44.

556 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 44 mit Verweis auf BVerfGE 125, 260 (309); 141, 220 (316). Ähnlich auch SHH-GG/*Guckelberger,* Art. 10 Rn. 24, die den Schutzbereich nur dann als eröffnet ansieht, wenn das Cloud-Computing für Kommunikationszwecke eingesetzt wird.

verfügbar bzw. erkennbar ist – für die Allgemeinheit bzw. für jedermann oder einen eingeschränkten Personenkreis.[557]

Dabei begründet *Guckelberger* ihre Ansicht mit dem technologischen Wandel und den damit einhergehenden gesellschaftlichen Veränderungen und vergleicht die im Internet geführte Kommunikation wertungsmäßig mit der herkömmlichen Telekommunikation mittels Telefon.[558] *Guckelberger* begründet insoweit ihre Auffassung mit dem einfachen Beispiel, dass der Abruf von Internetseiten heutzutage vielfach den individuellen telefonischen Anruf ersetze.[559]

Maßgebliches Abgrenzungskriterium ist nach dieser Auffassung also, welche Informationen der Allgemeinheit zur Verfügung stehen.[560]

Hiernach kommt *Guckelberger* zu der Differenzierung, dass zwar die von einer öffentlichen Internetseite abrufbaren Informationen allgemein zugängliche seien und damit keine Individualkommunikation, dass aber gerade nicht für jedermann erkennbar sei, wer welche Internetseiten aufrufe.[561] Deshalb könne zwar der Inhalt der Internetseite nicht geschützte Massenkommunikation sein, dass der Einzelne eine oder mehrere Internetseiten aufrufe, müsse dagegen vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sein, da dies gerade nicht von jedermann erkennbar sei.[562]

(4) Auseinandersetzung mit den vorstehenden Ansichten

Die vorstehenden Ansichten lassen sich in zwei unterschiedliche Ansätze gruppieren.

So stellen *Durner* und *Schenke* vorrangig auf die Art und Weise der geführten Telekommunikation ab.[563] Dagegen stellen das BVerfG[564] und

557 SHH-GG/*Guckelberger,* Art. 10 Rn. 22. So insbesondere auch *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107f. Ähnlich auch *Rückert*, ZStW 129 (2017), 302 (311f.) der sich insbesondere damit auseinandersetzt, welchen Aufwand ein Ermittler betreiben muss, um die jeweiligen Daten einsehen zu können.

558 SHH-GG/*Guckelberger,* Art. 10 Rn. 22.

559 SHH-GG/*Guckelberger,* Art. 10 Rn. 22.

560 SHH-GG/*Guckelberger,* Art. 10 Rn. 22. Ähnlich insoweit auch *Rückert*, ZStW 129 (2017), 302 (311f.).

561 SHH-GG/*Guckelberger,* Art. 10 Rn. 22 mit Verweis auf BVerfG NJW 2016, 3508.

562 SHH-GG/*Guckelberger,* Art. 10 Rn. 22 mit Verweis auf BVerfG NJW 2016, 3508.

563 Siehe hierzu bereits oben unter Kap. 4 B.I.1.c)(3)i.,ii. m.w.N.

564 Siehe hierzu bereits oben unter Kap. 4 B.I.1.c)(2) m.w.N.

Guckelberger[565] auf die Art und Weise der Verfügbarkeit der Kommunikation bzw. des Zugriffs auf die Telekommunikation ab. Einerseits wird also auf die Perspektive des Kommunikationsbeteiligten abgestellt, andererseits auf die Perspektive des Zugreifenden.[566]

Allen Ansichten zugrunde liegt dagegen die Frage, wann ein Kommunikationsteilnehmer nicht mehr davon ausgehen darf, dass die von ihm geführte Telekommunikation vertraulich ist. Unterschiedlich sind dabei nur die Ansätze der Bewertung dieser Frage, die einerseits beim Kommunikationsteilnehmer und den von ihm ergriffenen Schutzmaßnahmen ansetzen[567] und andererseits bei der Frage, wie der Staat bzw. ein Dritter hierauf zugreifen kann.[568]

Für das Abstellen auf die vom Kommunikationsteilnehmer ergriffenen Schutzmaßnahmen könnte sprechen, dass der Betroffene nur dann die Vertraulichkeit seiner Kommunikation erwarten kann, wenn er hierfür aktiv Maßnahmen zum Schutz der Vertraulichkeit ergreift – er kann Vertraulichkeit nur erwarten, wenn er sich bewusst hierfür entscheidet. Dem steht allerdings entgegen, dass auch bei der herkömmlichen Fernkommunikation keine aktiven Schutzmaßnahmen zur Gewährleistung der Vertraulichkeit erforderlich sind, damit der Schutzbereich des Art. 10 Abs. 1 GG eröffnet ist.[569] So ist etwa auch die unverschlossene Postkarte vom Briefgeheimnis des Art. 10 Abs. 1 GG erfasst.[570] Außerdem wäre sonst etwa beim herkömmlichen Telefonieren die Telekommunikation nur dann von Art. 10 Abs. 1 GG geschützt, wenn die Kommunikationsbeteiligten eine Geheimsprache oder andere Schutzmaßnahmen zur Wahrung der Vertraulichkeit ergreifen würden.[571]

Nachvollziehbar ist zwar, dass die Bewertung anhand der Perspektive der Kommunikationsteilnehmer vorgenommen wird, denn die Frage, ob

565 Siehe hierzu bereits oben unter Kap. 4 B.I.1.c)(3)iii. m.w.N.

566 So auch *Bauer*, Soziale Netzwerke, S. 101f., der sich intensiv mit der von *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 106ff. vertretenen Ansicht unter Berücksichtigung des Urteils BVerfGE 120, 274 (341) auseinandersetzt und *Bäckers* Wertung als einen Perspektivwechsel bezeichnet.

567 So etwa Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 122f.

568 So auch *Bauer*, Soziale Netzwerke, S. 101f.

569 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 93; Stern-Becker-GG/*Schenke,* Art. 10 Rn. 31.

570 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 93; Stern-Becker-GG/*Schenke,* Art. 10 Rn. 31.

571 Ausreichend dürfte hier wohl auch der Vertrag mit dem Telekommunikationsanbieter sein. Insoweit dienen die Beispiele nur zur Verdeutlichung der Argumentation.

Individual- oder Massenkommunikation vorliegt, kann insbesondere auch danach beurteilt werden, ob der Betroffene die Intention hatte, sich an einen individuellen Adressaten oder einen unbestimmten Adressatenkreis zu richten.[572] Diese Abgrenzung differenziert aber nicht zwischen den verschiedenen Kommunikationsebenen im Internet.[573] Denn wie oben dargestellt[574], gibt es im Internet einerseits die Kommunikation, die jeweils unmittelbar zwischen den einzelnen Rechnern stattfindet und andererseits die Kommunikation, die durch diese Verbindung mit anderen vermittelt wird.[575] Die von *Durner* und *Schenke* vertretenen Ansichten gehen insoweit nicht konkret darauf ein, wie diese unterschiedlichen Kommunikationsbeziehungen im Internet zu bewerten sind. Zwar wäre es auch möglich, mit den vorgestellten Ansätzen eine Bewertung der einzelnen Kommunikationsbeziehungen vorzunehmen. So ließe sich bei dem von *Durner* vertretenen Ansatz etwa begründen, dass zwar kein Zugangshindernis besteht, wenn der Staat „Google" aufruft, ein solches aber wohl dann gegeben sein dürfte, wenn der Staat zur Kenntnis nimmt, wer „Google" aufgerufen hat. Denn dies kann zunächst nur der jeweilige Telekommunikationsanbieter bzw. der Betreiber der Internetseite[576] einsehen. Dementsprechend könnte man ein faktisches Zugangshindernis annehmen. Eine ähnliche Begründung wäre auch bei der von *Schenke* vertretenen Ansicht möglich, denn das Allgemeine Angebot von „Google" ist insoweit nicht individuell adressiert, sobald aber ein konkreter Aufruf der Seite vorliegt, besteht eine individuelle Adressierung der abgerufenen Kommunikationsinhalte. Problematisch ist hieran allerdings, dass diese Auslegung beider Ansichten nicht eindeutig ist. So könnte die von *Schenke* vertretene Auffassung auch dahingehend verstanden werden, dass es auf den Inhalt der jeweiligen Kommunikation ankommt und ob diese individuell adressiert ist. So wäre etwa der Aufruf von „Google" insgesamt nicht hinreichend individuell adressiert, da sich das Angebot von Google grundsätzlich an einen unbestimmten Personenkreis richtet. Ähnlich ließe sich auch die von *Durner* vertretene Ansicht dahin

572 So insbesondere Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43. Insoweit ähnlich ist die typische Abgrenzung zwischen Telekommunikationsgeheimnis und anderen Kommunikationsrechten bei Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 70.

573 Hierzu bereits *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 104.

574 Siehe hierzu unter Kap. 4 B.I.1.c).

575 Vgl. insoweit *Bauer*, Soziale Netzwerke, S. 41ff.

576 Der Betreiber der Internetseite kann im Grundsatz allerdings nur einsehen, welche IP-Adresse auf die Internetseite zugegriffen hat, vgl. hierzu *Bauer*, Soziale Netzwerke, S. 41.

verstehen, dass sich etwa der Aufruf von „Google" nicht zum Schutz von Geheimnissen eignet und daher trotz bestehendem tatsächlichen Zugangshindernis keine von Art. 10 Abs. 1 GG geschützte Individualkommunikation vorliege, wenn staatliche Behörden den Abruf von „Google" zur Kenntnis nehmen. Insoweit besteht weiterhin das Problem, dass diese Ansichten die unterschiedlichen Kommunikationsbeziehungen im Internet nicht hinreichend trennscharf voneinander abgrenzen und beurteilen.

Außerdem soll Art. 10 Abs. 1 GG vor dem spezifischen Übermittlungsrisiko schützen – also vor dem unberechtigten *Zugriff* durch Dritte – das in der Regel bei Fernkommunikation besteht.[577] Insoweit legt auch der Schutzzweck des Art. 10 Abs. 1 GG nahe, auf den Modus des Zugriffs abzustellen und nicht auf die Art und Weise der geführten Fernkommunikation.

Problematisch ist darüber hinaus an der von *Schenke* vertretenen Ansicht, dass die Nutzung von Cloud-Diensten zur Datensynchronisation nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sein soll.[578] Auch wenn die Argumentation, dass hierbei kein vom Absender zu unterscheidender Adressat vorliege, grundsätzlich nachvollziehbar ist, würde sie zu einem widersprüchlichen Ergebnis kommen, wenn man sie auf die analoge Welt übertragen würde: dann wäre nämlich ein Brief, den eine Person an sich selbst, aber an eine andere Adresse verschicken würde, nicht vom Postgeheimnis geschützt. Auch dieses Ergebnis kann zwar noch nachvollziehbar sein, da Art. 10 Abs. 1 GG gerade nur Kommunikation schützen soll und keine Kommunikation vorliegt, wenn Empfänger und Adressat personenidentisch sind. Das würde aber dazu führen, dass zunächst die Umstände der konkreten Kommunikation wahrgenommen werden müssten, um zu ermitteln, dass die „Kommunikationsbeteiligten" personenidentisch sind. Insoweit müsste erst in den Schutzbereich des Art. 10 Abs. 1 GG in Form der Kommunikationsumstände eingegriffen werden, um beantworten zu können, ob ein Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG in Form des Kommunikationsinhalts vorliegt. Dieses Beispiel und seine Argumentation lässt sich auch auf den Schutzbereich des Telekommunikationsgeheimnisses übertragen. Denn von außen dürfte bei der Telekommunikation zwischen zwei verschiedenen IP-Adressen (beispielsweise bei einem genutzten

577 Siehe hierzu bereits unter Kap. 4, B.I.1.b).

578 Stern-Becker-GG/*Schenke,* Art. 10 Rn. 43. So auch SHH-GG/*Guckelberger,* Art. 10 Rn. 24 nach der allerdings der Schutzbereich eröffnet ist, soweit das Cloud-Computing für Kommunikationszwecke genutzt wird. Ähnlich auch BeckOK-GG/*Ogorek,* Art. 10 Rn. 41f.

Laptop und einem Handy, zwischen denen Daten automatisch über die Cloud ausgetauscht werden) zunächst einmal nicht erkennbar sein, dass beide IP-Adressen von der gleichen natürlichen Person genutzt werden. Insoweit stellt die von *Schenke*[579] vertretene Ansicht eher auf eine *ex post* Perspektive ab und bewertet die Frage nach dem Schutz des Art. 10 Abs. 1 GG auf der Grundlage der bereits ermittelten Kommunikation.

Insgesamt liegt den Ansichten, die die Abgrenzung aus der Perspektive der Kommunikationsbeteiligten beurteilen[580], das Problem zugrunde, dass eine trennscharfe Abgrenzung nicht anhand der verwendeten Kommunikationsmedien vorgenommen werden kann, sondern nur vorgenommen werden kann, wenn der Inhalt oder die Umstände der Kommunikation bereits ermittelt wurden. Dies setzt aber in der Regel bereits einen Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses voraus.

Dieses Problem der Internetkommunikation, dass ihr Schutz nach Art. 10 Abs. 1 GG nicht anhand der verwendeten Kommunikationsmedien beurteilt werden kann, vermag zwar auch die von der Rechtsprechung und *Guckelberger* vertretenen Ansicht nicht zu leisten, sie setzt allerdings nicht an der jeweiligen Kommunikation an, die ja erst ermittelt werden muss, sondern knüpft aus diesem Grund an die Art und Weise des Zugriffs an.

Da insoweit die von Rechtsprechung und *Guckelberger* vertretene Auffassung Abgrenzungsschwierigkeiten – insbesondere bei den unterschiedlichen Kommunikationsbeziehungen – vermeiden, indem das maßgebliche Abgrenzungskriterium darin liegt, ob auf die jeweilige Kommunikation ohne weitere „Autorisierung" von außen zugegriffen werden, ist sie insoweit vorzugswürdig.

(5) Zwischenergebnis – Telekommunikationsgeheimnis nur bei einem unautorisierten Zugriff von außen auf Telekommunikation

Der Schutzbereich des Telekommunikationsgeheimnisses ist deshalb dahingehend eingeschränkt, dass er nur bei Telekommunikation eröffnet ist, wenn von außen unautorisiert auf Telekommunikation zugegriffen wird.

579 Siehe hierzu oben unter Kap. 4 B.I.1.c)(3)ii.
580 Siehe hierzu oben unter Kap. 4 B.I.1.c)(3)i., ii.

d) Schutzbereich des Telekommunikationsgeheimnisses beim Be- oder Verhindern von (vertraulicher) Kommunikation

Umstritten sind darüber hinaus, ob einerseits der Schutzbereich des Art. 10 Abs. 1 GG auch betroffen ist, wenn bestimmte Telekommunikation verhindert wird, und andererseits, ob der Schutzbereich auch die Verschlüsselung von Kommunikation erfasst.

(1) Verhindern von Telekommunikation im Schutzbereich des Art. 10 Abs. 1 GG?

Ob Art. 10 Abs. 1 GG auch betroffen ist, wenn Telekommunikation verhindert wird, wurde insbesondere im Zusammenhang mit dem sog. *Access-Blocking* diskutiert.[581] *Access-Blocking* bezeichnet eine Zugangsbeschränkung von einzelnen Inhalten im Internet, die technisch in verschiedener Weise umgesetzt werden kann und in der juristischen Literatur häufig auch als „Sperrmaßnahme"[582] o.ä. bezeichnet wird.[583]

Hintergrund war zunächst eine im Jahre 2009 intensiv geführte Diskussion, um die Frage, ob der Zugang zu Internetseiten, auf denen kinderpornographische Inhalte abrufbar waren, durch (Access-)Provider gesperrt werden sollten.[584]

Diese Diskussion setzte sich anschließend auch vor den deutschen Zivilgerichten und dem EuGH fort.[585] Die Zivilgerichte mussten sich mit der Frage auseinandersetzen, ob dem Inhaber von Urheberrechten ein Unterlassungsanspruch gegen Telekommunikationsanbieter zusteht, um die Weiterleitung und damit den Abruf von Internetseiten, auf denen urheberrechtlich geschützte Werke frei zum Download verfügbar waren, zu verhindern.[586] Hierzu urteilte der BGH im Jahr 2016, dass ein Telekommunikationsanbieter grundsätzlich in Anspruch genommen werden könne,

581 *Marberth-Kubicki*, NJW 2009, 1792 (1792ff.); *Durner*, ZUM 2010, 833 (833ff.); *Frey/Rudolph/Oster*, MMR-Beil. Heft 3, 1 (1ff.).
582 So etwa SHH-GG/*Guckelberger,* Art. 10 Rn. 34 mit Verweis auf BGHZ 208, 82 (109).
583 Siehe zu den technischen Möglichkeiten *Greve,* Access Blocking, S. 116ff., zum Fernmeldegeheimnis S. 289ff.
584 *Marberth-Kubicki*, NJW 2009, 1792 (1792) m.w.N.
585 So etwa LG Hamburg MMR 2009, 506 (506ff); LG Hamburg ZUM 2010, 902 (902ff).; LG Köln MMR 2011, 833 (833ff.).; EuGH MMR 2014, 397 (397ff.).
586 So bereits *Durner*, ZUM 2010, 833 (833) mit einer umfassenden Darstellung.

um den Zugang zu urheberrechtlich geschützten Werken, die rechtswidrig öffentlich zugänglich gemacht wurden, zu unterbinden.[587]

Da über die mittelbare Drittwirkung[588] auch betroffene Grundrechte im Rahmen der Beurteilung einer Störerhaftung zu berücksichtigen sind[589], setzte sich der BGH insoweit auch mit der Frage und der in der Literatur geführten Diskussion auseinander, ob bereits die Verhinderung von Telekommunikation in den Schutzbereich des Art. 10 Abs. 1 GG fällt.[590] Der BGH gab an, dass die „bloße Verhinderung von Kommunikation […] nicht in den Schutzbereich des Art. 10 I GG [falle]"[591] und setzte sich nachfolgend mit den zu Sperrmaßnahmen vertretenen Ansichten auseinander.[592]

Technisch können diese insbesondere durch folgende drei Möglichkeiten umgesetzt werden:[593]

– Sog. *DNS-Blockade*: bei der DNS-Blockade setzt die Sperrmaßnahme an dem sog. *Domain Name System* (nachfolgend kurz als „*DNS*" bezeichnet) an.[594] Im Internet findet Kommunikation grundsätzlich zwischen IP-Adressen statt.[595] Da es aber etwa für den Aufruf von Internetseiten umständlich ist, in einen Browser die jeweilige IP-Adressen einzugeben, gibt es das *DNS*.[596] In diesem werden bestimmte Domain-Namen – wie etwa Google – einer oder mehreren bestimmten IP-Adressen zugeordnet – ähnlich wie bei einem Telefonbuch.[597] Diese *DNS*-Einträge werden u.a. von den Telekommunikationsanbieter für ihre Kunden vorgehalten. Gibt nun ein Nutzer www.google.de im Browser ein, gleicht ein *DNS*-Server diese Domain ab und der Nutzer wird an die dazugehörige IP-Adresse weitergeleitet.[598] Die *DNS-Blockade* macht sich diese Weiterleitung zunutze und verhindert bei bestimmten Domainnamen die Weiterleitung

587 So der Leitsatz des BGH GRUR 2016, 268 (268).
588 BVerfGE 7, 198 (205ff).
589 BGH GRUR 2016, 268 (272)
590 BGH GRUR 2016, 268 (275f.).
591 BGH GRUR 2016, 268 (275).
592 BGH GRUR 2016, 268 (275f.).
593 *Marberth-Kubicki*, NJW 2009, 1792 (1792); *Durner*, ZUM 2010, 833 (833); Ausführlich mit einer jeweils differenzierenden rechtlichen Bewertung *Leistner/Grisse*, GRUR 2015, 19 (22ff.); BGH GRUR 2016, 268 (275).
594 *Leistner/Grisse*, GRUR 2015, 19 (23).
595 *Leistner/Grisse*, GRUR 2015, 19 (23); *Bauer*, Soziale Netzwerke, S. 41f.
596 *Frey/Rudolph/Oster*, MMR-Beil. Heft 3, 1 (8f.).
597 BGH GRUR 2016, 268 (275); *Meinel/Sack*, Digitale Kommunikation, S. 152; *Leistner/Grisse*, GRUR 2015, 19 (23).
598 *Leistner/Grisse*, GRUR 2015, 19 (23).

an die entsprechende IP-Adresse.[599] Der Eintrag der Domain im *DNS* wird hierzu entweder schlicht gelöscht, sodass es keine Weiterleitung mehr stattfindet oder der Eintrag wird zu einer anderen IP-Adresse geändert, sodass der anfragende Nutzer etwa auf eine Seite weitergeleitet wird, die lediglich den Inhalt hat, dass die angeforderte Seite gesperrt oder nicht verfügbar ist.[600]

Die angeforderte Seite ist insoweit nicht mehr über die Domain verfügbar, das bedeutet aber nicht, dass sie nicht mehr existiert.[601] Sie kann etwa weiter über die schlichte Eingabe der IP-Adresse der Internetseite aufgerufen werden – vorausgesetzt, dass die IP-Adresse dem Nutzer bekannt ist.[602]

– Sog. *IP-Adressen-Sperre:* bei der *IP-Adressen-Sperre* wird schlicht die Übermittlung von Daten von oder an eine bestimmte IP-Adresse verhindert.[603] Die Kommunikation im Internet beruht grundsätzlich auf Weiterleitung von Datenpaketen zwischen Routern mittels sog. Routingtabellen.[604] Der Eintrag in einer solchen Routingtabelle des Telekommunikationsanbieters kann derart verändert werden, dass keine Datenpakete an oder von einer bestimmten IP-Adresse mehr weitergeleitet werden.[605]
– Sog. *URL-Sperre:* ähnlich wie die *DNS-Blockade,* nur zielgenauer, kann über die *URL-Sperre* der Zugriff auf eine einzelne Website eines Internetauftritts gesperrt werden.[606] Anders als bei Domain und IP-Adressen ist bei *URLs* das Ziel von Nutzeranfragen genau bezeichnet.[607] So gelangt man unmittelbar auf eine bestimmte Website – wie etwa einen bestimmten Zeitungsartikel o.Ä. – und nicht nur auf die allgemeine Zugangsseite eine Zeitungsanbieters.[608] Da die angefragte *URL* aber nur in den Daten-

599 *Leistner/Grisse*, GRUR 2015, 19 (23).
600 *Durner*, ZUM 2010, 833 (833); *Leistner/Grisse*, GRUR 2015, 19 (23).
601 *Leistner/Grisse*, GRUR 2015, 19 (23).
602 *Leistner/Grisse*, GRUR 2015, 19 (23).
603 *Durner*, ZUM 2010, 833 (833); *Leistner/Grisse*, GRUR 2015, 19 (23f.).
604 *Leistner/Grisse*, GRUR 2015, 19 (23f).
605 *Leistner/Grisse*, GRUR 2015, 19 (23f.).
606 *Leistner/Grisse*, GRUR 2015, 19 (24).
607 *Leistner/Grisse*, GRUR 2015, 19 (24).
608 *Leistner/Grisse*, GRUR 2015, 19 (24). Beispielsweise gelangt man über die Domain www.heise.de (letzter Abruf: 20. Dezember 2021) auf die Startseite des Online-Newsportals der Heise Medien GmbH & Co. KG. Über die genau URL – etwa https://www.heise.de/newsticker/meldung/Internetprovider-fordern-klare-gesetzliche-Regelung-fuer-Access-Blocking-198400.html (letzter Abruf: 20. Dezember 2021) gelangt man dagegen auf einen Artikel von *Stefan Krempl* mit dem Titel

> pakten der Nutzeranfrage enthalten ist, muss für eine *URL-Sperre* der gesamte Datenverkehr über einen sog. *Zwangs-Proxy-Server* umgeleitet werden, der die Datenpakte nach gesperrten *URLs* filtert und nur dann weiterleitet, wenn keine gesperrte *URL* aufgerufen wird.[609]

Ob diese technischen Möglichkeiten jeweils den Schutzbereich des Telekommunikationsgeheimnisses betreffen, war in Literatur und Rechtsprechung umstritten.

So nahm das OLG Hamburg 2014 an, dass alle drei technischen Methoden der Sperrmaßnahmen vom Schutzbereich des Art. 10 Abs. 1 GG erfasst seien[610] und begründete dies damit, dass Domain Namen, ebenso wie IP-Adressen und URLs Umstände von Telekommunikation seien, wenn diese in Bezug zu einem Übertragungs- oder Verbindungsvorgang gesetzt würden.[611] Da bereits der Versuch eines Verbindungsaufbaus bei der Abfrage eines *DNS*-Namens durch einen Nutzer in den Schutzbereich des Art. 10 Abs. 1 GG falle, sei bereits diese bloße Abfrage vom Schutzbereich des Art. 10 Abs. 1 GG erfasst.[612] Da im Übrigen bei den Sperrmaßnahmen der *IP-Adressen-Sperre* und der *URL-Sperre* konkrete Telekommunikationsvorgänge ausgewertet würden, sei Art. 10 Abs. 1 GG hier ohne weiteres betroffen.[613]

Dagegen ging eine differenzierende Ansicht in der Literatur davon aus, dass nur *IP-Adressen-Sperre* und *URL-Sperre* in den Schutzbereich des Art. 10 Abs. 1 GG fielen.[614] Denn hierbei würden konkrete Telekommunikationsumstände ausgewertet werden – nämlich die jeweils angesteuerte IP-Adresse bzw. URL-Adresse. Insoweit müsste zunächst konkrete Telekommunikation – teilweise über die Umleitung über einen (Zwangs-)Proxy-Server – ausgewertet werden, um die Telekommunikation zu verhindern.[615]

Der BGH und Teile der Literatur hielten dieser Auffassung insbesondere zur *DNS-Sperre* entgegen, dass Art. 10 zwar bei der Kenntnisnahme von näheren Umständen individueller Kommunikation und erfolgloser Kom-

---

„Internetprovider fordern klare gesetzliche Regelung für Access Blocking" aus dem Jahr 2009 zum umstrittenen Thema des Access-Blockings.

609 *Leistner/Grisse*, GRUR 2015, 19 (24f.).

610 OLG-Hamburg GRUR-RR 2014, 140 (145).

611 OLG Hamburg GRUR-RR 2014, 140 (146).

612 OLG Hamburg GRUR-RR 2014, 140 (146).

613 OLG Hamburg GRUR-RR 2014, 140 (146).

614 Vgl. hierzu den Verweis des BGH GRUR 2016, 268 (272).

615 Vgl. hierzu die Darstellung des BGH GRUR 2016, 268 (272) m.w.N.; *Leistner/Grisse*, GRUR 2015, 19 (24f.).

munikationsversuche betroffen sei, aber eben nicht bei der bloßen Verhinderung von Kommunikation einschlägig sei.[616] Die *DNS-Sperre* verhindere allerdings lediglich Telekommunikation, sodass nach dem Schutzzweck der Vertraulichkeit von Telekommunikation Art. 10 Abs. 1 GG dann nicht betroffen sei, wenn Telekommunikation gar nicht erst zustande käme.[617]

Darüber hinaus kritisiert ein Teil der Literatur, dass die formale Differenzierung nach den technischen Verarbeitungsprozessen zwischen DNS-Sperre einerseits und IP-Adressen-Sperre und URL-Sperre andererseits nicht ausreichend die Teleologie des Art. 10 Abs. 1 GG berücksichtige.[618]

Ähnlich begründet auch der BGH, dass der Schutzbereich des Art. 10 Abs. 1 GG bei keiner der drei Sperrmaßnahmen betroffen sei.[619] Denn zunächst sei das allgemein zugänglich gemachte Downloadangebot keine von Art. 10 Abs. 1 GG geschützte Telekommunikation.[620] Darüber hinaus würden auch bei *IP-Adressen-* und *URL-Sperre* lediglich die Daten, die zur Sperrung erforderlich seien, ausgewertet.[621] Eine weitergehende Sichtung und Auswertung der Daten finde dagegen nicht statt.[622] Insoweit verweist der BGH auf die Rechtsprechung des BVerfG[623] nach der kein Eingriff in Fernmeldevorgänge vorliegen soll, wenn diese lediglich technikbedingt erfasst und anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden aussortiert würden.[624]

Dieser Rechtsprechung des BGH ist im Ergebnis zuzustimmen, sodass sie als Grundlage der weiteren rechtlichen Bewertung verwendet wird.

Zwar ist dem OLG Hamburg dahingehend zuzustimmen, dass durch Domain-Namen, IP-Adressen und URLs jeweils Umstände von Telekommunikation vorliegen, da hierüber jeweils konkrete Telekommunikationsverbindungen aufgebaut werden können. Außerdem ist nachvollziehbar, dass das OLG Hamburg vor dem Hintergrund der geschützten Telekommunikationsumstände, von denen auch erfolglose Verbindungsversuche (etwa beim Telefon) erfasst sind, annimmt, dass bereits der erfolglose Versuch, eine Internetseite abzurufen, vom Schutzbereich des Art. 10 Abs. 1 GG erfasst ist.

616 BGH GRUR 2016, 268 (275); *Durner*, ZUM 2010, 833 (841f.); *Leistner/Grisse*, GRUR 2015, 19 (22f.).
617 *Durner*, ZUM 2010, 833 (842); BGH GRUR 2016, 268 (275).
618 *Durner*, ZUM 2010, 833 (842).
619 BGH GRUR 2016, 268 (276).
620 BGH GRUR 2016, 268 (276); siehe hierzu bereits oben unter Kap. 4 B.I.1.c)(3).
621 BGH GRUR 2016, 268 (276).
622 BGH GRUR 2016, 268 (276); so auch *Durner*, ZUM 2010, 833 (842).
623 BVerfGE 100, 313 (366); BVerfGE 107, 299 (328).
624 BGH GRUR 2016, 268 (276); so auch *Durner*, ZUM 2010, 833 (842).

Dem steht jedoch entgegen, dass bei dem schlichten Verhindern einer konkreten Verbindung, keine Umstände von Telekommunikation von außen zur Kenntnis genommen werden.[625] Die konkreten Telekommunikationsumstände sind insoweit nur betroffen, als dass sie lediglich technisch vom Telekommunikationsanbieter zur Kenntnis genommen werden, um die Telekommunikationsverbindung zu verhindern.[626] Dies entspricht insoweit nicht dem Schutzzweck des von Art. 10 Abs. 1 GG geschützten Teilbereichs der Telekommunikationsumstände.[627] Dieser liegt nämlich darin, dass auch durch die Umstände der Telekommunikation weitreichende Rückschlüsse auf die Persönlichkeit des Einzelnen möglich sind.[628] Da beim lediglich technisch bedingten Auswerten von Telekommunikationsumständen, die zum bloßen Verhindern einer Telekommunikationsverbindung führen, keinerlei weitere Auswertung ermöglicht werden, ist hier der Schutzzweck der geschützten Telekommunikationsumstände nicht betroffen.[629] Ebenfalls findet darüber hinaus auch keine inhaltliche Auswertung der Telekommunikation statt, da diese gerade durch die Sperrmaßnahmen unterbunden wird.

Im Ergebnis ist damit zumindest der Schutzbereich des Art. 10 Abs. 1 GG nicht betroffen, wenn lediglich der Aufbau einer Telekommunikationsbeziehung technisch verhindert wird, daran anschließend aber keinerlei Auswertung der hierbei gewonnenen Informationen über die beabsichtigte Telekommunikationsverbindung stattfindet.

625 So bereits ähnlich *Durner*, ZUM 2010, 833 (842); *Leistner/Grisse*, GRUR 2015, 19 (22f.).

626 BGH GRUR 2016, 268 (276). So bereits ähnlich *Durner*, ZUM 2010, 833 (842); *Leistner/Grisse*, GRUR 2015, 19 (22f.).

627 Ähnlich *Leistner/Grisse*, GRUR 2015, 19 (25).

628 Siehe hierzu bereits oben unter Kap. 4 B.I.1.; BVerfGE 125, 260 (328); *Bauer*, Soziale Netzwerke, S. 100.

629 BGH GRUR 2016, 268 (276).

(2) Verschlüsseln von Telekommunikation im Schutzbereich des Art. 10 Abs. 1 GG

Unstreitig dürfte zunächst sein, dass verschlüsselte Telekommunikationsinhalte selbst ebenfalls dem Schutz des Art. 10 Abs. 1 GG unterfallen[630], da Telekommunikation unabhängig von ihrem Inhalt erfasst ist.[631]

Fraglich ist allerdings, ob auch der Verschlüsselungsvorgang selbst vom Schutzbereich des Telekommunikationsgeheimnisses erfasst ist.

Nach einer im Schrifttum vertretenen Ansicht soll auch der Verschlüsselungsvorgang selbst vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sein.[632] Hierzu werden folgende Erwägungen zur Begründung herangezogen:

Einerseits soll der Verschlüsselungsvorgang zwar selbst nicht Teil des Übermittlungsvorgangs sein, aber jeweils in einem unmittelbaren Zusammenhang zu diesem geschützten Übermittlungsvorgang stehen.[633] Denn die Kommunikation wird gerade im Hinblick auf die bevorstehende Übermittlung verschlüsselt, um sie beim Übermittlungsvorgang vor einem unberechtigten Zugriff zu schützen.[634] Insoweit sei die Verschlüsselung selbst gerade „unmittelbar[e] Verwirklichung des grundrechtlich […] gewährleisteten Schutzes“[635].

Andererseits sollen sowohl der Wortlaut als auch der Normzweck des Art. 10 Abs. 1 GG für die Erfassung des Verschlüsselungsvorgangs sprechen.[636] Denn bereits der Wortlaut des „Geheimnisses“ in Art. 10 Abs. 1 GG spreche dafür, dass auch die Möglichkeit, vertraulich zu kommunizieren, erfasst sein müsse.[637] Außerdem sei nach dem Normzweck eine Vorbedingung der geschützten, vertraulichen Kommunikation, die Möglichkeit, vertrauliche Kommunikationsmöglichkeiten zu nutzen.[638]

630 Hierzu mit ausführlicher Begründung *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 130ff.; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 117; BeckOK-GG/*Ogorek,* Art. 10 Rn. 13.

631 Siehe hierzu bereits oben unter Kap. 4 B.I.1; BVerfGE 106, 28 (36); BVerfG NJW 2000, 55 (56); BVerfGE 130, 151 (179); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 103.

632 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137f.; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 71f., Rn. 117.

633 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

634 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

635 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

636 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 72.

637 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 72.

638 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 72.

Dieser Auffassung ist Folgendes entgegenzuhalten:

Es trifft zu, dass Verschlüsselung und Übermittlung in einem unmittelbaren Zusammenhang zueinanderstehen und die Verschlüsselung gerade im Hinblick auf die Übermittlung stattfindet. Andererseits liegt beim Verschlüsselungsvorgang gerade nicht die für Art. 10 Abs. 1 GG spezifische Übermittlungsgefahr vor, vor der das Telekommunikationsgeheimnis schützen soll.[639] Außerdem liegt der grundrechtlich gewährleistete Schutz maßgeblich darin, dass unberechtigt von außen auf Grund der spezifischen Übermittlungsgefahr bei Fernkommunikation zugegriffen werden kann.[640] Zwar soll die Verschlüsselung die tatsächliche Kenntnisnahme des Kommunikationsinhalts erschweren, aber kann nicht den Zugriff auf die Kommunikation selbst verhindern. Insoweit wäre eine unmittelbare Verwirklichung des grundrechtlich gewährleisteten Schutzes eher, die Übermittlung selbst vorzunehmen, als die Kenntnis vom Inhalt nach dem Zugriff zu erschweren.

Weiterhin müsste das angeführte Argument des Wortlauts und des Normzwecks[641] auch für das Verhindern von Telekommunikation gelten.[642] Denn, wenn eine Vorbedingung des Telekommunikationsgeheimnisses ist[643], vertrauliche Kommunikationsmittel zu nutzen, muss auch die Nutzung von Telekommunikation insgesamt eine Vorbedingung des Telekommunikationsgeheimnisses sein. Es wäre widersprüchlich, wenn nur die Möglichkeit, *vertraulich* zu kommunizieren eine Vorbedingung geschützter Telekommunikation wäre und nicht die Möglichkeit *überhaupt* zu kommunizieren.

Aus diesen Gründen erscheint die vom überwiegenden Teil der Literatur vertretene Auffassung, dass die Verschlüsselung selbst nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst ist, vorzugswürdig. Diese Auffassung wird darüber hinaus insbesondere mit der Teleologie des Art. 10 Abs. 1 GG dahingehend begründet, dass Art. 10 Abs. 1 die Vertraulichkeit eines konkreten Kommunikationsvorgangs schützen soll, aber nicht die Be- oder

639 Ähnlich Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 71.

640 Siehe hierzu bereits oben unter Kap. 4 B.I.1.c); BVerfGE 115, 166 (182); Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 59, 68f.; *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 196; *Bauer*, Soziale Netzwerke, S. 99f.

641 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 59, 68f.

642 Insoweit abweichend *Durner*, ZUM 2010, 833 (841f.), der davon ausgeht, dass das bloße Verhindern keinen Eingriff in das Telekommunikationsgeheimnis darstellt.

643 Siehe hierzu Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 73.

Verhinderung der Telekommunikation selbst.[644] Dass der Verschlüsselungsvorgang insoweit unabhängig von der Übermittlung ist, kommt auch darin zum Ausdruck, dass er zeitlich vor der Übermittlung (bzw. die Entschlüsselung nach der Übermittlung) stattfindet.[645] Maßgeblich muss insoweit die spezifische Gefahr des Übermittlungsgefahr sein.

Dementsprechend ist davon auszugehen, dass auch die Verschlüsselung von Kommunikation nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst ist.

(3) Zwischenergebnis

Sowohl das lediglich technische Verhindern von Kommunikation als auch das Verschlüsseln von Telekommunikation ist nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst.

e) Zwischenergebnis – Schutzbereich des Telekommunikationsgeheimnisses

Der Schutzbereich des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG erfasst die unkörperliche Übermittlung von Informationen an einen individuellen Empfängerkreis und die Umstände einer solchen individuellen Übermittlung.[646] Der Schutzbereich erfasst Telekommunikation unabhängig von ihrem Inhalt und Qualität[647], soweit die Kommunikation nicht nur zwischen technischen Geräten stattfindet und insoweit auf einem menschlichen Veranlassen beruht.[648] Zudem müssen fortlaufende Telekommunikationsbeziehungen betroffen sein oder die Telekommunika-

644 So stellt Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 72 die Argumentation der herrschenden Auffassung dar. Hierzu etwa auch *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

645 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

646 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1; BVerfGE 67, 157 (172); BVerfGE 106, 28 (35f.); BVerfGE 115, 166, 182; BeckOK-GG/*Ogorek,* Art. 10 Rn. 36; SHH-GG/*Guckelberger,* Art. 10 Rn. 22f.; Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 106.

647 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1; *Bauer*, Soziale Netzwerke, S. 100 mit Verweis auf BVerfGE 106, 28 (36); BVerfG NJW 2000, 55 (56); BVerfGE 130, 151 (179); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 103.

648 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.a); BVerfG NJW 2007, 351 (353 Rn. 57); BeckOK-GG/*Ogorek,* Art. 10 Rn. 56.

tion muss außerhalb des Herrschaftsbereichs des Betroffenen gespeichert werden.[649] Um eine geschützte Individualkommunikation handelt es sich nur, wenn von außen unautorisiert auf Telekommunikationsvorgänge zugegriffen wird[650] – nicht vom Schutzbereich erfasst wird dagegen das personengebundene Vertrauen in die Kommunikationsbeteiligten.[651] Außerdem vom Schutzbereich nicht erfasst ist das bloße Verhindern von Telekommunikation[652] sowie die Verschlüsselung von Telekommunikation.[653]

2. Ist der Schutzbereich des Telekommunikationsgeheimnisses bei den dargestellten Auswertungsmöglichkeiten eröffnet?

Insoweit stellt sich nun die Frage, ob bei den in Kapitel 3 dargestellten Auswertungsmethoden der soeben dargestellte Schutzbereich des Art. 10 Abs. 1 GG eröffnet ist.

Dies hängt insbesondere davon ab, welche Daten von Auswertungsmöglichkeiten ausgewertet werden, sodass nachfolgend hiernach differenziert wird.

a) Transaktionsdaten in Blockchains als geschützte Telekommunikation?

Maßgebliche Datengrundlage der in Kapitel 3 A. dargestellten Auswertungsmöglichkeiten sind die Transaktionsdaten, die in einer öffentlichen Blockchain enthaltenen sind. Die Transaktionsdaten gelangen dadurch in die Blockchain, dass zunächst ein Nutzer eine Transaktionsnachricht an das Netzwerk versendet und diese Nachricht stetig weitergeleitet und bestätigt wird und so schließlich dem Datensatz der Blockchain in einem neuen Block angehängt wird.[654]

649 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.b); BVerfG NJW 2009, 2431 (2432 Rn. 46); *Safferling/Rückert*, MMR 2015, 788 (792f.).

650 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.c); BVerfGE 120, 274 (341); *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 107.

651 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.c); BVerfGE 120, 274 (341).

652 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.d)(1); BGH GRUR 2016, 268 (275); *Durner*, ZUM 2010, 833 (841).

653 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.d)(2).

654 Siehe hierzu oben ausführlich unter Kap. 2 A.II.7., III.1.c); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43f.; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 183f.

Insoweit sind die so über das *Peer-to-Peer-Netzwerk* einer Blockchain-Technologie zwischen den Nutzern versendeten, ausgetauschten und weitergeleiteten Transaktionsnachrichten zunächst einmal unkörperlich übermittelte Informationen im Sinne des Art. 10 Abs. 1 GG. Da der Schutzbereich auch nicht auf bestimmte Kommunikationsinhalte beschränkt ist, sind auch die Informationen bzgl. der jeweiligen Transaktionen erfasst.

Der Schutzbereichseröffnung steht außerdem nicht entgegen, dass das primäre Ziel der Auswertungsmethoden nicht die Erhebung dieser Transaktionsnachrichten ist, sondern erst die systematische Auswertung der Transaktionsnachrichten. Denn die Schutzwirkung des Art. 10 Abs. 1 GG erstreckt sich auch auf die nach der Kenntnisnahme von geschützter Telekommunikation anschließenden Datenverarbeitungsprozesse.[655]

(1) Blockchain-Inhalte als menschlich veranlasste Telekommunikation

Fraglich ist dagegen, ob in der Blockchain enthaltenen Transaktionsdaten menschlich veranlasste Telekommunikationsvorgänge sind. Denn die Transaktionsnachrichten werden lediglich mittels eines Algorithmus automatisch nach einem bestimmten Muster innerhalb der beteiligten Rechner weitergeleitet und so verbreitet.[656] Dabei versendet der Ersteller einer Transaktionsnachricht diese in der Regel an seine 8 *peers* – also diejenigen Nutzer, mit denen er unmittelbar verbunden ist.[657] Diese leiten die so empfangene Transaktionsnachricht dann an ihre *peers* weiter, die dann wiederum die Transaktionsnachricht an ihre *peers* weiterleiten, sodass sich die neue Transaktionsnachricht im Netzwerk ausbreitet und schließlich durch Bestätigung der anderen Nutzer in die Blockchain als neue Transaktion aufgenommen wird.[658]

Problematisch ist das deshalb, da zwar einerseits der Ersteller und erstmalige Absender einer Transaktionsnachricht diese in der Regel bewusst und willentlich an seine *peers* versendet, sodass die nach dem BVerfG[659] erforderliche menschlich veranlasste Telekommunikation hier vorliegt. Ande-

655 BVerfG NJW 2000, 55 (57).
656 Zur technischen Funktionsweise des Weiterleitungsmechanismus von Bitcoin ausführlich *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).
657 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3f.).
658 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3ff.).
659 BVerfG NJW 2007, 351 (353 Rn. 57); BVerfGE 130, 151 (179, 181); BVerfG NJW 2016, 3508 (3510 Rn. 38).

rerseits sind Gegenstand der Auswertungsmethoden erst die in der Blockchain enthaltenen Transaktionsdaten, die auf dem lediglich technischen Verfahren des Weiterleitens und Bestätigens beruhen.[660]

Hinzu kommt, dass auch das Herunterladen der Blockchain-Daten rein technisch abläuft, denn hierzu reicht es aus, die entsprechende Software[661] herunterzuladen und auszuführen und so selbst *full-node* des Blockchain-Netzwerks zu werden.[662] Dieser *Bitcoin-Core-Client* stellt automatisch eine Verbindung mit anderen Nutzern her und lädt von ihnen die vollständige Blockchain herunter. Ein willensgesteuertes Handeln liegt hier also nur beim „Starten" der Software vor. Deshalb stellt sich die Frage, ob es für die menschlich veranlasste Telekommunikation ausreicht, dass nur der erstmalige Versand auf einem bewussten, willensgetragenen Handeln beruht.

Dafür spricht, dass es nicht darauf ankommen kann, wie eine ursprünglich bewusst versandte Nachricht, technisch übermittelt wird. Maßgeblich muss sein, dass ein konkreter Telekommunikationsvorgang vorliegt, der auf einem bewussten, menschlichen Handeln beruht. Denn andernfalls wäre Fernkommunikation, die auf einer automatischen, technischen Weiterleitung – etwa allein bei der Nutzung eines *VPN-Clients*[663] – beruhen würde, insgesamt vom Schutzbereich des Telekommunikationsgeheimnis ausgenommen, sodass der Schutzbereich des Art. 10 Abs. 1 GG teilweise vom Zufall der technischen Weiterleitung abhängen würde. Außerdem beruht Internetkommunikation in der Regel ohnehin auf automatischer Weiterleitung von Informationen, denn beispielsweise beim Aufruf einer Internetseite wird dieser Zugriffswunsch des Nutzers zunächst an den jeweiligen Telekommunikationsanbieter gesendet, der dann wiederum diesen Kommunikationswunsch automatisch an den Server bzw. Telekommunika-

660 Siehe hierzu etwa die in Kap. 3 A.I. dargestellten Auswertungsmethoden. In den technischen Papern hierzu wird jeweils dargestellt, wann die jeweilige Blockchain heruntergeladen wurde, vgl. *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (5), deren maßgebliche Blockchain-Daten etwa vom 05. Februar 2019, 08:13:31 Uhr stammt.

661 Bspw. ein sog. *Bitcoin-Core-Client*, vgl. *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 140f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.

662 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43f.

663 Durch einen VPN-Client („virtual private network") ist es möglich, sich über das Internet unmittelbar mit einem bestimmten Rechner bzw. Server zu verbinden, über den dann die weitere Internetkommunikation laufen kann, vgl. *Meinel/Sack*, Digitale Kommunikation, S. 159f.

tionsanbieter der aufgerufenen Internetseite weiterleitet.[664] Hervorzuheben ist außerdem, dass beim Versenden einer solchen Transaktionsnachricht an die jeweiligen *peers* das Ziel des Absenders gerade die Verbreitung im gesamten Blockchain-Netzwerk ist, denn nur so kann eine neue Transaktionsnachricht bestätigt und in die Blockchain aufgenommen werden.[665] Es ließe sich daher argumentieren, dass beim erstmaligen Versand der Transaktionsnachricht ein bewusster Wille des Absenders bestand, dass die Nachricht entsprechend weitergeleitet wird.

Außerdem ist der ursprüngliche Versand einer Transaktionsnachricht kein getrennt von der darauffolgenden Aufnahme in die Blockchain zu betrachtender Sachverhalt – die Aufnahme in die Blockchain beruht ja gerade auf dem ursprünglichen Versenden mit dem bewussten Ziel der Verteilung im gesamten Netzwerk.[666]

Hinzukommt, dass die Teilnahme an Blockchain-Netzwerke bewusst auf aktive Teilnahme am Netzwerk ausgerichtet ist. Denn das Ziel in Blockchain-Netzwerken ist gerade die Loslösung von staatlichen Intermediären, sodass deren Verwaltungsaufgaben vom Netzwerk selbst übernommen werden.[667] Deshalb liegt der Teilnahme an so einem Netzwerk ein entsprechendes, aktives menschliches Verhalten zugrunde, von dem die Weiterleitung der Transaktionsnachrichten getragen wird. Denn die Teilnahme an einem Netzwerk, dass auf aktive Mitgestaltung durch die beteiligten Rechner ausgelegt ist, geht insoweit über das bloße Einschalten eines Mobiltelefons hinaus, bei dem eine Kommunikationsverbindung zur Funkzelle nur hergestellt wird, um erreichbar zu sein. Denn die Kommunikationsverbindung zur Funkzelle wird nur im Falle eines tatsächlichen Anrufs verwendet und wird insoweit nur passiv fortwährend durch das Mobiltelefon aktualisiert.[668] Die Teilnahme an einem Blockchain-Netzwerk umfasst immer auch die aktive Mitgestaltung hieran.

Dementsprechend genügen auch die in der Blockchain enthaltenen Transaktionsdaten den Anforderungen des BVerfG an bewusst, menschlich veranlasste Kommunikation.

664 Technisch sind diese Ausführungen stark vereinfacht, die Kommunikationsverbindungen beruhen auf einer Vielzahl an einzelnen Weiterleitungen im Internet.
665 Siehe hierzu bereits oben unter Kap. 2 A.II.7., III.1.
666 Siehe hierzu bereits oben unter Kap. 2 A.II.7.
667 Siehe hierzu oben unter Kap. 2 A.I.
668 Vgl. BVerfG zum IMSI-Catcher.

(2) Blockchain-Inhalte als fortlaufende oder außerhalb des Herrschaftsbereichs des Betroffenen gespeicherte Telekommunikation

Fraglich ist darüber hinaus aber, ob sie auch außerhalb des Herrschaftsbereichs des Betroffenen gespeichert sind bzw. ob sie fortlaufende Kommunikation darstellen.

Einerseits sind bei Blockchains die Inhaltsdaten im Grundsatz auf den Rechnern aller beteiligten Nutzer gespeichert[669] – also sowohl auf dem Rechner des Betroffenen und damit in seinem Herrschaftsbereich als auch außerhalb seines Herrschaftsbereichs auf anderen Rechnern.[670] Maßgeblich muss in diesem Kontext allerdings sein, dass die ausgewerteten Daten *auch* außerhalb des Herrschaftsbereichs des Betroffenen gespeichert werden, denn hierdurch wird gerade die vom BVerfG zur Begründung herangeführte spezifische Gefahr des Zugriffs auf Telekommunikation durch Dritte begründet.[671] Es kann insoweit nicht maßgeblich sein, dass die Telekommunikation auch im Herrschaftsbereich des Betroffenen gespeichert wird, sondern nur, dass sie auch außerhalb seines Herrschaftsbereichs gespeichert wird.

Selbst wenn dem entgegen angenommen werden sollte, dass sich der Schutzbereich des Art. 10 Abs. 1 GG auf Telekommunikation im Zeitraum ihres Übermittelungsvorgangs beschränkt und endet, wenn die Nachricht beim Empfänger angekommen ist[672], dürfte der Schutzbereich für Inhaltsdaten in Blockchains trotzdem eröffnet sein.[673] Denn nachdem eine Transaktionsnachricht in das Netzwerk versendet wurde, wird diese zunächst an alle anderen im Netzwerk beteiligten Rechner weitergeleitet und anschließend durch die anderen Nutzer bestätigt und insoweit in einen neuen „Block" aufgenommen.[674] Eine Transaktion gilt einerseits erst nach ca. sechs weiteren, neuen Blöcken als „sicher".[675] Insoweit wird die Sicherheit der Transaktion mit der fortlaufenden Erweiterung der Blockchain auch fortlaufend verstärkt.[676] Andererseits bildet die Aufnahme einer Transaktion in die Blockchain gerade die notwendige Voraussetzung für

669 Siehe hierzu bereits Kap. 2 A.II.8; *Safferling/Rückert*, MMR 2015, 788 (793).
670 So bereits *Safferling/Rückert*, MMR 2015, 788 (793).
671 Vgl. insoweit BVerfG NJW 2009, 2431 (2432 Rn. 46).
672 So etwa Stern-Becker-GG/*Schenke*, Art. 10 Rn. 48.
673 So bereits *Safferling/Rückert*, MMR 2015, 788 (793).
674 Siehe hierzu bereits oben unter Kap. 2 A.II.7.;III.1.
675 Siehe hierzu *Safferling/Rückert*, MMR 2015, 788 (793).
676 So bereits *Safferling/Rückert*, MMR 2015, 788 (793).

eine weitere Transaktion[677], sodass insoweit ebenfalls von fortlaufender Telekommunikation auszugehen ist.

(3) Blockchain-Inhalte als Individual- oder Massenkommunikation?

Auch für die Frage, ob bei Blockchain-Daten Individual- oder Massenkommunikation vorliegt, könnte grundsätzlich der Weiterleitungsmechanismus problematisch sein. Denn es ließe sich zunächst argumentieren, dass bei der Weiterleitung von Transaktionsnachrichten an die 8 *peers*[678] jeweils eine individuelle Kommunikationsbeziehung vorliegt und hierfür der Schutzbereich des Telekommunikationsgeheimnisses eröffnet ist. Wenn nun die so weitergeleiteten und später in der Blockchain zusammengefassten Transaktionsnachrichten von Ermittlungsbehörden ausgewertet werden, könnte man annehmen, dass durch den Zugriff auf die Blockchain-Daten diese jeweils individuellen Kommunikationsbeziehungen des Einzelnen mit seinen 8 *peers* betroffen sind.

Dem steht allerdings entgegen, dass die Kommunikationsbeziehung des Einzelnen mit seinen *peers* gerade auf Weiterleitung von Transaktionsnachrichten zur Verteilung im gesamten Netzwerk angelegt ist.[679] Selbst wenn ein Nutzer davon ausgehen würde, dass die mit seinen *peers* geführte Telekommunikation vertraulich sei, wird die von ihm geführte Telekommunikation unmittelbar durch seine *peers* weitergeleitet und so werden alle weiteren Nutzer im Netzwerk „autorisiert". Denn das Telekommunikationsgeheimnis schützt eben nicht das personengebundene Vertrauen in die Kommunikationsbeteiligten[680], sodass durch die Weiterleitung der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet ist.

Insoweit kann das Telekommunikationsgeheimnis nicht bei Blockchain-Daten betroffen sein, da keinerlei Autorisierung erforderlich ist, um sich als *full-node* mit dem Blockchain-Netzwerk zu verbinden und die Transaktionsdaten der Blockchain herunterzuladen.[681] Wenn sich nun eine staatliche Stelle dergestalt mit einem Blockchain-Netzwerk verbindet, liegt hierin kein

677 Siehe hierzu bereits oben unter Kap. 2 A.II.7.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 50; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 25; *Safferling/Rückert*, MMR 2015, 788 (793).
678 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3ff.).
679 Siehe hierzu bereits oben unter Kap. 2 II.7., III.1., Kap. 4 B.I.2.a)(1).
680 BVerfGE 120, 274 (341).
681 So bereits *Safferling/Rückert*, MMR 2015, 788 (793).

Zugriff von außen auf eine Telekommunikationsbeziehung vor, sondern die staatliche Stelle begibt sich in eine Telekommunikationsbeziehung, deren Daten im Anschluss ausgewertet werden. Hiervor schützt allerdings gerade nicht Art. 10 Abs. 1 GG.[682]

Da aus diesem Grund bei den Daten in der Blockchain keine Individualkommunikation vorliegt, ist der Schutzbereich des Telekommunikationsgeheimnisses für die in einer Blockchain enthaltenen Transaktionen nicht eröffnet.[683]

(4) Zwischenergebnis – Blockchain-Inhalte sind keine geschützte Telekommunikation

Die in einer öffentlich geführten Blockchain enthaltenen Daten sind keine von Art. 10 Abs. 1 GG geschützte Telekommunikation, da die Blockchain-Inhalte keine Individual-, sondern Massenkommunikation darstellen.[684]

b) Netzwerkverbindungen und Netzwerkverhalten als geschützte Telekommunikation?

Anders als bei der Auswertung von Blockchain-Inhalten beruhen die in Kapitel 3 B. dargestellten Auswertungsmöglichkeiten maßgeblich auf Netzwerk-Daten, die beim Versenden einzelner Transaktionsnachrichten anfallen. Da es hier – anders als bei der Auswertung der unmittelbaren Blockchain-Daten – keine einheitliche Datengrundlage gibt, ist zwischen den Daten der einzelnen Maßnahmen zu differenzieren.

682 BVerfGE 120, 274 (341).

683 Siehe hierzu bereits *Safferling/Rückert*, MMR 2015, 788 (793), die allerdings als maßgebliche Begründung hierfür auf die Perspektive der Nutzer abstellen (vgl. insoweit die oben unter Kap. 4 B.I.1.c) dargestellten, unterschiedlichen Ansichten zur Abgrenzung zwischen Massen- und Individualkommunikation) und angeben, dass kein Nutzer einer öffentlich geführten Blockchain davon ausgehen kann, dass es sich um vertrauliche Kommunikation handele.

684 So auch *Safferling/Rückert*, MMR 2015, 788 (793f.).

(1) Auswertung der Verbreitung von Transaktionsnachrichten

Bei den in Kap. 3 B.I., II. dargestellten Auswertungsmöglichkeiten wird die IP-Adresse einzelnen Bitcoin-Adressen dadurch zugeordnet, dass ausgewertet wird, von welchem *peer* eine Transaktionsnachricht zuerst in das Netzwerk versandt wurde.[685] Betroffen sind insoweit einerseits die Telekommunikationsumstände, denn es wird ausgewertet, wann welche Kommunikation zwischen welchen Beteiligten stattgefunden hat. Andererseits muss auch der Telekommunikationsinhalt ausgewertet werden, um zu ermitteln, welche Transaktionsnachricht jeweils versendet und weitergeleitet wurde.

Da hier der erstmalige Versand wiederum auf einem menschlich veranlassten Handeln beruht, liegt auch hier eine menschlich veranlasste Telekommunikation vor.[686] Soweit auch die Weiterleitungen durch die anderen Teilnehmer von der Auswertung betroffen sind, sind auch diese vom Schutzbereich erfasst – einerseits, da Gegenstand der Weiterleitung hier eine ursprünglich menschlich veranlasste Telekommunikation ist[687] und andererseits die aktive Teilnahme an einem Blockchain-Netzwerk über das Einschalten und die passive Empfangsbereitschaft eines Handys hinausgehen[688].

Für diese Auswertungsmöglichkeit wird außerdem auf gerade stattfindende Telekommunikation zugegriffen[689], die entweder bereits beim Zugriff ausgewertet wird oder unmittelbar danach. Da sich der Schutzbereich des Art. 10 Abs. 1 GG auch auf die nach der Informationsgewinnung angeschlossene Datenverarbeitung erstreckt[690], liegt auch hier die erforderliche fortlaufende Telekommunikation vor.

Fraglich ist hier allerdings ebenfalls, ob Telekommunikation mit einem individuellen Empfängerkreis vorliegt. Im Grundsatz ist von der Auswer-

685 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (5ff.).

686 Insoweit gilt die soeben (unter Kap. 4 B.I.2.a)(1)) dargestellte Argumentation hier entsprechend.

687 Insoweit gilt die soeben (unter Kap. 4 B.I.2.a)(1)) dargestellte Argumentation hier entsprechend.

688 Insoweit gilt die soeben (unter Kap. 4 B.I.2.a)(2)) dargestellte Argumentation hier entsprechend.

689 Denn zur Auswertung wird eine Verbindung zu möglichst allen *peers* hergestellt, um so den ersten Versender ermitteln zu können, vgl. oben Kap. 3 B.I.; *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (5ff.).

690 Dürig/Herzog/Scholz/*Durner,* Art. 10 Rn. 113 mit Verweis auf BVerfGE 93, 181 (188); BVerfGE 100, 313 (359).

tungsmethode gerade die individuelle Telekommunikation der Nutzer mit ihren *peers* betroffen. Denn Gegenstand der Auswertung ist gerade, welche Transaktionsnachrichten von welchen *peers,* wann empfangen wurden und insoweit nur die Umstände der an die einzelnen *peers* versendeten Transaktionsnachrichten.

Allerdings wird hier wiederum nicht durch eine staatliche Stelle von außen auf individuelle Telekommunikationsvorgänge zugegriffen, sondern die staatliche Stelle begibt sich in eine Telekommunikationsbeziehung mit den Betroffenen, um diese Informationen zu ermitteln.[691] Art. 10 Abs. 1 GG schützt aber nur vor dem unberechtigten Zugriff von außen auf eine individuelle Telekommunikationsbeziehung.[692] Dagegen schützt Art. 10 Abs. 1 GG nicht das personengebundene Vertrauen der Kommunikationsbeteiligten zueinander und damit auch nicht davor, dass sich eine staatliche Stelle in eine Kommunikationsbeziehung mit dem Betroffenen begibt.[693] Da es für das Blockchain-Netzwerk keinerlei Zugangsbeschränkungen gibt[694], ist der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet, wenn von staatlichen Stellen zur Kenntnis genommen wird, wie sich eine Transaktionsnachricht im Netzwerk ausgebreitet hat.

Daher ist der Schutzbereich für die Auswertung der Verbreitung von Transaktionsnachrichten nicht eröffnet.

(2) Bloom-Filter-Attacks

Grundsätzlich findet auch bei den oben in Kap. 3 B.III. dargestellten *Bloom-Filter-Attacks* eine Übermittlung von unkörperlich übermittelten Informationen mittels Fernmeldetechnik statt, denn der *full-node* fragt hierzu beim *SPV-Client* alle Bitcoin-Adressen und *public keys* ab, um zu ermitteln, welche Bitcoin-Adresse zur IP-Adresse des *SPV-Clients* gehören.[695]

Fraglich ist hier allerdings, ob in diesem Fall die erforderliche menschliche veranlasste Telekommunikation stattfindet. Denn der betroffene *SPV-Client* verbindet sich lediglich mit dem *full-node,* um dort den *Bloom-Filter*

691 Siehe hierzu oben unter Kap. 3 B.I.
692 Siehe hierzu bereits oben unter Kap. 4 B.I.1.c).
693 BVerfGE 120, 274 (341).
694 Siehe hierzu bereits oben unter Kap. 2 A.II.1.
695 Siehe hierzu ausführlich oben unter Kap. 3 B.III. *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (326ff); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9ff.

mit seinen *Bitcoin-Adressen* und *public keys* zu hinterlegen, um vom *full-node* benachrichtigt zu werden, wenn eine neue Transaktionsnachricht, die ihn betrifft, dort eingeht.[696] Insoweit ist das Hinterlegen des *Bloom-Filters* vergleichbar damit, dass sich ein eingeschaltetes Handy mit einer Funkzelle verbindet, um erreichbar zu sein, wenn dort eine an das Handy gerichtete Kommunikation eintrifft.

Da sich auch die Auswertungsmethode der *Bloom-Filter-Attacks* nur auf die so beim *full-node* hinterlegten *Bloom-Filter* bezieht und hierzu keine weitere Kommunikation zwischen Betroffenem und Ermittelndem erforderlich ist, fehlt es hier an der für Art. 10 Abs. 1 GG erforderlichen menschlich veranlassten Telekommunikation.

Im Übrigen begibt sich bei den *Bloom-Filter-Attacks* wiederum eine staatliche Stelle in eine Kommunikationsbeziehung zu dem Betroffenen, sodass der für Art. 10 Abs. 1 GG erforderliche unautorisierte Zugriff von außen auf Telekommunikation nicht vorliegt.

(3) Verhindern der Verbindung über das Tor-Netzwerk

Fraglich ist allerdings, ob der Schutzbereich des Art. 10 Abs. 1 GG dann betroffen ist, wenn über die bereits dargestellte Auswertung des Netzwerkverhaltens[697] zur Ermittlung von IP-Adressen hinaus, die Verschleierung von IP-Adressen über das *Tor-Netzwerk* verhindert wird.[698] Dies könnte insoweit der Fall sein, als dass durch diese Maßnahme Nutzern ein bestimmter Kommunikationsweg unmöglich gemacht wird, um auf das Blockchain-Netzwerk zuzugreifen und hierdurch die Verschleierung von IP-Adressen unmöglich gemacht bzw. erschwert wird.

Insoweit weist diese Maßnahme Ähnlichkeit mit der im Rahmen des Schutzbereichs dargestellten Verhinderung von Telekommunikation oder mit der Verhinderung von Verschlüsselung von Telekommunikation auf.[699] Wäre diese Maßnahme vergleichbar, könnte man annehmen, dass hier ebenfalls der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet wäre.

Ähnlichkeit des Verhinderns der Verbindung über das *Tor-Netzwerk* besteht zunächst mit der im Rahmen des *Access-Blockings* dargestellten *IP-*

696 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.
697 Siehe hierzu oben unter Kap. 3 B.I., Kap. 4 B.I.1.2.b).
698 Siehe hierzu oben ausführlich unter Kap. 3 B.II.
699 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.d).

Adressen-Sperre[700]. Denn die Maßnahme führt dazu, dass die IP-Adressen der *Tor-Exit-Relays* auf Grund des *DoS*-Schutzes des Blockchain-Netzwerks von der Teilnahme am Blockchain-Netzwerk ausgeschlossen werden.[701] So wird eine unmittelbare Verbindung mit dem Blockchain-Netzwerk über die *Tor-Exit-Relays* verhindert, da die Verbindung über deren bestimmte IP-Adresse verhindert wird – ähnlich wie bei der Sperrmaßnahme der *IP-Adressen-Sperre*, bei der die Verbindung zu einer bestimmten IP-Adresse ebenfalls verhindert wird. Ein Unterschied beider Maßnahmen liegt allerdings in ihrer unterschiedlichen Stoßrichtung. Denn beim *Access-Blocking* wird der Zugriff auf eine bestimmte IP-Adresse verhindert.[702] Beim Verhindern der Teilnahme am Blockchain-Netzwerk über das *Tor-Netzwerk* wird dagegen nur verhindert, über eine bestimmte IP-Adresse zuzugreifen.[703] Sowohl die Verbindung mit dem *Tor-Netzwerk* als auch die Verbindung mit dem jeweiligen Blockchain-Netzwerk bleibt möglich. Nur die Kombination aus beiden wird unterbunden – also die Verbindung *über* das *Tor-Netzwerk mit* dem Blockchain-Netzwerk. Die hier gegenständliche Maßnahme sperrt also nur eine bestimmte IP-Adresse, über die die Verbindung erfolgen kann und nicht die IP-Adresse des Zugriffsziels. Insoweit richtet sich die Maßnahme gegen den Zugreifenden nicht gegen das Zugriffsziel.

Fraglich ist allerdings, ob diese unterschiedliche Stoßrichtung beider Maßnahmen eine andere rechtliche Bewertung zur Folge haben kann.

Gegen eine abweichende rechtliche Bewertung spricht, dass unabhängig davon, gegen wen sich die Verhinderung von Telekommunikation richtet, eine bestimmte Telekommunikationsverbindung verhindert wird. Das Verhindern von Telekommunikation fällt aber auf Grund der Teleologie des Art. 10 Abs. 1 GG gerade nicht in den Schutzbereich des Telekommunikationsgeheimnisses.[704] Sinn und Zweck des Telekommunikationsgeheimnisses ist es, die Vertraulichkeit von Kommunikationsvorgängen vor dem unberechtigten Zugriff von außen zu schützen.[705] Dieser Schutzzweck kann aber

700 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.d)(1); *Durner*, ZUM 2010, 833 (833); *Leistner/Grisse*, GRUR 2015, 19 (23f.).
701 Siehe hierzu ausführlich oben unter Kap. 3 B.II.; *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3f).
702 *Durner*, ZUM 2010, 833 (833); *Leistner/Grisse*, GRUR 2015, 19 (23f.).
703 Siehe hierzu ausführlich oben unter Kap. 3 B.II.; *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f).
704 Siehe hierzu ausführlich oben unter Kap. 4 B.I.1.d).
705 Siehe hierzu insbesondere oben unter Kap. 4 B.I.1.c); BVerfGE 120, 274 (340f.).

gar nicht erreicht werden, wenn keine schützenswerte Telekommunikation vorliegt.

Für eine andere rechtliche Bewertung spricht dagegen, dass durch die Verlagerung der Stoßrichtung – anders als bei der Sperrmaßnahme der *IP-Adressen-Sperre* – nicht Kommunikation als solches verhindert wird, sondern schlicht ein bestimmter Kommunikationsweg. Insoweit kann weiterhin schützenswerte Telekommunikation stattfinden, nur über einen anderen Verbindungsweg. Ziel der Maßnahme ist es nicht, dass keine Verbindung mehr zum Blockchain-Netzwerk aufgebaut wird, sondern nur, dass bei dieser Verbindung IP-Adressen nicht verschleiert werden. Anders als bei der nicht geschützten Verhinderung von Telekommunikation liegt hier insoweit Telekommunikation vor. Damit stellt sich die Frage, ob von Art. 10 Abs. 1 GG auch die Verbindung über einen bestimmten Kommunikationsweg geschützt ist – konkret hier ein Verbindungsweg, der die Kommunikationsumstände verschleiert.

Dementsprechend könnte die hier zu bewertende Maßnahme eher vergleichbar mit der ebenfalls nicht von Art. 10 Abs. 1 GG geschützten Verschlüsselung von Telekommunikation sein. Denn die Umstände der Telekommunikation – die IP-Adressen der Kommunikationsbeteiligten – werden durch die Verwendung des *Tor-Netzwerks* verschleiert. Für das Zugriffsziel ist beim Zugriff über das *Tor-Netzwerk* nicht mehr unmittelbar die IP-Adresse des Zugreifenden erkennbar.[706] Verschleiert werden hierdurch die Telekommunikationsumstände, sodass der Zugriff von außen zur Kenntnisnahme der Telekommunikationsumstände erschwert wird. Dies ähnelt daher der Verschlüsselung von Telekommunikationsinhalten, denn hierdurch wird ebenfalls der Zugriff von außen erschwert bzw. unmöglich gemacht. Die hier gegenständliche Maßnahme verhindert gerade diese Verschleierung der Telekommunikationsumstände.

Gegen die Vergleichbarkeit von Verschlüsselung und Verschleierung spricht zunächst offensichtlich, dass einerseits *Inhalte* und andererseits *Umstände* der Telekommunikation betroffen sind. Hinzukommt, dass nicht Inhalte *verschlüsselt,* sondern Umstände *verschleiert* werden. Fraglich ist aber, ob diese Unterschiede auch einen Unterschied in der rechtlichen Bewertung zur Folge haben können.

Dass der Schutzbereich des Art. 10 Abs. 1 GG die Verschlüsselung nicht erfasst, wird einerseits damit begründet, dass beim Verschlüsselungsvor-

706 Siehe hierzu ausführlich oben unter Kap. 3 B.II.

gang nicht die spezifische Übermittlungsgefahr der Fernkommunikation besteht und deshalb nicht der Schutz des Telekommunikationsgeheimnisses erforderlich ist.[707] Andererseits ist der Verschlüsselungsvorgang ein vom Übermittlungsvorgang getrennt zu betrachtender eigener technischer Vorgang, der zunächst unabhängig von der Übermittlung stattfindet.[708]

Fraglich ist daher, ob diese Begründung auch auf die Verschleierung der IP-Adressen durch das *Tor-Netzwerk* übertragen werden kann.

Dagegen spricht, dass anders als bei Verschlüsselungsvorgängen die Verschleierung mittels des *Tor-Netzwerks* gerade dadurch stattfindet, dass eine Kommunikationsverbindung derart weitergeleitet wird, dass ihr Verbindungsweg von außen nicht mehr nachvollziehbar ist.[709] Die Verschleierung findet also gerade mittels einer bestimmten Telekommunikation statt. Insoweit könnte hier ebenfalls die spezifische Übermittlungsgefahr bestehen – anders als bei einem vorgelagerten Verschlüsselungsvorgang. Dementsprechend könnte man außerdem annehmen, dass die Verschleierung auch kein technisch von der Übermittlung unabhängiger Vorgang ist.

Andererseits liegt auch hier eine andere Stoßrichtung der Maßnahme vor. Denn die Maßnahme verhindert gerade Telekommunikation, bei der die spezifische Übermittlungsgefahr bestehen würde. Von daher ist hier ebenfalls nicht die spezifische Übermittlungsgefahr von Fernkommunikation betroffen. Das erscheint zunächst widersprüchlich, ergibt im Ergebnis aber Sinn. Denn das Telekommunikationsgeheimnis soll seinem Schutzzweck nach davor schützen, dass von außen auf Telekommunikationsinhalte oder -umstände zugegriffen werden kann. Bei einem Verbot von Verschlüsselung etwa ist dieser Schutzzweck nicht erfüllt, da dieses Verbot zwar eine Vorbedingung für den Zugriff auf Telekommunikation schafft, aber hierdurch gerade nicht selbst auf die Telekommunikation zugegriffen wird. Ähnlich ist es daher, wenn faktisch unterbunden wird, dass Telekommunikationsumstände verschleiert werden. Hierdurch wird ebenfalls nicht auf die Telekommunikationsumstände selbst zugegriffen, sondern nur die Bedingung des Zugriffs geschaffen. Wenn aber die Vorbedingung der Verschlüsselung nicht vom Schutzbereich des Telekommunikationsgeheimnisses erfasst ist – da insoweit eben nicht auf Telekommunikation zugegriffen

707 Siehe hierzu oben unter Kap. 4 B.I.1.d)(2).

708 Siehe hierzu oben unter Kap. 4 B.I.1.d)(2); siehe hierzu auch *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 137.

709 Siehe hierzu ausführlich oben unter Kap. 3 B.II.

wird – kann auch die Vorbedingung für den Zugriff auf Telekommunikationsumstände nicht vom Schutzbereich erfasst sein.

Aus diesem Grund ist der Schutzbereich des Telekommunikationsgeheimnisses auch nicht betroffen, wenn zur Ermittlung von IP-Adressen durch das Netzwerkverhalten der beteiligten Nutzer Verschleierungsmöglichkeiten der IP-Adressen über das *Tor-Netzwerk* unterbunden werden.

(4) Auswertung des Datenverkehrs durch Ausnutzen der technischen Funktionsweise des Tor-Netzwerks

Fraglich ist, ob das Telekommunikationsgeheimnis dagegen betroffen ist, wenn nicht nur die Verschleierung von IP-Adressen über das *Tor-Netzwerk* durch technische Eigenheiten des *DoS*-Schutzes eines Blockchain-Netzwerks verhindert wird, sondern darüber hinaus, technische Eigenheiten des *Tor-Netzwerks* ausgenutzt werden, um den Datenverkehr selbst auszulesen und zu ermitteln.[710] Technisch werden hierzu selbst eigene *Tor-Exit-Relays* zur Verfügung gestellt, über die dann der Datenverkehr zum Blockchain-Netzwerk stattfindet.[711] Insoweit begibt sich die ermittelnde Stelle hierdurch selbst in eine Kommunikationsbeziehung zum Betroffenen – sie leitet seinen Datenverkehr an das Blockchain-Netzwerk weiter. Vom Telekommunikationsgeheimnis nicht erfasst ist allerdings das personengebundene Vertrauen in eine Kommunikationsbeziehung[712] – denn hierbei findet kein Zugriff von außen auf stattfindende Telekommunikation statt. Insoweit schützt Art. 10 Abs. 1 GG nicht davor, dass sich der Staat nicht in eine Kommunikationsbeziehung mit dem Betroffenen begibt.[713]

Aus diesem Grund ist auch hier der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet.

(5) Zwischenergebnis

Auch die Daten der Netzwerkverbindungen bei Blockchain-Systemen sind nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst. Insbesondere sind auch diese Daten keine geschützte Individualkommunikation. Auch, wenn

710 Siehe hierzu bereits oben unter Kap. 3 B.II.
711 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (125f.).
712 BVerfGE 120, 274 (340f.) m.w.N.
713 BVerfGE 120, 274 (340f.).

ein bestimmter Kommunikationsweg verhindert wird, ist hiervon nicht der Schutzbereich des Art. 10 Abs. 1 GG betroffen.

c) Anderweitig verfügbare Daten als geschützte Telekommunikation

Schließlich stellt sich die Frage, ob durch die Auswertung der in Kapitel 3 C. dargestellten weiteren verfügbaren Daten der Schutzbereich des Art. 10 Abs. 1 GG betroffen sein könnte. Da hier wiederum keine einheitliche Datengrundlage vorliegt, wird nach den einzelnen Maßnahmen differenziert.

(1) Durchsuchen des Internets nach Bitcoin-Adressen

Soweit mittels *Web-Crawler*[714] das Internet nach veröffentlichten Bitcoin-Adressen durchsucht wird, wird hierzu keinerlei Zugangsbeschränkung zum Zugriff auf die Kommunikation überschritten, sodass kein unautorisierter Zugriff von außen auf vertrauliche Kommunikation vorliegt. Damit liegt hierbei keine geschützte Individualkommunikation vor, sodass der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet ist.

(2) Auswertung von Dritt-Anbieter-Cookies

Ob bei der Auswertung von Dritt-Anbieter-Cookies[715] der Schutzbereich des Art. 10 Abs. 1 GG betroffen ist, hängt maßgeblich davon ab, woher die Daten der Dritt-Anbieter-Cookies stammen. Soweit auf die an Dritte übermittelten Daten von außen zugegriffen wird, erscheint es möglich, dass der hierdurch auf geschützte Telekommunikation zugegriffen wird. Soweit der Dritte, an den die Daten in Kenntnis des Betroffenen zur Abwicklung als Dienstleister übermittelt werden, und dieser die Auswertung vornimmt, liegt hier wiederum kein Zugriff von außen auf eine Telekommunikationsbeziehung vor, sodass der Schutzbereich des Art. 10 Abs. 1 GG nicht betroffen ist.

714 Siehe hierzu oben Kap. 3 C.I.
715 Siehe hierzu oben Kap. 3 C.II.

(3) Standort-Daten-Ermittlung bei IoT-Blockchain-Anwendungen

Dies gilt ähnlich bei Auswertungen im Zusammenhang mit IoT-Blockchain-Anwendungen[716]. Ob hiervon der Schutzbereich des Telekommunikationsgeheimnisses betroffen ist, hängt maßgeblich von den jeweils stattfindenden Telekommunikationsbeziehungen ab. Da es bisher weder konkrete und eingesetzte blockchain-basierte IoT-Anwendungen gibt noch entsprechende konkrete Auswertungsmethoden, kann von daher hierzu kein einheitliches Ergebnis festgestellt werden.

Die bisher lediglich theoretische Auswertungsmöglichkeit von *Shahid et.al.*[717] beruht etwa darauf, dass andere Verkehrsteilnehmer, mit denen der Betroffene (bzw. das Ziel der Auswertung) über die Blockchain seine Fahrdaten ausgetauscht hat, ihrerseits Standortdaten an eine auswertende Stelle übermitteln.[718] So könnten Rückschlüsse darauf gezogen werden, wann der Betroffene an welchem Ort war.[719] Diese Rückschlüsse können dahingehend erweitert werden, dass klassische Navigationsalgorithmen[720] verwendet werden, um die Strecke zwischen zwei oder mehr bekannten Punkten des Betroffenen zu berechnen und so Rückschlüsse auf sein Bewegungsprofil zu erhalten.[721]

Allerdings schützt das Telekommunikationsgeheimnis nicht das personengebundene Vertrauen in den Kommunikationsbeteiligten[722], sodass der Schutzbereich des Art. 10 Abs. 1 GG hier nicht eröffnet ist.

Soweit darüber hinaus allerdings die Zuordnung eines zur Blockchain-Kommunikation verwendeten *public keys* zu einer natürlichen Person durch die Abfrage bei einer zentralen, die *public keys* verwaltenden Stelle, ermittelt wird[723], käme dagegen eine Schutzbereichseröffnung des Telekom-

716 Siehe hierzu oben Kap. 3 C.III.

717 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (116ff.).

718 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 116 (120).

719 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 116 (120).

720 Bspw. Google Maps (https://www.google.com/maps letzter Abruf: 20. Dezember 2021).

721 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 116 (120).

722 Siehe hierzu oben ausführlich unter Kap. 4 B.I.1.c); BVerfGE 120, 274 (341).

723 So eine der von *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 116 (120) dargestellten, theoretischen Auswertungsmöglichkeiten.

munikationsgeheimnisses für den Schutz der Telekommunikationsumstände grundsätzlich in Betracht.

d) Zwischenergebnis

Die Daten, die von den in Kapitel 3 dargestellten Methoden ausgewertet werden, sind nicht vom Schutzbereich des Art. 10 Abs. 1 GG erfasst, da sie weitgehend nicht die für das Telekommunikationsgeheimnis erforderliche Individualkommunikation darstellen.

3. Zwischenergebnis

Der Schutzbereich des Telekommunikationsgeheimnis ist daher bei den in Kapitel 3 dargestellten Auswertungsmethoden nicht eröffnet.

II. Recht auf informationelle Selbstbestimmung – „RiS"

Allerdings könnte durch die dargestellten Auswertungsmethoden ein Eingriff in das sog. Recht auf informationelle Selbstbestimmung (nachfolgend als „RiS" bezeichnet) vorliegen, da durch die Erhebung und Auswertung der Blockchain-Daten, der Daten über das Netzwerkverhalten und anderweitig verfügbare Daten personenbezogene Daten betroffen sein könnten.

Dabei stellen sich drei wesentliche Probleme und Fragen:

- Sind die im Rahmen der Auswertungen erhobenen Daten „personenbezogene Daten" im Sinne des RiS?
- Wie wirkt es sich aus, dass die erhobenen und ausgewerteten Daten keinerlei Zugangsbeschränkungen unterliegen und insoweit öffentlich zugängliche Daten[724] sein könnten?
- Wirkt es sich auf den Schutzbereich oder den Eingriff in das RiS und die Abgrenzung zum Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus, dass die in einer Blockchain enthaltenen Daten bereits systematisch und chronologisch geordnet sind?

Um diese Fragen zu beantworten, wird nachfolgend zunächst der Schutzbereich des RiS und seine Herleitung dargestellt (hierzu unter 1.) und

724 Siehe zur Begriffsbestimmung öffentlich zugänglicher Daten sogleich unter Kap. 4, B.III.1.d)(1).

anschließend thematisiert wodurch ein Eingriff hierin vorliegen kann und welche Grenzen hier zu beachten sind (hierzu unter 2.).

I. Schutzbereich

Der Schutzbereich des RiS umfasst im Grundsatz die Befugnis des Einzelnen selbst über die Preisgabe seiner personenbezogenen Daten zu entscheiden.[725]

a) Herleitung des RiS – insbesondere Volkszählungsurteil des BVerfGE[726]

Das RiS wurde vom BVerfG im sog. Volkszählungsurteil von 1983 als Ausprägung des Allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschaffen[727], um den Gefahren für die Persönlichkeit des Einzelnen zu begegnen, die sich aus der Datenverarbeitung mit moderner Informationstechnologie ergeben.[728]

Das BVerfG begründet die Notwendigkeit des RiS damit, dass vom Allgemeinen Persönlichkeitsrecht auch die Befugnis des Einzelnen umfasst sei, selbst zu entscheiden, welche persönlichen Lebenssachverhalte wann und innerhalb welcher Grenzen offenbart würden.[729] Diese Befugnis müsse nach dem BVerfG auch an die modernen Bedingungen der Datenverarbeitung angepasst werden, mit denen es möglich sei, aus verschiedenen Einzelangaben ein teilweises oder vollständiges Persönlichkeitsbild zu erstellen.[730]

Von dieser Informationserhebung und -verarbeitung sei das Allgemeine Persönlichkeitsrecht insoweit betroffen, als dass der Einzelne, der nicht wisse, welche Daten über ihn erhoben und verarbeitet würden, in seiner Freiheit gehemmt sei, selbst zu entscheiden und zu handeln.[731] Denn das Allgemeine Persönlichkeitsrecht erfasse im Grundsatz die freie Entfaltung

725 *Hufen*, Staatsrecht II - Grundrechte, § 12 Rn. 4; Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Abs. 1 Rn. 175; *Bauer*, Soziale Netzwerke, S. 105; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 26.
726 BVerfGE 65, 1ff.
727 BVerfGE 65, 1 (43).
728 BVerfGE 65, 1 (42).
729 BVerfGE 65, 1 (42) mit Verweis auf BVerfGE 56, 37 (41ff.); BVerfGE 63, 131 (142f.).
730 BVerfGE 65, 1 (42).
731 BVerfGE 65, 1 (43).

der Persönlichkeit des Einzelnen erfasse.[732] Diese freie Entfaltung der Persönlichkeit sei eingeschränkt, wenn der Einzelne seine Entscheidungen und Handlungen nicht frei treffen könne, weil er nicht wisse, welche Informationen über ihn erhoben und verarbeitet würden.[733]

Darüber hinaus nimmt das BVerfG[734] an, dass das RiS nicht nur auf Grund einer möglichen Verhaltenseinschränkung des Einzelnen betroffen sein könne, sondern auch dadurch, dass die berechtigten Geheimhaltungsinteressen des Einzelnen durch die Verknüpfung von Informationen berührt sein können.[735]

Aus diesen Gründen setze die freie Entfaltung der Persönlichkeit den effektiven Schutz vor unbegrenzter „Erhebung, Speicherung, Verwendung und Weitergabe […] persönliche[r] Daten voraus"[736], der durch das RiS gewährleistet werde und „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[737] erfasse.

Hierdurch erweitert und flankiert das RiS den grundrechtlichen Schutz der Verhaltensfreiheit und Privatheit, indem der Schutz schon auf der Stufe der Persönlichkeitsgefährdung beginnt.[738] Nach dem BVerfG kann eine derartige Gefährdungslage schon „im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden, die der Betroffene weder überschauen noch verhindern kann."[739]

b) Schutz von personenbezogenen Daten

Geschützt sind personenbezogene Informationen.[740] Das BVerfG benennt diese im Volkszählungsurteil als „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (perso-

732 BVerfGE 65, 1 (43).
733 BVerfGE 65, 1 (43).
734 BVerfGE 120, 378ff.
735 BVerfGE 120, 378 (398); BVerfGE 118, 168 (184f.) mit Verweis auf BVerfGE 65, 1 (42f.), BVerfGE 113, 29 (45f.), BVerfGE 115, 320 (342).
736 BVerfGE 65, 1 (43).
737 BVerfGE 65, 1 (43).
738 BVerfGE 120, 274 (312)
739 BVerfGE 120, 274 (312).
740 BVerfGE 65, 1 (42); BVerfGE 118, 168 (184) m.w.N.

nenbezogene Daten [vgl. 2 Abs. 1 BDSG])“[741]. Hiervon erfasst sind nicht nur sensible Daten, sondern auch Daten, die für sich genommen nur einen geringen Informationsinhalt haben[742], da diese „je nach Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit haben“[743] können. Hintergrund dieser umfassenden Erfassung personenbezogener Daten ist, dass sich durch moderne Möglichkeiten elektronischer Datenverarbeitung auch aus Informationen mit geringem Gehalt durch Verknüpfung neue Informationen ergeben können, die über den Gehalt der einzelnen Information hinausgehen können.[744]

Unklar ist in diesem Zusammenhang allerdings zunächst, unter welchen Voraussetzungen eine „bestimmbare Person“[745] vorliegt. Relevant ist dies insbesondere vor dem Hintergrund der ausgewerteten Blockchain-Daten, da die dort verwendeten *public keys* selbst zunächst keinerlei Rückschlüsse auf die hinter ihnen stehenden Personen oder Organisationen ermöglichen[746] und insbesondere anders als bei herkömmlichen Kennziffern oder Kennzeichen keine zentrale Verwaltungsstelle besteht, die einen derartigen Personenbezug herstellen kann.[747]

Insoweit stellt sich die Frage, ab wann eine Person „bestimmbar“ ist.

(1) Rechtsprechung des BVerfG

Im grundlegenden Volkszählungsurteil des BVerfG verweist der Senat in diesem Zusammenhang auf den damals geltenden § 2 Abs. 1 BDSG, der in seiner damaligen Fassung wie folgt lautete[748]:

741 BVerfGE 65, 1 (42).
742 BVerfGE 120, 274 (312).
743 BVerfGE 120, 274 (312) mit Verweis auf BVerfGE 118, 168 (184f.).
744 BVerfGE 120, 274 (312) mit Verweis auf BVerfGE 65, 1 (42), BVerfGE 113, 29 (45f.); BVerfGE 115, 320 (342); BVerfGE 118, 168 (184f.).
745 BVerfGE 65, 1 (42).
746 Siehe hierzu bereits ausführlich unter Kap. 2, A.II.2. mit Verweis auf *Boehm/Pesch*, MMR 2014, 75 (76).
747 Siehe hierzu bereits ausführlich unter Kap. 2, A.III. mit Verweis auf *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1f.; *Kaulartz*, CR 2016, 474 (476).
748 Bis zur am 23.05.2018 in Kraft getretenen VO (EU) 2016/679 (nachfolgend als „DSGVO“ bezeichnet) galt diese Begriffsbestimmung der personenbezogenen Daten im BDSG fort, später allerdings in § 3 Abs. 1 BDSG.

> *„Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangeben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“*

Diesen Wortlaut übernimmt das BVerfG wortgleich in seine Volkszählungs-Entscheidung.[749] In späteren Entscheidungen des BVerfG zum RiS übernimmt das Gericht diese Formulierung jeweils mit einem Verweis auf das grundlegende Volkszählungsurteil[750] – ein erneuter Verweis auf eine entsprechende Vorschrift im BDSG fehlt dagegen in nachfolgenden Entscheidungen. Zur Frage, wann eine Person „bestimmbar“ ist, hat sich das BVerfG bisher allerdings nicht allgemeingültig geäußert.

Allerdings gibt das BVerfG im Urteil zur Verfassungsmäßigkeit des Gentechnikgesetzes[751] an, dass jedenfalls ein „bestimmbarer“ Personenbezug vorläge, wenn „eine unbestimmte Vielzahl von Empfängern über Zusatzwissen verfüg[e], das es ihnen ohne großen zeitlichen oder finanziellen Aufwand ermöglich[e], die Bezugsperson zu identifizieren“[752].

Konkret ging es im gegenständlichen Verfahren unter anderem um ein im Internet abrufbares Standortregister mit Angaben zu freigesetzten und angebauten gentechnisch veränderten Organismen.[753] In dem allgemein zugänglichen Teil des Standortregisters waren nur Angaben zu sachlichen Verhältnissen und keine persönlichen Angaben, wie Namen und Anschriften, enthalten.[754] Das BVerfG nahm in diesem Zusammenhang jedoch an, dass auch die allgemein zugänglichen Informationen über lediglich sachliche Verhältnisse nicht ihren Personenbezug verlieren würden.[755] Dieser bestehe „fort, solange die Bezugsperson ‚bestimmbar‘ oder ‚individualisierbar‘“[756] bleibe, sodass es maßgeblich auf die Abgrenzung der Bestimmbarkeit ankäme.[757] Da es ohne Weiteres – insbesondere für Ortsansässige –

749 BVerfGE 65, 1 (42).
750 Siehe etwa BVerfGE 67, 100 (143); BVerfGE 84, 239 (279); BVerfGE 103, 21 (33); BVerfGE 115, 320 (341); BVerfG NJW 2008, 1335 (1436); BVerfGE 120, 378 (397f.); BVerfGE 128, 1 (43); BVerfGE 147, 50 (142); BVerfGE 150, 244 (264). In seinen Entscheidungen spricht das BVerfG allerdings häufig auch von „individualisierbaren“ Informationen und nicht immer nur von „bestimmbaren“ Informationen.
751 BVerfGE 128, 1 ff.; zur Bezeichnung der Entscheidung siehe BVerfG NVwZ 2011, 94 ff.
752 BVerfGE 128, 1 (46).
753 BVerfGE 128, 1 (45f.); ZUR 2011, 133 (139).
754 BVerfGE 128, 1 (45f.).
755 BVerfGE 128, 1 (46).
756 BVerfGE 128, 1 (46).
757 BVerfGE 128, 1 (46).

möglich sei, einen unmittelbaren Personenbezug herzustellen, entfiele nicht bereits dadurch der Personenbezug, dass die gegenständlich veröffentlichten Daten keinen unmittelbaren Personenbezug enthielten.[758]

Hieraus lässt sich zunächst annehmen, dass „Bestimmbarkeit" nach der Rechtsprechung des BVerfG jedenfalls vorliegt, wenn es für mehrere Personen möglich ist mit einem verhältnismäßigen Aufwand, einen Personenbezug herzustellen.[759]

Offen bleibt in diesem Zusammenhang allerdings, welche Personen den Personenbezug herstellen können müssen und wie die Grenze des verhältnismäßigen Aufwands zu bestimmen ist.

Diese Fragen sind auch im Rahmen des Datenschutzrechts umstritten. Insoweit werden die im Datenschutzrecht vertretenen Positionen im Folgenden zunächst vorgestellt, um anschließend darauf einzugehen, ob und inwieweit die Grundsätze des Datenschutzrechts zur Auslegung des RiS herangezogen werden können.

(2) „Bestimmbarkeit" im Datenschutzrecht

Bereits im Zusammenhang mit der Vorschrift des § 2 Abs. 1 bzw. § 3 Abs. 1 BDSG war umstritten, ab wann eine Person „bestimmbar" ist.[760]

Hierzu wird ein Meinungsspektrum von der sog. relativen Theorie (auch sog. subjektive Theorie) bis zur sog. absoluten Theorie (auch sog. objektive Theorie) vertreten.[761] Dabei sind relative und objektive Theorie jeweils die Extrempositionen.[762] Beide Positionen werden in der Regel aber nicht in ihrer Reinform vertreten.[763]

Nach der relativen bzw. subjektiven Theorie kommt es für die Bestimmbarkeit darauf an, ob die verarbeitende Stelle (nachfolgend auch als „Ver-

758 BVerfGE 128, 1 (46).

759 So etwa auch BeckOK-InfoMedienR/*Guckelberger,* IFG § 5 Rn. 4 zu personenbezogenen Daten im Informationsfreiheitsrecht, die in diesem Zusammenhang auf die zitierte Verfassungsrechtsprechung abstellt, um diese Grenze der Bestimmbarkeit zu ziehen.

760 Siehe hierzu ausführlich *Bergt*, ZD 2015, 365 (365f.); *Herbst*, NVwZ 2016, 902 (903f.).

761 Siehe hierzu ausführlich *Herbst*, NVwZ 2016, 902 (904f.); *Bergt*, ZD 2015, 365 (365f.).

762 Siehe hierzu ausführlich *Herbst*, NVwZ 2016, 902 (904f.); *Bergt*, ZD 2015, 365 (365f.).

763 *Herbst*, NVwZ 2016, 902 (904).

antwortlicher" bezeichnet) selbst die Möglichkeit hat, einen unmittelbaren Personenbezug herzustellen.[764] Insoweit hängt die Frage, ob personenbezogene Daten vorliegen, von der Perspektive des Verantwortlichen ab und kann insoweit nicht einheitlich beantwortet werden.[765]

Eine abgemilderte Variante dieser Position stellt auch auf mögliches Zusatzwissen Dritter ab, das sich der Verantwortliche aneignen kann.[766]

Dagegen stellt die absolute bzw. objektive Theorie darauf ab, ob es grundsätzlich – also für irgendjemanden – möglich ist, einen Personenbezug herzustellen.[767] Diese Position wird in der Regel jedoch auch abgemildert vertreten, und zwar dahingehend, dass es darauf ankommt, ob ein Personenbezug mit einem verhältnismäßigen Aufwand hergestellt werden kann.

Bis zur am 25.05.2018 in Kraft getretenen VO (EU) 2016/679 (nachfolgend als „DSGVO" bezeichnet) galt diese Begriffsbestimmung der personenbezogenen Daten in der Form des § 2 Abs. 1 bzw. § 3 Abs. 1 BDSG[768] fort[769]. Mit Inkrafttreten der DSGVO wurde auch das BDSG an die Änderungen der DSGVO angepasst. So bestimmt nun § 46 Nr. 1 BDSG den Begriff der personenbezogenen Daten wortgleich wie die Vorschrift des Art. 4 Nr. 1 DSGVO als:

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann"*

Auch hieraus ergibt sich allerdings keine klare Vorgabe zur Bestimmbarkeit personenbezogener Daten.[770] Denn im Wesentlichen wurde hierdurch

764 *Herbst*, NVwZ 2016, 902 (903).
765 *Bergt*, ZD 2015, 365 (365f.).
766 *Herbst*, NVwZ 2016, 902 (904).
767 *Herbst*, NVwZ 2016, 902 (903f.).
768 Die Begriffsbezeichnung der personenbezogenen Daten ist lediglich von § 2 Abs. 1 BDSG in § 3 Abs. 1 BDSG verschoben worden.
769 Sie befand sich später allerdings in § 3 Abs. 1 BDSG.
770 Zur Rechtsprechung des EuGH zum Personenbezug dynamischer IP-Adresse und die in den Erwägungsgründen Nr. 26 zur DSGVO enthaltenen Angaben sogleich.

nur der Begriff der „Einzelangaben über persönliche und sachliche Verhältnisse" des Einzelnen durch „Informationen" ersetzt und die Vorgabe der Bestimmbarkeit durch die „Identifizierbarkeit" ausgetauscht.[771] Auch die in Art. 4 Nr. 1 Hs. 2 DSGVO enthaltene nähere Bestimmung, wann eine Person als „identifizierbar" angesehen wird, enthält insoweit nur eine gesetzliche Vermutungsregel, wann Identifizierbarkeit vorliegt. Eine klare Vorgabe für ein objektives oder subjektives Verständnis der Bestimmbarkeit personenbezogener Daten, ist allerdings auch hieraus nicht erkennbar. Allerdings gibt Erwägungsgrund Nr. 26 zur DSGVO[772] zur Bestimmbarkeit natürlicher Personen folgendes an:

> *„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."*

In diesem Zusammenhang und diesem Sinne entschied auch der EuGH, dass dynamische IP-Adressen „bestimmbare" personenbezogene Daten seien, wenn die verarbeitende Stelle „über rechtliche Mittel verfüg[e], die es ihm erlauben, die betreffende Person anhand von Zusatzinformationen […] bestimmen zu lassen."[773]

Die Entscheidung des EuGH bezog sich hierbei noch auf die vor der DSGVO geltende RL (EG) 95/46 (nachfolgend als „DS-RL" bezeichnet), in

771 So etwa *Krügel*, ZD 2017, 455 (455f.).

772 Und fast wortgleich auch Erwägungsgrund Nr. 21 zur RL (EU) 2016/680.

773 EuGH NJW 2016, 3579 Ls. 1, allerdings noch zu der vor der DSGVO geltenden RL (EG) 95/46 (nachfolgend als „DS-RL" bezeichnet). Die Vorschriften zu personenbezogenen Daten unterscheiden sich allerdings lediglich darin, dass Art. 2 lit. a) DS-RL von „bestimmte[n] oder bestimmbare[n] natürliche[n] Person" spricht, wohingegen Art. 4 Nr. 1 DSGVO den Begriff der Bestimmtheit bzw. Bestimmbarkeit durch eine „identifizierte oder identifizierbare natürliche Person" ersetzt. Siehe zu den begrifflichen Unterschieden, die sachlich wohl keinen Unterschied ausmachen werden *Krügel*, ZD 2017, 455 (455f.).

der in Art. 2 lit. a) eine mit Art. 4 Nr. 1 DSGVO vergleichbare Bestimmung enthalten war.[774]

Nach der vom EuGH vertretenen Auffassung kommt es daher maßgeblich darauf an, ob die verarbeitende Stelle die tatsächliche und rechtliche Möglichkeit hat, um die betroffene Person zu identifizieren.[775] Ausgangspunkt ist insoweit nach dem EuGH eine subjektive Perspektive, nach der es auf die Möglichkeiten der jeweiligen datenverarbeitenden Stelle ankommt und inwieweit der Verantwortliche gesetzlich zulässige Zusatzinformationen hinzuziehen kann und ob dies in einem wirtschaftlich vertretbaren Verhältnis zum erstrebten Ziel steht.[776]

Der Maßstab zur Bestimmbarkeit von Daten im Datenschutzrecht ist insoweit, ob die verarbeitende Stelle in einer rechtlich zulässigen Art und Weise Zusatzinformationen heranziehen kann und dies in einem wirtschaftlich vertretbaren Verhältnis zum Ziel der Verarbeitung steht.

(3) Anwendbarkeit dieser Maßstäbe im Verfassungsrecht

Insoweit stellt sich nun die Frage, ob dieser Maßstab des Datenschutzrechts zur Bestimmbarkeit personenbezogener Daten auch im Rahmen des grundrechtlich geschützten RiS angewendet werden kann.

Dafür spricht zunächst der wörtliche Verweis des BVerfG im grundlegenden Volkszählungsurteil auf die Bestimmung des § 2 Abs. 1 BDSG.[777] Es ließe sich insoweit annehmen, dass das BVerfG für die Definition und Auslegung des Begriffs der personenbezogenen Daten auf das geltende Datenschutzrecht verweist.

Dem steht zunächst entgegen, dass das BVerfG mit dem Zusatz „vgl." auf § 2 Abs. 1 BDSG verweist, sodass eher davon auszugehen ist, dass beide Definitionen im konkreten Fall deckungsgleich sind[778], aber keine Rückschlüsse für die weitergehende Auslegung der Begriffe gezogen werden können.

Außerdem ist der Schutzumfang grundrechtlicher Gewährleistungen grundsätzlich autonom auszulegen und unabhängig von einfachgesetzli-

774 *Krügel*, ZD 2017, 455 (455f.).
775 Specht/Mantz-HdB DSR/*Mantz/Marosi*, § 3 Rn. 14.
776 Specht/Mantz-HdB DSR/*Mantz/Marosi*, § 3 Rn. 14; *Krügel*, ZD 2017, 455 (459).
777 BVerfGE 65, 1 (42).
778 So etwa Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Abs. 1 Rn. 175.

chen Vorschriften[779] – insbesondere ist das Recht auf informationelle Selbstbestimmung nicht auf den Anwendungsbereich der jeweiligen Datenschutzgesetze des Bundes und der Länder beschränkt.[780] Unter Umständen können jedoch auch die einfachgesetzlichen Normen des Datenschutzrechts zur Erläuterung der Begriffsbestimmung personenbezogener Daten zunächst herangezogen werden.[781] Dies erfordert jedoch, dass kein wesentlicher Unterschied zwischen den Normen des Datenschutzrechts und des RiS bzw. deren Sinn und Zweck besteht.

Sinn und Zweck des RiS ist es, einerseits den Schutz berechtigter Geheimhaltungsinteressen des Einzelnen und andererseits den Schutz der freien Entfaltung der Persönlichkeit dadurch zu gewährleisten, dass der Einzelne nicht auf Grund seiner Unkenntnis der über ihn erhobenen Daten sein Verhalten und seine Entscheidungen verändert.[782] Auch das einfachgesetzliche Datenschutzrecht dient diesem Zweck, dass es für den Einzelnen überblickbar sein muss, welche Daten über ihn erhoben und verarbeitet werden.[783] Insoweit ließe sich annehmen, dass keine wesentlichen Unterschiede zwischen RiS und Datenschutzrecht bestehen.

Problematisch ist allerdings die Anwendung der Rechtsprechung des EuGH zur Bestimmbarkeit von Personen dahingehend, dass der EuGH darauf abstellt, ob der verarbeitenden Stelle „rechtliche Mittel" zur Verfügung stehen, um den unmittelbaren Personenbezug herzustellen.[784] Es erscheint insoweit auf den ersten Blick widersprüchlich, die Frage, ob ein grundrechtlich geschütztes Verhalten vorliegt, davon abhängig zu machen, ob eine einfachgesetzliche Möglichkeit besteht, einen Personenbezug herzustellen. Dieser Widerspruch kann allerdings dahingehend aufgelöst werden, dass nur dann die freie Entfaltung der Persönlichkeit des Einzelnen gefährdet ist, wenn er befürchten muss, dass die über ihn erhobenen Daten auch in einen unmittelbaren Bezug zu ihm gesetzt werden können. Da gerade nicht von einem rechtswidrigen Handeln des Staates ausgegangen werden kann, ist es auch zur Bestimmung des Schutzbereichs des RiS

779 Stern/*Stern*, Staatsrecht: Die einzelnen Grundrechte Bd. IV/1, § 99 S. 233f.
780 BVerfGE 78, 77 (84).
781 Stern/*Stern*, Staatsrecht: Die einzelnen Grundrechte Bd. IV/1, § 99 S. 233f.
782 Siehe hierzu bereits oben ausführlich unter Kap. 4, III.1.a) mit Verweisen auf BVerfGE 65, 1 (42f.); BVerfGE 113, 29 (45f.), BVerfGE 115, 320 (342); BVerfGE 118, 168 (184f.); BVerfGE 120, 378 (398).
783 Siehe insoweit Erwägungsgründe Nr. 1, 2 DSGVO, die darauf abstellen, dass die DSGVO dem Schutz der Grundrechte der Bürger innerhalb der Union dienen sollen.
784 EuGH ZD 2017, 24 (26).

vorzugswürdig, darauf abzustellen, ob dem Staat als verarbeitende Stelle tatsächliche und rechtliche Möglichkeiten zur Verfügung stehen, um einen unmittelbaren Personenbezug herzustellen.

(4) Zwischenergebnis

Das RiS schützt Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren bzw. identifizierbaren Person.[785] Bestimmbar ist eine Person nach dem BVerfG jedenfalls, wenn mehrere Personen anhand von Zusatzwissen ohne wesentlichen Aufwand einen unmittelbaren Personenbezug herstellen können.[786] Weiterhin kommt es für die Frage, ob eine Person bestimmbar ist, darauf an, ob die jeweils verarbeitende Stelle tatsächlich und rechtlich dazu in der Lage ist, mit einem nicht unverhältnismäßigen Aufwand einen Personenbezug herzustellen.[787] Für die Frage der Verhältnismäßigkeit kommt es darauf an, dass das Herstellen eines unmittelbaren Personenbezugs vom tatsächlichen und wirtschaftlichen Aufwand nicht außer Verhältnis zu dem mit der Verarbeitung angestrebten Zweck steht.[788]

c) Ausgewertete Daten als personenbezogene Daten?

Insoweit stellt sich nun die Frage, ob die von den Auswertungsmethoden erhobenen und ausgewerteten Daten personenbezogene Daten in diesem Sinne sind.

785 Ständige Rechtsprechung des BVerfG: BVerfGE 67, 100 (143); BVerfGE 84, 239 (279); BVerfGE 103, 21 (33); BVerfGE 115, 320 (341); BVerfG NJW 2008, 1335 (1436); BVerfGE 120, 378 (397f.); BVerfGE 128, 1 (43); BVerfGE 147, 50 (142); BVerfGE 150, 244 (264).

786 BVerfGE 128, 1 (46).

787 In entsprechender Anwendung EuGH ZD 2017, 24 (26). Zu diesem Ergebnis kommen auch *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 77; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 27, die allerdings ohne weitere Begründung davon ausgehen, dass die im Datenschutzrecht geltenden Grundsätze zur „Bestimmbarkeit" einer Person auch im Rahmen des RiS Anwendung finden.

788 In entsprechender Anwendung EuGH ZD 2017, 24 (26).

(1) Unmittelbare Blockchain-Daten

Die in Kap. 3 A. dargestellten Auswertungsmethoden werten zunächst die unmittelbaren Blockchain-Daten aus.[789] Die Blockchain-Daten enthalten Informationen über Transaktionen im jeweiligen Anwendungskontext der einzelnen Blockchain – in der Regel betrifft dies bisher Transaktionen von Kryptowährungen.[790]

Auch Kontotransaktionen haben Persönlichkeitsrelevanz, da sie unter anderem Rückschlüsse auf das Konsumverhalten, soziale Kontakte und Gewohnheiten des Einzelnen zulassen.[791] Nichts anderes kann insoweit für Kryptowährungen gelten, sodass hierin Einzelangaben über sachliche Verhältnisse des Einzelnen zu sehen sind.[792] Soweit die Blockchain-Technologie in einer anderen Form angewendet wird, dürften die in ihr enthaltenen Daten ebenfalls vom Schutzbereich des RiS erfasst sein[793], da auch sie über sachliche Verhältnisse des Einzelnen Auskunft geben können und sich nach der Rechtsprechung des BVerfG der Schutz des RiS auf alle Informationen erstreckt, die über die Bezugsperson etwas aussagen können.[794]

Fraglich ist allerdings, ob die Blockchain-Daten auch personenbezogene Daten sind.[795] Denn die dort verwendeten *public keys* lassen zunächst keinerlei Rückschlüsse auf die dahinterstehenden *Entitäten* zu.[796] Anders als bei Kontodaten[797], Kfz-Kennzeichen[798] und dynamischen IP-Adressen[799] gibt es bei *public keys* auf Grund der dezentralen Verwaltung auch keine zentrale Instanz, die etwa ein Register über die Zuordnung von *public keys* zu *Entitäten* führt und so die Zuordnung eines *public keys* zu einer *Entität* ermöglichen kann.[800]

789 Gegebenenfalls unter Hinzuziehung von Daten über Hintergründe von bekanntem Transaktionsverhalten.
790 Siehe hierzu ausführlich oben unter Kap. 2 A.II.8, B.
791 Siehe hierzu ausführlich BVerfGE 118, 168 (185f.).
792 Siehe hierzu bereits *Rückert*, ZStW 129 (2017), 302 (315).
793 Soweit ein Personenbezug besteht. Hierzu sogleich.
794 BVerfGE 128, 1 (44).
795 Siehe zu der Frage, ob Blockchain-Daten personenbezogene Daten im Sinne der DSGVO sind, bereits ausführlich *Finck*, Blockchain and the GDPR, S. 14ff.
796 Siehe hierzu bereits ausführlich Kap. 2 A.II.2., 3. mit Verweis auf *Boehm/Pesch*, MMR 2014, 75 (76).
797 Siehe hierzu BVerfGE 118, 168 (185f.).
798 Siehe hierzu BVerfGE 150, 244 (269); BVerfGE
799 Siehe hierzu EuGH NJW 2016, 3579 (3581).
800 Vgl. *Boehm/Pesch*, MMR 2014, 75 (76).

Allerdings ist es nicht ausgeschlossen, dass ein Personenbezug hergestellt werden kann. Ziel der dargestellten Auswertungsmethoden zu Strafverfolgungszwecken ist es ja gerade, die *public keys* einer *Entität*[801] zuzuordnen.[802]

Hinzukommt, dass nach dem zum 01.01.2020 in Kraft getretenen Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie nun unter anderem auch Dienstleister im Zusammenhang mit virtuellen Währungen[803] „Verpflichtete" im Sinne des Gesetzes zum Aufspüren von Gewinnen aus schweren Straftaten (nachfolgend als „GwG" bezeichnet) sind. Insoweit müssen diese Dienstleister das sog. „*Know-Your-Customer-Prinzip*" des Geldwäschepräventionsrechts anwenden und sind hieraus insbesondere dazu verpflichtet, jegliche Kunden zu identifizieren und deren Identitäten zu überprüfen.[804] Hiernach sollen nun auch „Dienstleistungsanbieter […], die den Umtausch von gesetzlichen Währungen in virtuelle Währungen und umgekehrt ausführen, sowie […] Anbieter, von elektronischen Geldbörsen"[805] dem KYC-Prinzip unterliegen.[806] Diese gesetzliche Regelung setzt insoweit an der Schnittstelle zwischen virtueller und analoger Welt an. Ziel ist es, die Anonymität der Nutzer von Kryptowährungen soweit es geht aufzuheben.[807] So ist es im Verdachtsfall für die Strafverfolgungsbehörden möglich, nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG über die Zentralstelle für Finanztransaktionsuntersuchung, Informationen über Identitäten von *public keys* bei Krypto-

801 Siehe zum Begriff der Entität oben unter Kap. 3, A.I. Eine Entität ist hiernach eine Person oder Organisation, die über eine oder mehrere Bitcoin-Adressen verfügen kann.

802 Siehe hierzu bereits ausführlich Kap. 4, A.

803 Nachfolgend werden diese Dienstleister einheitlich als „Kryptowährungsdienstleistungsanbieter" bezeichnet.

804 So das erklärte Ziel des Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, BT-Drs. 19/13827, S. 48. Siehe hierzu auch *Brian/Frey/Krais*, CCZ 2019, 245 (246f.) zum Regierungsentwurf des Gesetzes. Maßgebliche Vorschriften dieses Prinzips sind die §§ 10 ff. GwG.

805 BT-Drs. 19/13827, S. 48.

806 Hierzu sind nun sog. *Kryptoverwahrgeschäfte* als Finanzdienstleistungen nach § 1 Abs. 1a Nr. 6 KWG und virtuelle Währungen als „Kryptowerte" nach § 1 Abs. 11 Nr. 10 KWG erfasst, sodass sie nach § 2 Abs. 1 Nr. 2 GwG Verpflichtete des Geldwäschepräventionsrechts sind und damit unter anderem die Kundensorgfaltspflichten nach §§ 10 ff. GwG erbringen müssen. Vgl. insoweit BT-Drs. 19/13827 S. 48. Siehe hierzu auch *Brian/Frey/Krais*, CCZ 2019, 245 (246f.) zum Regierungsentwurf des Gesetzes.

807 BT-Drs. 19/13827, S. 48.

währungen bei Verpflichteten abzufragen.[808] Insoweit ist für die Strafverfolgungsbehörden möglich, an der Schnittstelle von virtueller zu analoger Welt, *public keys* einer *Entität* zuzuordnen, soweit der Dienstleister in der EU ansässig ist.[809]

Ob allerdings ein konkreter Personenbezug hergestellt werden kann, hängt maßgeblich auch vom Transaktionsverhalten des Einzelnen ab. So empfiehlt etwa bereits *Satoshi Nakamoto* im grundlegenden Bitcoin White-Paper, für jede neue Transaktion eine neue *Bitcoin-Adresse* zu verwenden, um ausreichende Privatsphäre zu gewährleisten.[810] Darüber hinaus gibt es bestimmte Services im Kryptowährungskontext, die Transaktions- und Zahlungsströme zum Schutz der Privatsphäre verschleiern.[811] Insoweit ist es für den Einzelnen möglich, die Herstellung eines Personenbezugs aktiv zu verhindern.[812]

Dass der Einzelne Maßnahmen ergreifen kann, um die Herstellung eines Personenbezugs zu verhindern oder erschweren, kann allerdings nicht herangezogen werden, um die Blockchain-Daten vom Schutzbereich des RiS auszuschließen. Denn, wenn der Sinn und Zweck des RiS unter anderem darin liegt, dass der Einzelne frei bestimmte Entscheidungen treffen können soll und danach handeln können soll, wäre es widersinnig diesen Schutz mit dem Hinweis darauf zu verwehren, dass der Einzelne sich durch ein bestimmtes Verhalten selbst vor der Herstellung eines Personenbezugs schützen kann. Der Schutz des RiS, der die Freiheit des Verhaltens gewährleisten soll, kann insoweit nicht davon abhängen, wie sich der Einzelne verhält.

Hinzukommt weiterhin, dass es nach der Begründung des BVerfG zum RiS auf Grund moderner Informationstechnologie kein „belangloses Datum“[813] gibt, da auch Daten mit jeweils für sich genommen geringem

808 Siehe hierzu auch Herzog-GWG/*Barreto da Rosa,* § 30 Rn. 17ff; vgl. BeckOK-GWG/*Ziegner,* § 30 Rn. 14f.

809 Ähnlich insoweit auch *Finck*, Blockchain and the GDPR, S. 27.

810 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 6f.

811 *Boehm/Pesch*, MMR 2014, 75 (76); *Safferling/Rückert*, MMR 2015, 788 (791); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (755). Siehe hierzu etwa ein aktuell sehr beliebtes Tool “CoinJoin”, durch das mehrere verschiedene Transaktionen vermischt und so die jeweiligen Absender und Empfänger unkenntlich gemacht werden, vgl. https://en.bitcoin.it/wiki/CoinJoin (letzter Abruf: 20. Dezember 2021).

812 Diese Tools schließen allerdings nicht vollständig aus, dass ein Personenbezug hergestellt werden kann, sondern erschweren dies nur. Vgl. insoweit bereits oben unter Kap. 3, A.I.4.

813 BVerfGE 65, 1 (45).

Informationsgehalt je nach Verarbeitungs- und Verknüpfungsmöglichkeiten grundrechtserhebliche Auswirkungen auf den Einzelnen haben können.[814] Insoweit ist auch die Besonderheit der Blockchain-Technologie dahingehend zu berücksichtigen, dass die dort enthaltenen Transaktions-Daten für sich genommen zwar zunächst „unsensibel" sind, da sie selbst zunächst keinen Rückschluss auf die dahinterstehende *Entität* zulassen. Anders als bei anderen Datenerhebungen im Internet, liegen sie jedoch bereits einheitlich in der Blockchain selbst vor und sind insoweit einfach und umfassend verfügbar. Dementsprechend sind keine aufwändigen Verknüpfungsmöglichkeiten verschiedener Datensätze erforderlich, um etwa ein umfassendes Persönlichkeitsprofil bzw. Profil von *public keys* zu erstellen.[815] Ein derartiges Persönlichkeitsprofil dürfte selbst schon als „sensibles Datum" einzustufen sein. Geschützt sind diese Daten insoweit dadurch, dass sie nicht unmittelbar einer Person zugeordnet werden können. Die dargestellten Auswertungsmethoden verfolgen aber gerade das Ziel, einen derartigen Personenbezug herzustellen.

Insoweit ist auch das Verhältnis zwischen Aufwand zum Herstellen eines Personenbezugs und den daraus resultierenden Erkenntnissen zu berücksichtigen. Zwar ist dieser Aufwand möglicherweise höher als bei anderen „bestimmbaren" Daten, die daraus resultierenden Erkenntnisse können aber ebenso weit über einzelne Daten hinausgehen.[816] Insoweit gehen die Erkenntnisse, die durch das Herstellen eines unmittelbaren Personenbezugs gezogen werden können, etwa weit über die Erkenntnisse hinaus, die dadurch erlangt werden, dass eine dynamische IP-Adresse einer Person zugeordnet werden kann. Wenn etwa eine derartige IP-Adresse von einem Server als Logdaten erhoben werden, ist hieraus nur erkennbar, ob, wann und – unter Umständen – wie häufig ein Betroffener eine bestimmte Internetseite aufgerufen hat. Wenn dagegen die Identität eines *public keys* ermittelt werden kann, können jegliche mit diesem *public key* (und etwaiger zugehöriger anderer *public keys*)[817] jemals getätigten Transaktionen ermittelt, analysiert und dieser Person zugeordnet werden.[818]

Insoweit muss es für die „Bestimmbarkeit" im Sinne des RiS ausreichen, dass bei Blockchain-Daten unter Umständen die Möglichkeit besteht, für

814 BVerfGE 120, 274 (312).
815 Ähnlich auch *Hofert*, ZD 2017, 161 (163).
816 Ähnlich auch *Hofert*, ZD 2017, 161 (163).
817 Siehe zum Entitätsclustering, das bereits aus den unmittelbaren Blockchain-Daten möglich ist, oben unter Kap. 3 A.I.
818 Ähnlich auch *Hofert*, ZD 2017, 161 (163).

einzelne (oder auch mehrere) Transaktionen und Bitcoin-Adressen einen unmittelbaren Personenbezug herzustellen. Insbesondere, da einerseits die rechtliche Möglichkeit zur Abfrage bei Kryptowährungsdienstleistungsanbietern für Strafverfolgungsbehörden besteht und andererseits das Ziel der Erhebung und Auswertung gerade darin liegt, einen unmittelbaren Personenbezug herzustellen. Insoweit dürfte ein relativ weiter Spielraum für die Verhältnismäßigkeit zwischen objektivem Aufwand zur Herstellung eines unmittelbaren Personenbezugs und dem mit der Datenverarbeitung bezweckten Ziel bestehen.

Die unmittelbaren Blockchain-Daten sind damit personenbezogene Daten im Sinne des RiS in Form von „bestimmbaren" Daten.[819]

(2) Daten über Netzwerkverbindungen und Netzwerkverhalten

Gegenstand der in Kap. 3, B. dargestellten Auswertungsmöglichkeiten sind Daten über das Netzwerkverhalten der beteiligten Rechner und Nutzer. Ziel und Gegenstand der Auswertungen sind in der Regel die (dynamischen) IP-Adressen der beteiligten Rechner und Nutzer, um diese einer oder mehreren Bitcoin-Adressen zuordnen zu können.[820] Auch die Informationen, ob und wie eine Person an einem Blockchain-Netzwerk teilnimmt, ist vom Schutzbereich des RiS erfasst, da insoweit eine Information vorliegt, die etwas über die Bezugsperson aussagen kann.[821] Da das Ziel dieser Auswertungsmethoden gerade in Erhebung von (dynamischen) IP-Adressen liegt und (dynamische) IP-Adressen personenbezogene Daten in der Form von „bestimmbaren" personenbezogenen Daten sind[822], sind die ausgewerteten Netzwerkdaten ebenfalls personenbezogene Daten im Sinne des RiS.

(3) Anderweitig verfügbare Daten

Auch für die in Kap. 3, C. dargestellten Auswertungsmöglichkeiten kommt es darauf an, inwieweit die so erhobenen und ausgewerteten Daten einen

819 So im Ergebnis auch *Hofert*, ZD 2017, 161 (163); *Rückert*, ZStW 129 (2017), 302 (315); *Finck*, Blockchain and the GDPR, S. 26ff.

820 Siehe hierzu bereits ausführlich oben unter Kap. 3, B.

821 Vgl. BVerfGE 128, 1 (44). Ähnlich insoweit bereits oben unter Kap. 4, B.III.1.c)(1).

822 Siehe hierzu ausführlich oben unter Kap. 4, B.III.1.b)(2); EuGH NJW 2016, 3579 (3581).

Personenzug aufweisen. Eine sachliche Information über den Einzelnen dürfte nach der bereits erwähnten Rechtsprechung des BVerfG[823] dahingehend vorliegen, dass auch die Information, dass ein Einzelner eine Kryptowährung nutzt, eine Angabe über sachliche Verhältnisse i.S.d. RiS darstellt.

Soweit etwa mittels eines Internet-Crawlers[824] das Internet nach veröffentlichten *public keys* durchsucht wird, werden hiervon mindestens auch personenbezogenen Daten erhoben, da etwa einen Personenbezug hergestellt werden kann, wenn *public keys* in Signaturen in Diskussionsforen angegeben werden. Denn entweder lassen bereits die in den Diskussionsforen verwendeten Pseudonyme Rückschlüsse auf die jeweilige Person zu oder der Anbieter von Diskussionsforen erhebt im Rahmen der Anmeldung bei Diskussionsforen personenbezogene Daten über den Nutzer, die in Form eines Auskunftsverlangens nach §§ 161, 163 StPO[825] abgefragt werden können.

Ähnlich muss dies auch für die Auswertung von Dritt-Anbieter-Cookies[826] und die Standortdaten-Ermittlung bei IoT-Anwendungen[827] gelten, soweit diese Rückschlüsse auf (natürliche) Personen zulassen. Da bisher die Möglichkeiten und Ergebnisse dieser Auswertungsmethoden bisher noch wenig geklärt sind, kann hierzu keine allgemeingültige Aussage getroffen werden.

d) (Umstrittene) Erfassung öffentlich verfügbarer Daten

Fraglich ist, ob es bereits Auswirkungen auf den Schutzbereich des RiS haben kann, dass insbesondere die Blockchain-Daten öffentlich verfügbar sind. Denn in der Literatur wird teilweise vertreten, dass öffentlich verfügbare Daten grundsätzlich nicht vom Schutzbereich des RiS erfasst sind.[828]

823 BVerfGE 128, 1(44).
824 Siehe hierzu unter Kap. 3, C.I.
825 Bzw. i.V.m. § 14 Abs. 2 TMG
826 Siehe hierzu unter Kap. 3, C.II.
827 Siehe hierzu unter Kap. 3, C.III. Siehe zum Personenbezug von Geodaten ausführlich *Krügel*, ZD 2017, 455 (456ff.).k
828 So insbesondere *Böckenförde*, Die Ermittlung im Netz, S. 185ff. Ähnlich auch *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 78.

(1) Begriffsbestimmung öffentlich verfügbarer Daten

Der Begriff der öffentlich verfügbaren oder öffentlich zugänglichen Daten umfasst solche Informationen, die ohne Überwindung von Zugangsbeschränkungen von einem unbestimmten Adressatenkreis zur Kenntnis genommen werden können.[829]

(2) Erfassung öffentlich verfügbarer Daten?

Insbesondere *Böckenförde* nimmt an, dass im Rahmen des RiS zwischen einer geschützten „Privatsphäre" und einer nicht geschützten „Öffentlichkeitssphäre" zu differenzieren ist.[830]

Seine Ansicht begründet *Böckenförde* insbesondere mit der Herleitung aus dem allgemeinen Persönlichkeitsrecht. Denn das RiS sei unter ausdrücklichem Verweis auf das allgemeine Persönlichkeitsrecht aus diesem hergeleitet worden und könne in seinem Schutzgehalt nicht über dessen Schutzbereich hinausgehen.[831] Insoweit gelte nach *Böckenförde* auch der im Rahmen des allgemeinen Persönlichkeitsrechts abgestufte und bereichsspezifische Persönlichkeitsschutz.[832] Auch das zur Informationsgewinnung in öffentlich zugänglichen Netzwerken grundlegende Urteil des BVerfG zum Online-Durchsuchungsgesetz NRW[833] legt *Böckenförde* dahingehend aus, dass auch das BVerfG zwischen einer geschützten „Privatsphäre" und einer nicht geschützten „Öffentlichkeitsphäre" differenziere.[834] In diesem Zusammenhang geht *Böckenförde* jedoch nicht näher darauf ein, dass das BVerfG die Frage des Schutzes von öffentlich verfügbaren Daten nicht im Rahmen des Schutzbereichs des RiS diskutiert, sondern lediglich darauf abstellt, dass kein „Eingriff" bei der Kenntnisnahme öffentlich zugänglicher Daten in das RiS vorliege.[835] Zwar zitiert das BVerfG in seinem Urteil

829 Vgl. BVerfGE 120, 274 (345); BVerfGE 120, 351 (361); *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 118 m.w.N.
830 *Böckenförde*, Die Ermittlung im Netz, S. 185ff.; *Böckenförde*, JZ 2008, 925 (935).
831 *Böckenförde*, Die Ermittlung im Netz, S. 178f.
832 *Böckenförde*, Die Ermittlung im Netz, S. 181.
833 BVerfGE 120, 274ff.
834 *Böckenförde*, JZ 2008, 925 (935). In diesem Zusammenhang nimmt *Böckenförde* die Differenzierung allerdings bereits auf Eingriffs- und nicht mehr auf Schutzbereichsebene vor. Vgl. hierzu auch *Bauer*, Soziale Netzwerke, S. 110f.
835 BVerfGE 120, 274 (344f.).

Böckenförde ausdrücklich, gibt in diesem Zusammenhang aber an, dass „kein Eingriff"[836] vorliege, wenn „eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte"[837] erhebe, die sich an jedermann richten.

Der von *Böckenförde* vertretenen Auffassung steht insbesondere der Sinn und Zweck des RiS und seine Herleitung entgegen.[838] Denn das BVerfG begründet die Notwendigkeit des Schutzes des RiS insbesondere mit den persönlichkeitsrechtlichen Gefährdungen, die durch die Möglichkeiten informationstechnischer Datenverarbeitungen bestehen.[839] Derartige Gefährdungen ergeben sich nach dem BVerfGE bereits aus der Möglichkeit, dass Informationen mit für sich genommen geringem Informationsgehalt verknüpft werden könnten und so ein über die einzelne Information hinausgehender Informationsgehalt erlangt werden könne.[840] Deshalb nimmt das BVerfG an, dass das RiS den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit „flankiert und erweitert"[841]. Der Schutz des RiS beginne bereits auf der Ebene der Persönlichkeitsgefährdung insoweit, dass er bereits im „Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter"[842] anwendbar sei. Sinn und Zweck des Schutzes des RiS ist es insoweit, die freie Entfaltung der Persönlichkeit des Einzelnen zu schützen und zu erhalten.[843] Diese kann auch bereits dann betroffen sein, wenn der Einzelne nicht überblicken kann, welche Informationen über ihn erhoben und verarbeitet werden.[844] Vor diesem Hintergrund kann zumindest auf der Ebene des Schutzbereichs nicht zwischen öffentlich verfügbaren Daten und nicht öffentlich verfügbaren Daten differenziert werden.[845] So nimmt das BVerfG nun mittlerweile ausdrücklich an, dass die öffentliche Verfügbarkeit nichts daran ändert, dass diese Daten ebenfalls vom Schutzbereich des RiS erfasst sind.[846]

Insoweit erstreckt sich der Schutzbereich des RiS auch auf öffentlich zugängliche Daten.

836 BVerfGE 120, 274 (344).
837 BVerfGE 120, 274 (344f.).
838 Ähnlich auch *Bauer*, Soziale Netzwerke, S. 107f.
839 Grundlegend BVerfGE 65, 1 (42f.); BVerfGE 120, 274 (312) m.w.N.
840 BVerfGE 120, 274 (312).
841 BVerfGE 120, 274 (312).
842 BVerfGE 120, 274 (312).
843 BVerfGE 65, 1 (42f.).
844 BVerfGE 118, 168 (184).
845 So auch *Bauer*, Soziale Netzwerke, S. 107. Ähnlich auch *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 27.
846 BVerfGE 142, 234 ((251); BVerfGE 150, 244 (265).

Soweit die ausgewerteten Blockchain-Daten[847] oder Daten des Netzwerkverhaltens und der Netzwerkverbindungen[848], sowie die ausgewerteten anderweitig verfügbaren Daten[849] öffentlich verfügbare Daten sind, hat dies insoweit keine Auswirkungen darauf, dass sie vom Schutzbereich des RiS erfasst sind.

e) Zwischenergebnis

Der Schutzbereich des RiS ist für alle Daten eröffnet, die im Rahmen der in Kap. 3 dargestellten Auswertungsmöglichkeiten, erhoben und verarbeitet bzw. ausgewertet werden.

2. Eingriff

Fraglich ist deshalb, ob durch die Erhebung und/oder Auswertung der Daten ein Eingriff in das RiS vorliegt.

a) Grundsatz – Eingriffe in das RiS

In Literatur und Rechtsprechung wird in der Regel zwischen einem klassischen und einem „modernen" bzw. „erweiterten" Eingriffsbegriff differenziert.[850] Nach dem klassischen Eingriffsbegriff liegt ein Grundrechtseingriff vor, wenn ein staatlicher Rechtsakt den grundrechtlich geschützten Gewährleistungsbereich unmittelbar, zielgerichtet und imperativ verkürzt.[851]

Der mittlerweile vorherrschende moderne Eingriffsbegriff erweitert den Begriff des Eingriffs dahingehend, dass ein Eingriff bei jeder Verkürzung des tatbestandlich gewährleisteten grundrechtlichen Schutzbereichs vorliegt, die dem Staat zugerechnet werden kann.[852]

---

847 Siehe hierzu oben unter Kap. 3, A.
848 Siehe hierzu oben unter Kap. 3, B.
849 Siehe hierzu oben unter Kap. 3, A.
850 BVerfGE 130, 151 (184). *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 216f. m.w.N.
851 BVerfGE 105, 279 (299f.).
852 *Bauer*, Soziale Netzwerke, S. 217 m.w.N.

Insbesondere im Bereich des von Art. 2 Abs. 1 GG gewährleisteten Schutzbereichs ist umstritten, ob die Anwendung des modernen Eingriffsbegriffs nicht zu einer uferlosen Gewährleistung des Einzelnen gegen jedes staatliche Handeln führt und deshalb anderweitig begrenzt werden muss.[853]

Weitgehende Einigkeit besteht dagegen für Eingriffe in das RiS.[854] Im Bereich des RiS geht die Literatur davon aus, dass jeweils ein Eingriff bei jeder Kenntnisnahme, Erhebung, Speicherung, Abgleichung, Abfrage, Weitergabe oder Veröffentlichung von personenbezogenen Daten[855] vorliegt.[856] Ebenso nimmt das BVerfG an, dass beim Umgang mit personenbezogenen Daten jeweils einzelne, aufeinander aufbauende Eingriffe vorliegen, die nach „Erhebung, Speicherung und Verwendung"[857] von Daten zu unterscheiden sind. Als Eingriff ist insoweit jeglicher Umgang mit personenbezogenen Daten erfasst.[858] Dementsprechend liegt im Grundsatz ein Eingriff bei jeglicher Kenntnisnahme, Erhebung, Erfassung, Sammlung, Aufzeichnung, Speicherung, Sicherstellung, Verknüpfung, Abgleichung, Abfrage, Übermittlung, Weitergabe oder Veröffentlichung (nachfolgend zusammenfassend als „Datenverarbeitung" bezeichnet[859]) personenbezogener Daten[860] vor.

b) Eingriff bei öffentlich verfügbaren/allgemein zugänglichen Daten

Fraglich ist jedoch, ob auch ein Eingriff in das RiS vorliegt, wenn öffentlich verfügbare bzw. allgemein zugängliche Daten verarbeitet werden.

Um diese Frage zu beantworten, wird nachfolgend zunächst die wesentliche Verfassungsrechtsprechung betrachtet (hierzu unter (1)), anschließend auf hiervon abweichende Literaturauffassungen eingegangen (hierzu unter

853 Sachs-GG/*Murswiek/Rixen,* Art. 2 Rn. 79ff.

854 So etwa BeckOK-GG/*Lang,* Art. 2 Rn. 51, der davon ausgeht, dass eine Begrenzung des Eingriffsbegriffs im Bereich des allgemeinen Persönlichkeitsrechts nicht notwendig sei.

855 Siehe zum Begriff der personenbezogenen Daten bereits oben unter Kap. 4, B.III.1.b).

856 So insbesondere Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Abs. 1 Rn. 176; Stern-Becker-GG/*Horn,* Art. 2 Rn. 93; *Bauer,* Soziale Netzwerke, S. 110.

857 BVerfGE 150, 244 (266f.) mit Verweis auf BVerfGE 130, 151 (184); BVerfGE 100, 313 (366f.); BVerfGE 115, 320 (343f.); BVerfGE 120, 378 (400f.); BVerfGE 125, 260 (310).

858 Vgl. BVerfGE 130, 151 (184); BVerfGE 150, 244 (266).

859 Siehe hierzu die deckungsgleiche Begriffsbestimmung des Art. 4 Nr. 1 DSGVO. So auch BVerfGE 150, 244 (266).

860 Vgl. für die Aufzählung Stern-Becker-GG/*Horn,* Art. 2 Rn. 93.

(2)), um abschließend die Frage nach Eingriffen in das RiS bei öffentlich verfügbaren Daten beantworten zu können (hierzu unter (3)).

(1) Rechtsprechung des BVerfG

Zum Umgang mit öffentlich verfügbaren Daten hat sich das BVerfG grundlegend in seiner Entscheidung zum VSG NRW (hierzu unter i.) geäußert. Die dort herausgearbeiteten Grundsätze wurden auch in den darauffolgenden Entscheidungen zur Datensammlung über steuerliche Auslandsbeziehungen (hierzu unter ii.), zur automatisierten Kfz-Kennzeichenerfassung (hierzu unter iii.) und zur automatisierten Kfz-Kennzeichenerfassung II (hierzu unter iv.) aufgenommen und weiter ausgeführt.

i. BVerfGE 120, 274 ff. – VSG NRW[861]

Die Entscheidung des BVerfG zum VSG NRW betraf die Frage der Verfassungsmäßigkeit mehrerer Vorschriften des VSG NRW, die den Verfassungsschutz NRW einerseits „zum heimlichen Beobachten und sonstigen Aufklären des Internet“[862] und andererseits „zum heimlichen Zugriff auf informationstechnische Systeme“[863] ermächtigten. Neben der Entwicklung und Begründung des „Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme“[864] äußerte sich das BVerfG in diesem Zusammenhang auch zur Verfassungsmäßigkeit des heimlichen Aufklärens des Internets.[865] Hierzu nahm das BVerfG an, dass beim heimlichen Aufklären des Internets ein Eingriff in das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG vorliege, wenn eine staatliche Stelle Telekommunikation zwar auf dem technisch dafür vorgesehenen Weg wahrnehme, aber hierzu nicht durch mindestens einen der Kommunikationsbeteiligten autorisiert sei.[866] Daran

861 Siehe hierzu ebenfalls ausführlich oben unter Kap. 4, B.I.1.c)(1).
862 BVerfGE 120, 274 (276).
863 BVerfGE 120, 274 (276).
864 BVerfGE 120, 274 (Ls. 1, 302). Siehe zur ausführlichen Begründung der Notwendigkeit des Schutzes durch das IT-Grundrecht BVerfGE 120, 274 (303ff.).
865 Hierzu ausführlich BVerfGE 120, 274 (340ff.).
866 BVerfGE 120, 274 (341). Siehe hierzu bereits ausführlich oben unter Kap. 4, B.I.1.c)(1). Konkret betraf dies den Fall, dass die Verfassungsschutzbehörde „zugangsgesicherte Kommunikationsinhalte überwacht[e], indem sie Zugangsschlüssel nutzt[e],

anschließend gab das BVerfG allerdings an, dass die Verfassungsschutzbehörde allerdings „weiterhin Maßnahmen der Internetaufklärung treffen [dürfe], soweit diese nicht als Grundrechtseingriffe anzusehen [seien]“[867]. Ein Grundrechtseingriff in das RiS liege in der Regel bei Maßnahmen der Internetaufklärung nicht vor.[868] Dem Staat sei die Kenntnisnahme öffentlich zugänglicher Informationen grundsätzlich nicht verwehrt, auch wenn im Einzelfall personenbezogene Daten erhoben werden könnten.[869] Daher liege kein Eingriff in das RiS vor, „wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erheb[e], die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.“[870] Als Beispiele hierfür nennt das BVerfG den Aufruf von allgemein zugänglichen Internetseiten oder das Beobachten eines offenen Chats.[871]

Die Grenze zum Eingriff in das RiS definiert das BVerfG daran anschließend wie folgt:

> *„Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann allerdings gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert, und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.“*[872]

Hieraus lassen sich insoweit zwei Voraussetzungen für einen Eingriff in das RiS bei öffentlich verfügbaren Daten ableiten:

- Die gezielte Datenverarbeitung öffentlich verfügbarer Daten,
- Eine sich daraus ergebende besondere Gefahrenlage für die Persönlichkeit des Betroffenen

Nach dem BVerfG stellt daher die „reine Internetaufklärung in aller Regel keinen Grundrechtseingriff“[873] dar.

---

die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat[te]“ BVerfGE 120, 274 (341).

867 BVerfGE 120, 274 (340, 344).

868 BVerfGE 120, 274 (344).

869 BVerfGE 120, 274 (344).

870 BVerfGE 120, 274 (344f.).

871 BVerfGE 120, 274 (345).

872 BVerfGE 120, 274 (345). Siehe zur Frage, ob diese Grundsätze auch auf die Ermittlungen von Strafverfolgungsbehörden übertragen werden können, ausführlich *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 83ff.

873 BVerfGE 120, 274 (345).

ii. BVerfGE 120, 351 ff. – Datensammlung über steuerliche Auslandsbeziehungen

Entsprechend äußerte sich das BVerfG in Bezug auf die Datenverarbeitung bei im Ausland öffentlich verfügbaren Daten:

> *„Werden Daten, die aus im Ausland öffentlich zugänglichen Quellen gewonnen werden, in die Sammlung aufgenommen, liegt zwar noch nicht in der Erhebung dieser Daten ein Grundrechtseingriff, wohl aber kann er in ihrer Sammlung und systematischen Erfassung bestehen.*
> *Es ist dem Staat nicht verwehrt, von jedermann zugänglichen Informationsquellen unter denselben Bedingungen wie jeder Dritte Gebrauch zu machen*“[874].

Insoweit ist hiernach die Grenze der Datenverarbeitung öffentlich verfügbarer Daten wiederum dann überschritten, wenn die Verarbeitung über die bloße Kenntnisnahme/Erhebung der Daten hinausgeht. Das Urteil des BVerfG geht insoweit nur mit seiner Begründung, dass staatliche Stellen öffentlich zugängliche Quellen genauso benutzen können müssen, wie jeder Dritte, über das Urteil zum VSG NRW[875] hinaus.

iii. BVerfGE 120, 378 ff. – Automatisierte Kfz-Kennzeichenerfassung

Ähnlich nimmt das BVerfG für die automatisierte Kfz-Kennzeichenerfassung an, dass die Grenze zum Eingriff in das RiS überschritten sei, wenn ein erfasstes Kennzeichen gespeichert wird und so Grundlage weiterer Maßnahmen werden kann.[876] Hierzu führt das BVerfG im Einzelnen aus:

> *„Auch entfällt der grundrechtliche Schutz nicht schon deshalb, weil die betroffene Information öffentlich zugänglich ist […]. Auch wenn der Einzelne*

874 BVerfGE 120, 351 (361).

875 Siehe hierzu bereits Kap. 4, B.III.2b)(1)i.

876 BVerfGE 120, 378 (399). Vgl. insoweit auch *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 233, der allerdings einen Widerspruch zwischen den Entscheidungen der automatisierten Kfz-Kennzeichenerfassung und dem VSG NRW annimmt. Der von *Eisenmenger* angenommene Widerspruch lässt sich allerdings dahingehend auflösen, dass sich das BVerfG in der Entscheidung zur automatisierten Kfz-Kennzeichenerfassung zunächst zum Schutzbereich des RiS dahingehend äußert, dass die öffentliche Verfügbarkeit von Informationen hierdurch nicht bereits ausgeschlossen sei und erst im Anschluss auf die Grenze zum Eingriff eingeht.

> *sich in die Öffentlichkeit begibt, schützt das Recht der informationellen Selbstbestimmung dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwertung erfasst werden"*[877].
>
> *„Andererseits begründen Datenerfassungen keinen Gefährdungstatbestand, soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden […].*
>
> *[…]*
>
> *Demgegenüber kommt es zu einem Eingriff in das Grundrecht, wenn ein erfasstes Kennzeichen im Speicher festgehalten wird und gegebenenfalls Grundlage weiterer Maßnahmen werden kann."*[878]

Maßgeblich ist insoweit wiederum nicht die bloße Kenntnisnahme öffentlich verfügbarer Daten, sondern die möglichen, sich daran anschließenden weiteren Maßnahmen der Datenverarbeitung – hier konkret die Speicherung, da ab diesem Zeitpunkt das erfasste Kennzeichen zur Auswertung durch staatliche Stellen zur Verfügung steht.[879]

iv. BVerfGE 150, 244 ff. – Automatisierte Kfz-Kennzeichenerfassung II

Fraglich ist, ob sich die Rechtsprechungsänderung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung[880] auch auf die Frage des Eingriffs bei der Verarbeitung öffentlich verfügbarer Daten auswirkt.

In seiner ersten Entscheidung zur automatisierten Kfz-Kennzeichenerfassung[881] nahm das BVerfG noch an, dass ein Eingriff in das RiS dann nicht vorliege, wenn die erfassten Kfz-Kennzeichen unverzüglich mit dem Fahndungsbestand abgeglichen würden, negativ ausfielen und technisch sichergestellt sei, dass die Daten anonym blieben und sofort spurenlos gelöscht würden.[882] Die maßgebliche Begründung des BVerfG lag in einem

877 BVerfGE 120, 378 (399). Diese Passage betrifft insoweit zunächst den Schutzbereich des RiS und noch nicht den Eingriff in das RiS, vgl. bereits Fn. 856.
878 BVerfGE 120, 378 (399).
879 BVerfGE 120, 378 (399f.).
880 BVerfGE 150, 244ff.
881 BVerfGE 120, 378ff.
882 BVerfGE 120, 378 (399).

Verweis auf die Rechtsprechung des BVerfG zum G-10-Gesetz, wonach kein Eingriff vorliege, „soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit einen Personenbezug herzustellen, ausgesondert werden“[883], da derartige Datenerfassungen „keinen Gefährdungstatbestand“[884] begründen würden.

In seiner zweiten Entscheidung zur automatisierten Kfz-Kennzeichenerfassung[885] weicht das BVerfG dagegen von dieser Rechtsprechung ab und nimmt auch einen Eingriff in das RiS bei einem „Nichttreffer“[886] an. Dies begründet das BVerfG wie folgt:

Ein Eingriff in das RiS liege grundsätzlich bei der Erhebung personenbezogener Daten vor, allerdings dann nicht, wenn die personenbezogenen Daten lediglich technikbedingt und ungezielt miterfasst würden und diese „unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert“[887] würden. Eine Rückausnahme hiervon gelte allerdings, wenn „die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung“ sei.[888] 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 behördlicher Interesse an den betroffenen Daten bereits derart verdichtet habe, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen“[889] sei.

Das BVerfG setzt insoweit zunächst seine Rechtsprechung dahingehend fort, dass kein Eingriff in das RiS vorliege, wenn Daten lediglich technikbedingt miterfasst würden und anonym und spurenlos ohne weiteren Erkenntnisgewinn wieder ausgesondert würden.

883 BVerfGE 120, 378 (399) mit Verweis auf BVerfGE 100, 313 (366); BVerfGE 107, 209 (328); BVerfGE 115 320 (343).
884 BVerfGE 120, 378 (399).
885 BVerfGE 150, 244ff.
886 BVerfGE 150, 244 (266). Ein Nichttreffer liegt vor, wenn das Kfz-Kennzeichen erfasst wird, mit dem Fahndungsbestand abgeglichen wird, hierin nicht enthalten ist und deshalb ausgesondert wird.
887 BVerfGE 150, 244 (266) mit Verweis auf BVerfGE 100, 313 (366) und BVerfGE 115, 320 (343).
888 BVerfGE 150, 244 (266).
889 BVerfGE 150, 244 (266) mit Verweis auf BVerfGE 115, 320 (343) und BVerfGE 120, 378 (398).

Hiervon formuliert das BVerfG nun allerdings die Rückausnahme, dass dies dann nicht gelte, wenn zwar weiterhin Daten unmittelbar nach ihrer Erfassung ausgesondert würden, aber die Erfassung des gesamten Datenbestandes gerade mit dem Ziel der Verkleinerung des Datenbestandes vorgenommen würde, wenn also die Erfassung des gesamten Datenbestandes nicht lediglich technikbedingt stattfinde, sondern gerade mit dem Ziel hiervon einen bestimmten Teilbereich auszusondern. Ob diese Rückausnahme vorliege, hänge maßgeblich davon ab, ob ein behördliches Interesse an den betroffenen Daten in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen sei.

Bei der automatisierten Kfz-Kennzeichenerfassung würden zwar ebenfalls die „Nichttreffer" unmittelbar nach deren Erfassung und dem Abgleich mit dem Fahndungsbestand ausgesondert werden. Es bestünde aber gerade ein spezifisches Interesse eben auch an den „Nichttreffern", da die moderne Informationstechnik einen Abgleich mit großen Datenmengen innerhalb kürzester Zeit ermögliche. Denn maßgebliches Ziel einer automatisierten Kfz-Kennzeichenkontrolle sei es gerade, die „Treffer" herauszufiltern.[890] Dieses Ziel könne aber nur erreicht werden, wenn auch die „Nichttreffer" erfasst würden.[891] Notwendig sei es insofern, den gesamten Datenbestand zu erheben, sodass aus diesem Grund auch ein gezieltes, spezifisches Interesse an den erhobenen „Nichttreffern" bestünde.[892] Denn, wenn gezielt „mittels Datenabgleich Personen im öffentlichen Raum daraufhin überprüft würden, ob sie oder die von ihnen mitgeführten Sachen polizeilich gesucht [würden], besteht an deren Daten auch dann ein verdichtetes behördliches Interesse, wenn diese Daten im Anschluss an die Überprüfung unmittelbar wieder gelöscht werden.[893] So kommt das BVerfG zu dem Ergebnis, dass jede automatisierte Erfassung der Kfz-Kennzeichen einen Eingriff in das RiS begründet.[894]

Da auch Kfz-Kennzeichen öffentlich sichtbar sind, stellt sich daher die Frage, ob diese Rechtsprechungsänderung auch eine veränderte Grenzziehung zwischen Eingriff und Nichteingriff in das RiS bei öffentlich verfügbaren Daten zur Folge hat. So könnte das BVerfG dahingehend zu verstehen sein, dass ein Eingriff in das RiS bei öffentlich verfügbaren Daten

890 BVerfGE 150, 244 (267f.).
891 BVerfGE 150, 244 (267f.).
892 BVerfGE 150, 244 (267f.).
893 BVerfGE 150, 244 (267).
894 BVerfGE 150, 244 (266).

nicht mehr nur bei einem „gezielten Zusammentragen“[895] solcher Daten vorliegt, sondern bereits die bloße Kenntnisnahme öffentlich verfügbarer Daten einen Eingriff in das RiS darstellt.

Für eine so veränderte Grenzziehung spricht zunächst, dass das BVerfG in seiner Entscheidung konkret ausführt, dass bereits die Erhebung und der Datenabgleich der öffentlich sichtbaren Kfz-Kennzeichen jeweils zu differenzierende Grundrechtseingriffe darstellen.

Dem steht allerdings entgegen, dass nach dieser Rechtsprechung nur dann ein Eingriff in das RiS bei öffentlich verfügbaren Kfz-Kennzeichen vorliegt, wenn an ihrer Erhebung bzw. Erfassung ein spezifisches behördliches Interesse besteht. Diese Anforderung des spezifischen behördlichen Interesses geht insoweit über die bloße Kenntnisnahme von öffentlich verfügbaren Daten hinaus. Denn, wie das BVerfG ausführlich begründet ist das Ziel und die notwendige Voraussetzung der Erfassung der Kfz-Kennzeichen gerade, dass alle Kfz-Kennzeichen erfasst werden und daher gerade auch ein Interesse an denen besteht, die nach dem Datenabgleich als „Nichttreffer“ aussortiert werden. Insoweit liegt bei der Erfassung aller Kfz-Kennzeichen ein „gezieltes Zusammentragen“ von Daten vor, das über die bloße Kenntnisnahme hinausgeht.

Dieser Unterschied schlägt sich auch sprachlich nieder. Denn das BVerfG spricht in diesem Kontext nicht von der „Kenntnisnahme“[896] oder „Erhebung“[897] – wie bei öffentlich verfügbaren Daten im Internet –, sondern von der „Erfassung“ der Kfz-Kennzeichen.

Insoweit ist die Entscheidung des BVerfG nicht dahingehend zu verstehen, dass bereits die bloße Kenntnisnahme von öffentlich verfügbaren Daten einen Eingriff in das RiS darstellt, sondern sie konkretisiert lediglich die Grenze ab wann ein einen Eingriff begründendes gezieltes Zusammentragen von öffentlich verfügbaren Daten vorliegt.[898]

---

895 Vgl. BVerfGE 120, 274 (345).

896 BVerfGE 120, 274 (344). Nachfolgend spricht das BVerfG allerdings im gleichen Zusammenhang von „Erhebung“. Auf Grund des inhaltlichen Zusammenhangs der Ausführungen ist allerdings davon auszugehen, dass das BVerfG hier „Kenntnisnahme“ und „Erhebung“ synonym verwendet. Vgl. insoweit ähnlich die Ausführungen zum datenschutzrechtlichen Begriff der Datenerhebung in BeckOK-DSR/*Schild,* Art. 4 DS-GVO Rn. 35, wonach das Erheben das „Beschaffen der personenbezogenen Daten“ darstellt und von der Speicherung abgegrenzt werden kann.

897 BVerfGE 120, 274 (344f.).

898 Zur bisher unklaren Grenzziehung des gezielten Zusammentragens *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 233f.

Die Entscheidung des BVerfG zur automatisierten Kfz-Kennzeichenkontrolle[899] lässt sich daher dahingehend auslegen, dass ein derartiges „gezieltes Zusammentragen" vorliegt, wenn öffentlich verfügbare Daten technikgestützt, automatisiert erfasst werden und ein spezifisches Interesse an den erhobenen Daten vorliegt.

Zu berücksichtigen ist jedoch auch, dass das BVerfG zu Beginn seiner Ausführungen zum Eingriff in das RiS darstellt, dass sowohl die Erfassung, als auch der Abgleich der erfassten Kfz-Kennzeichen jeweils einen eigenständigen Grundrechtseingriff begründet.[900] Anschließend geht das BVerfG allerdings darauf ein, dass beide Schritte der Kfz-Kennzeichenkontrolle (Erfassung und Abgleich) unmittelbar aufeinander bezogen seien, da die „Kennzeichenerfassung [...] unmittelbar dem Abgleich mit den [...] Fahndungsbeständen [diene]"[901]. Im Folgenden stellt das BVerfG dann nur noch einheitlich auf beide Maßnahmen als Grundrechtseingriffe ab und äußert sich insoweit nicht spezifisch, ob bereits jede der Datenverarbeitungsmaßnahmen einen eigenständigen Grundrechtseingriff begründeten.[902]

Dementsprechend ließe sich vertreten, dass bereits die Erfassung öffentlich verfügbarer Daten nur dann einen Eingriff in das RiS begründet, wenn sie zu einem über die Erfassung hinausgehenden Zweck – etwa einem weitergehenden Abgleich – erfasst würden. Diese Auslegung wird auch dadurch unterstützt, dass es für den Eingriff auch darauf ankommt, ob ein spezifisches Interesse an den erhobenen Daten besteht.

Zusammenfassend ermöglicht die Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung daher folgende Auslegung für den Eingriff bei öffentlich verfügbaren Daten:

Die bloße nicht automatisierte Kenntnisnahme öffentlich zugänglicher Daten stellt weiterhin keinen Eingriff in das RiS dar.

Die Grenze zum Eingriff ist allerdings dann in Form eines „gezielten Zusammentragens" überschritten, wenn öffentlich verfügbare Daten technikgestützt, automatisiert erfasst werden, ein spezifisches Interesse an den

899 BVerfGE 150, 244ff.

900 BVerfGE 150, 244 (266), wonach „in der Erfassung und dem Abgleich [...] Eingriff*e* in sein Grundrecht" vorliegen.

901 BVerfGE 150, 244 (267).

902 Siehe insoweit folgende Formulierung, BVerfGE 150, 244 (267): „Die Erfassung der Kennzeichen und der sich anschließende Abgleich stellen sich in diesem Zusammenhang als Grundrechtseingriffe gegenüber allen Personen dar, deren Kennzeichen in die Kontrolle einbezogen wurden." Hieraus geht insoweit nicht eindeutig hervor, ob jede Datenverarbeitung für sich genommen bereits einen Eingriff in das RiS begründen.

erfassten Daten besteht, und die Erhebung zu einem weitergehenden Zweck erfolgt.

v. Zwischenergebnis

Die grundlegende Entscheidung zur rechtlichen Bewertung von Eingriffen in das RiS bei öffentlich verfügbaren Daten war das Urteil des BVerfG zum VSG NRW[903], in dem das BVerfG erstmals Maßstäbe zur Kenntnisnahme öffentlich verfügbarer Daten im Internet vorgab. Maßgebliches Abgrenzungskriterium für einen Eingriff in das RiS ist hiernach das gezielte Zusammentragen, Speichern und Verknüpfen von öffentlich verfügbaren Informationen, wenn sich daraus eine besondere Gefährdungslage für die Persönlichkeit des Betroffenen ergibt.[904] Diese Vorgaben setzte das BVerfG in seinen folgenden, vergleichbaren Entscheidungen fort und führte darüber hinaus zur Begründung aus, dass es dem Staat nicht verwehrt sein könne, öffentlich verfügbare Informationen, wie jeder andere zur Kenntnis zu nehmen.[905] Darüber hinaus nahm das BVerfG in seinen Entscheidungen zu automatisierten Kfz-Kennzeichenerfassungen[906] an, dass jede Datenverarbeitungsmaßnahme einen eigenständigen Grundrechtseingriff darstelle.[907]

Nach dieser Rechtsprechung muss für die Abgrenzung, ob ein Eingriff vorliegt, maßgeblich darauf abgestellt werden, ob sich aus der jeweiligen Datenverarbeitung eine Persönlichkeitsgefährdung für den Betroffen ergeben kann.[908] Das ist dann nicht der Fall, wenn öffentlich verfügbare Daten lediglich zur Kenntnis genommen werden, da der Betroffene die Informationen (in der Regel) bewusst veröffentlicht hat und deshalb weder die Gefahr besteht, dass er nicht überblicken kann, welche Informationen über ihn erhoben wurden noch seine berechtigten Geheimhaltungsinteressen betroffen sind. Diese Grenze ist aber in der Regel bei jeder darüber hinausgehenden Datenverarbeitungsmaßnahme überschritten.

903 BVerfGE 120, 274ff.
904 BVerfGE 120, 274 (345).
905 BVerfGE 120, 351 (361).
906 BVerfGE 120, 378ff.; BVerfGE 150, 244ff.
907 BVerfGE 150, 244 (265f.).
908 Vgl. insoweit BVerfGE 120, 378 (399), wonach ein Eingriff bei der Erhebung ausscheide, wenn auf Grund der unmittelbar anschließenden Löschung eine Persönlichkeitsgefährdung des Einzelnen ausgeschlossen werden kann.

(2) Eingriffseinschränkungen und -erweiterungen in der Literatur

Abweichend von der dargestellten Rechtsprechung werden in der Literatur verschiedene Ansätze diskutiert, um entweder einen Eingriff bei öffentlich verfügbaren Daten nur unter einschränkenden Voraussetzungen anzunehmen oder auch weitergehend bereits bei der bloßen Kenntnisnahme von in sozialen Medien öffentlich verfügbaren Daten anzunehmen.

i. Bagatellvorbehalt

So wurde insbesondere diskutiert, ob auf Grund der Weite des modernen Eingriffsbegriffs nicht eine Einschränkung dahingehend angenommen werden muss, dass nur solche Maßnahmen einen Eingriff in das RiS darstellen, die eine gewisse Relevanzschwelle überschreiten.[909] So sollen etwa Eingriffe von bloßen „Belästigungen"[910] unterhalb der Eingriffsschwelle abgegrenzt werden. Belästigungen sind dabei Verkürzungen des grundrechtlich geschützten Gewährleistungsbereichs, die von jedem „Mitglied eines Gemeinwesens toleriert werden [müssten]"[911]. Beispiele für derartige Bagatellfälle sind etwa „das Notieren von Namen oder Kfz-Kennzeichen auf einem Merkzettel, der Blick ins Telefonbuch oder das Inspizieren einer Gaststätte während eines Streifengangs"[912].

Der Annahme eines solchen Bagatellvorbehaltes steht jedoch entgegen, dass es hierbei an Trennschärfe fehlen würde und daher die Gefahr bestünde, dass ein Eingriff vorschnell unter einem Hinweis auf die Geringfügigkeit der Beeinträchtigung abgelehnt werden könnte und so die notwendige verfassungsrechtliche Rechtfertigung umgangen würde.[913] Hinzukommt, dass nach der grundlegenden Entscheidung des BVerfG (dem Volkszäh-

909 Siehe hierzu ausführlich *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 33, 35, der sich allerdings allgemein mit der Eingriffsschwelle im Bereich des RiS auseinandersetzt und sich nicht konkret auf öffentlich verfügbare Daten bezieht. So aber *Bauer*, Soziale Netzwerke, S. 107, 113ff. m.w.N., der sich mit der Anwendung dieser Relevanzschwelle bei der sog. Online-Streife für öffentlich verfügbare Daten auseinandersetzt, aber zu dem Ergebnis kommt, dass eine solche für den Eingriff in das RiS nicht geboten ist.

910 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 33.

911 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 33.

912 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 35.

913 Siehe hierzu insbesondere *Bauer*, Soziale Netzwerke, S. 113f.

lungsurteil)[914] Daten unabhängig von ihrer Qualität schützenswert sind,[915] sodass es widersprüchlich wäre, „der Erhebung bestimmter ‚unsensibler' Daten [...] pauschal die Eingriffsqualität"[916] abzusprechen.[917] Daher ist der Bagatellvorbehalt abzulehnen.

ii. Grundrechtsverzicht

Möglich erscheint bei öffentlich verfügbaren Daten auf den ersten Blick jedoch ein Grundrechtsverzicht des Betroffenen.[918]

Zu berücksichtigen ist jedoch, dass selbst wenn man in der Nutzung von Blockchain-Technologien die mindestens erforderliche konkludente Grundrechtsverzichtserklärung sehen würde[919], für einen wirksamen Grundrechtsverzicht erforderlich wäre, dass der Betroffene jederzeit seine Verzichtserklärung widerrufen können muss.[920] Das ist aber auf Grund der technischen Funktionsweise von Blockchain-Technologien[921] nicht möglich, da eine nachträgliche Veränderung der Inhalte in Blockchains faktisch nicht möglich ist.[922]

Mindestens fraglich dürfte darüber hinaus auch die erforderliche Freiwilligkeit eines Grundrechtsverzichts[923] sein. Denn wenn bereits bei der Nutzung sozialer Netzwerke, bei der zumindest noch die Möglichkeit besteht, die Privatsphäreeinstellungen manuell zu verändern[924], ein freiwilliger Grundrechtsverzicht auf Grund eines möglichen faktischen Zwangs

914 BVerfGE 65, 1ff.
915 BVerfGE 65, 1 (45).
916 *Bauer*, Soziale Netzwerke, S. 113f mit Verweis auf Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Abs. 1 Rn. 174.
917 So auch HGR Bd. IV/*Rudolf,* § 90 Rn. 65.
918 Siehe hierzu insbesondere ausführlich *Bauer*, Soziale Netzwerke, S. 114ff m.w.N. Zur Möglichkeit eines Grundrechtsverzichts auch *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 36ff.
919 Siehe zur Nutzung von sozialen Netzwerken als konkludente Verzichtserklärung *Bauer*, Soziale Netzwerke, S. 115f.
920 *Bauer*, Soziale Netzwerke, S. 116 m.w.N.
921 Siehe hierzu ausführlich oben unter Kap. 2.
922 Siehe hierzu oben ausführlich Kap. 2, A.III.2. Siehe zur Frage einer datenschutzrechtlichen Einwilligung bei der Nutzung von Blockchain-Technologien *Hofert*, ZD 2017, 161 (164ff.).
923 *Bauer*, Soziale Netzwerke, S. 117.
924 Siehe hierzu ausführlich *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 97ff.

fraglich erscheint[925], dürfte diese Freiwilligkeit bei Blockchain-Technologien insoweit mindestens genauso fraglich sein. Denn die Technologie setzt die Veröffentlichung der jeweiligen Daten notwendigerweise voraus, sodass allenfalls Freiwilligkeit hinsichtlich der Nutzung oder Nichtnutzung bestehen kann.

Aus diesen Gründen ist auch die Annahme eines möglichen eingriffsausschließenden Grundrechtsverzichts – zumindest bei der Nutzung von Blockchain-Technologien – abzulehnen.

iii. Eingriffserweiterung bei Kenntnisnahme sozialer Netzwerke?

Diskussionswürdig erscheint die von *Eisenmenger* vertretene Auffassung, dass bereits bei der Kenntnisnahme von Daten in sozialen Netzwerken und öffentlich zugänglichen Diskussionsforen ein Eingriff vorliege.[926] Konkret betrifft die von *Eisenmenger* vertretene Auffassung die Kenntnisnahme solcher Daten im Rahmen einer sog. Online-Streife, also der anlassunabhängigen Aufklärung des Internets.[927]

Seine Auffassung begründet *Eisenmenger* insbesondere mit zwei Argumenten:

Einerseits habe sich durch soziale Netzwerke und bei ihrer Nutzung das Verständnis von Privatheit und Öffentlichkeit maßgeblich verändert.[928] Diese Veränderung sei auch im Rahmen der Grundrechtsrelevanz zu berücksichtigen.[929]

Andererseits setzt sich *Eisenmenger* ausführlich mit der herrschenden Literaturauffassung und der Rechtsprechung des BVerfG und deren Begründung, weshalb die Online-Streife keinen Grundrechtseingriff darstelle, auseinander und arbeitet heraus, dass diese Begründung nicht ausreiche. Hierzu führt *Eisenmenger* zunächst aus, dass die maßgebliche Entscheidung des BVerfG zur anlasslosen Internetaufklärung – das Urteil zum VSG

925 *Bauer*, Soziale Netzwerke, S. 117.
926 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 232ff.
927 Siehe zur Begriffsbestimmung ausführlich *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 130ff. Zur vertretenen Auffassung, dass bereits die Kenntnisnahme einen Eingriff darstellt *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 232ff., 236.
928 Siehe hierzu ausführlich *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 93ff., 110f.
929 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 234f.

NRW[930] – in seiner Begründung maßgeblich auf einer Analogiebildung zur analogen Streife beruhe.[931] Da diese analoge Streifenfahrt nicht grundrechtsrelevant sei, greife auch die so vergleichbare Online-Streife nicht in Grundrechte ein.[932] Anschließend stellt *Eisenmenger* dar, dass der für die Analogiebildung herangezogene Vergleich auf Grund von tatsächlichen Unterschieden zwischen analoger und virtueller Streife nicht möglich sei.[933] Hierzu führt er insbesondere an, dass die analoge Streife „offen" vorgenommen werde und innerhalb von räumlichen, zeitlichen und sozialen Grenzen stattfinde.[934] Dagegen würden Online-Streifen „verdeckt" stattfinden und auf Grund der technischen Gegebenheiten von sozialen Netzwerken nicht lediglich innerhalb räumlicher, zeitlicher und sozialer Grenzen stattfinden.[935] Denn die Verknüpfungsdichte und Persistenz von Daten in sozialen Netzwerken sei im Vergleich zu einer analogen Streifenfahrt wesentlich erhöht.[936] Anders als bei der typischen Beobachtung eines Marktplatzes, bei der eine Kenntnisnahme des Geschehens nur durch die zu gleicher Zeit am gleichen Ort Anwesenden Personen möglich sei[937], sei es nämlich bei der Online-Streife möglich, einen unbegrenzten Personenkreis zur Kenntnis zu nehmen und insbesondere die zur Kenntnis genommenen Informationen – etwa Profilseiten von Nutzern – viel schneller mit anderen Informationen zu verknüpfen.[938] Darüber hinaus bestünde für den Betroffenen die Gefahr, dass die anlasslose Ermittlungstätigkeit der Online-Streife jederzeit in eine gezielte hoheitliche Ermittlungstätigkeit umschlagen könne.[939]

Dieser im Grundsatz nachvollziehbaren Ansicht von *Eisenmenger* ist Folgendes entgegenzuhalten:

Soweit bereits die bloße Kenntnisnahme von öffentlich verfügbaren Daten im Internet einen Grundrechtseingriff darstellen soll, würde dies zunächst zum praktischen Problem führen, dass insoweit (fast[940]) jeder

930 BVerfGE 120, 274ff. Siehe hierzu bereits ausführlich Kap. 4, B.III.2.b)(1)i.
931 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 160f.
932 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 161.
933 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 171f.
934 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 171.
935 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 171.
936 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 171.
937 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 168f.
938 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 168f., 234f.
939 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 235.
940 Dies kann insoweit nur gelten, wenn personenbezogene Daten (siehe zum Begriff bereits ausführlich oben unter Kap. 4, B.III.1.b)) hierdurch zur Kenntnis genommen werden.

Aufruf einer Internetseite zu einem Eingriff in das RiS führen würde. Damit wäre für jeden Aufruf einer Internetseite durch eine staatliche Stelle eine entsprechende Ermächtigungsgrundlage erforderlich. Dies würde insoweit zu einer ausufernden Annahme von rechtfertigungsbedürftigen Grundrechtseingriffen führen. Dem ließe sich zwar auf den ersten Blick entgegenhalten, dass für den Bereich der Strafverfolgung die Generalermittlungsklausel des § 161 StPO bestünde. Hiergegen spricht jedoch, dass die Frage, ob insgesamt eine verfassungsrechtliche Rechtfertigung in Form einer gesetzlichen Grundlage notwendig ist, nicht mit dem Verweis beantwortet werden kann, dass für einen Teilbereich eine derartige gesetzliche Grundlage besteht. Darüber hinaus findet die Generalermittlungsklausel des § 161 StPO für den von *Eisenmenger* betrachteten Bereich der anlasslosen Internetaufklärung mangels Anfangsverdacht ohnehin keine Anwendung.[941]

Soweit *Eisenmenger* diesen ausufernden Grundrechtseingriff auf besonders persönlichkeitsbezogene im Internet verfügbare Inhalte begrenzt[942], birgt diese Abgrenzung das Problem der fehlenden Trennschärfe. Zwar ist der Hintergrund insoweit nachvollziehbar, als dass das RiS gerade diese persönlichkeitsrelevante Ebene schützen soll, es stellt sich aber die Frage, ab wann dieser Schutz betroffen sein kann.

Hinzukommt, dass die fehlende Vergleichbarkeit von analoger und virtueller Streife zwar auf den unterschiedlichen tatsächlichen Gegebenheiten – hohe Verknüpfungsdichte, Persistenz und Durchsuchbarkeit von Informationen in sozialen Netzwerken – beruht, ob ein grundrechtseingriff vorliegt oder nicht, sollte jedoch nicht von den technischen Gegebenheiten des Internets, sondern vom jeweiligen staatlichen Handeln abhängig gemacht werden.[943]

Insoweit ist die von *Eisenmenger* vertretene Auffassung, dass jede Kenntnisnahme von öffentlich verfügbaren Daten im Internet, soweit sie eine gewisse Persönlichkeitsrelevanz haben, abzulehnen.

(3) Zwischenergebnis

Vorzugswürdig erscheint im Sinne der Rechtsprechung des BVerfG für die Grenze eines Eingriffs in das RiS bei öffentlich verfügbaren Daten auf den

941 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 267.
942 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 236.
943 Hierzu sogleich ausführlich.

Modus der Datenverarbeitung und nicht auf den Inhalt bzw. die Persönlichkeitsrelevanz der verarbeiteten Daten abzustellen.

Denn Hintergrund des RiS ist der Schutz der freien Entfaltung der Persönlichkeit. Zu ihrer Gewährleistung ist erforderlich, dass einerseits die berechtigten Geheimhaltungsinteressen des Einzelnen gewahrt werden und andererseits der Einzelne überblicken kann, wer wann was über ihn weiß und deshalb nicht sein Verhalten anpasst.[944]

Maßgeblich ist insoweit, ob durch die Datenverarbeitung durch staatliche Stellen eine Gefährdung für die Persönlichkeit des Einzelnen besteht.

Zwar ist die von *Eisenmenger* vertretene Auffassung dahingehend nachvollziehbar, dass sich durch die Kenntnisnahme von persönlichkeitsrelevanten Daten in sozialen Netzwerken Gefahren für die Persönlichkeit des Einzelnen ergeben können, diese Gefahren beruhen jedoch nicht auf der Art der zur Kenntnis genommenen Daten, sondern auf der Art und Weise der Datenverarbeitung.

Denn es besteht insoweit keine Gefahr für die Persönlichkeitsentfaltung des Einzelnen, wenn eine staatliche Stelle Inhalte zur Kenntnis nimmt, die der Betroffene selbst preisgegeben hat. Durch die Preisgabe ist dem Betroffenen insoweit bewusst, dass die Inhalte von einem unbestimmten Personenkreis – und damit auch von staatlichen Stellen – zur Kenntnis genommen werden können. Insoweit besteht nicht die Gefahr, dass der Einzelne aus diesem Grund sein Verhalten anpasst oder seine berechtigten Geheimhaltungsinteressen betroffen sind.

Eine Gefahr für die Persönlichkeitsentfaltung des Betroffenen liegt jedoch dann vor, wenn über die bloße Kenntnisnahme – die der Betroffene bewusst selbst ermöglich hat – hinaus Daten im Sinne einer erweiterten Erfassung oder Verknüpfung verarbeitet werden. Sobald der Einzelne nicht mehr überblicken kann, welche Informationen sich hieraus über ihn ergeben (können), besteht sowohl die Möglichkeit, dass eine Gefahr für seine berechtigten Geheimhaltungsinteressen bestehen bzw. eine Anpassung seines Verhaltens stattfindet. Dies hängt aber maßgeblich davon ab, welche Datenverarbeitungsmaßnahmen ergriffen werden, denn erst durch eine über die Kenntnisnahme hinausgehende Verknüpfung der Daten lassen sich weitergehende Informationen über den Betroffenen ermitteln.

Die Grenze zwischen einer eingriffsbegründenden und einer nicht eingriffsbegründenden persönlichkeitsgefährdenden Datenverarbeitung hängt

944 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.III.1.a).

damit auch davon ab, wann der Einzelne nicht mehr überblicken kann, welche Daten über ihn erhoben und ermittelt werden.

Bei selbstveröffentlichten Daten nimmt der Betroffene an, dass diese von Dritten zur Kenntnis genommen werden – er veröffentlicht sie ja gerade zu diesem Zweck.

Dagegen hat er keinerlei Möglichkeit zu überblicken, welche sich daran anschließenden Datenverarbeitungsmaßnahmen sich aus seinen veröffentlichten Daten ergeben. Selbst wenn ihm bewusst wäre, welche Daten er insgesamt selbst veröffentlicht hat, wird er in der Regel kein tiefgreifendes technisches Verständnis davon haben, welche informationstechnischen Verknüpfungsmöglichkeiten sich hieraus ergeben.

Insoweit muss der Schutz des RiS gerade an dieser Grenze ansetzen. Dem Einzelnen müsste zwar jeweils bewusst sein, wenn und dass er Daten öffentlich verfügbar macht und sie dadurch für Dritte zur Kenntnis genommen werden, alle darüberhinausgehenden Datenverarbeitungsmöglichkeiten kann er dagegen nicht überblicken. So kann er bereits nicht mehr feststellen, welche Daten, die er im Internet preisgegeben hat, von Dritten gespeichert wurden.

Deshalb muss der Schutz des RiS an dieser Grenze ansetzen.

Daraus ergibt sich, dass für öffentlich verfügbare Daten die Grenze zum Eingriff überschritten ist, wenn über die bloße Kenntnisnahme hinaus, öffentlich verfügbare Daten erhoben und gespeichert werden und sich eine Persönlichkeitsgefährdung des Einzelnen daraus ergibt, dass er nicht mehr überblicken kann, welche Daten über ihn erhoben werden und welche Schlüsse durch weitergehende Datenverarbeitungsmaßnahmen sich hieraus ergeben können.

c) Liegt durch die dargestellten Auswertungsmethoden ein Eingriff in das RiS in diesem Sinne vor?

Dementsprechend stellt sich nun die Frage, ob und für welche Auswertungsmethoden nach den so herausgearbeiteten Kriterien ein Eingriff in das RiS vorliegt.

(1) Auswertung der unmittelbaren Blockchain-Daten

Für die in Kap. 3, A. dargestellten Auswertungsmethoden sind die unmittelbaren Blockchain-Daten die maßgebliche Datengrundlage.[945]

Fraglich ist zunächst, ob ein Eingriff in das RiS bereits durch die Erhebung der Blockchain-Daten, also das unmittelbare Herunterladen der jeweiligen Blockchain, vorliegt.

Dafür spricht insoweit die soeben herausgearbeitete Grenze, dass bei öffentlich verfügbaren Daten bereits ihre Speicherung einen Eingriff begründen kann. Zu berücksichtigen ist jedoch, dass sich aus der Speicherung die Gefahr einer Persönlichkeitsgefährdung dahingehend ergeben muss, dass der Einzelne nicht mehr überblicken kann, welche Informationen, über ihn erhoben und gespeichert werden.

Bei der Erhebung von Blockchain-Daten müssen auch deren technische Besonderheiten berücksichtigt werden. Denn anders als bei herkömmlichen Internetseiten ist die dezentrale Verwaltung der Inhaltsdaten eine ihrer wesentlichen technischen Eigenschaften. Aus dieser technischen Eigenschaft folgt auch, dass die Blockchain-Daten bei unzählig vielen Nutzern gespeichert sind und nachträglich nicht verändert werden können.

Insoweit muss dem Nutzer einer Blockchain-Technologie bewusst sein, dass seine Daten von einem unbestimmten Personenkreis gespeichert werden und nachträglich nicht veränderbar sind. Dementsprechend kann auch bei einer staatlichen Beteiligung an einem Blockchain-Netzwerk aus diesem Grund kein Eingriff durch das Herunterladen der Blockchain vorliegen.

Auch, dass die Blockchain-Daten bereits chronologisch geordnet sind, ändert hieran nichts, denn insoweit gilt ebenfalls, dass dies eine technische Eigenheit der Blockchain-Technologie ist und dem Nutzer dies insoweit bewusst sein muss, sodass das Herunterladen wiederum nicht über das hinausgeht, was ein Nutzer selbst preisgegeben hat.

Die Grenze zur Persönlichkeitsgefährdung dürfte jedoch dann überschritten sein, wenn über das Herunterladen der Blockchain-Daten hinaus, aus ihnen Rückschlüsse gezogen werden, die über die bloßen Inhaltsdaten der Blockchain hinausgehen. Dies dürfte bei allen in Kap. 3, A. dargestellten Auswertungsmethoden der Fall sein. Denn bei jeder Auswertungsmethode werden die in der Blockchain enthaltenen Transaktionsinformationen dahingehend ausgewertet, dass über die Kenntnisnahme der einzelnen Transkationen hinaus weitere Rückschlüsse auf das dahinterste-

945 Siehe hierzu ausführlich Kap. 3, A.

hende Verhalten bzw. die dahinterstehende *Entität* gezogen werden. Denn bereits beim sog. *Entitätsclustering* wird der über die Kenntnisnahme der einzelnen Transaktionen hinausgehende Rückschluss gezogen, dass hinter mehreren verschiedenen *Bitcoin-Adressen* die gleiche *Entität* steht. Das gilt insoweit auch für die darüberhinausgehenden Auswertungen beim Aufdecken von bestimmten Transaktionsverhalten und dem Vergleich mit bekanntem Transaktionsverhalten – etwa zur Kategorisierung von *Entitäten*.

(2) Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens

Dementsprechend liegt ebenfalls bereits ein Eingriff vor, soweit durch die Auswertung der Verbreitung von Transaktionsnachrichten eine IP-Adresse einer *Bitcoin-Adresse* zugeordnet wird.[946] Zwar ließe sich noch argumentieren, dass die hierzu erforderliche Verbindung mit den anderen Nutzern des jeweiligen Blockchain-Netzwerks keinen rechtfertigungsbedürftigen Eingriff darstellt, da hierbei lediglich Informationen zur Kenntnis genommen werden, die der Betroffene jeweils selbst preisgibt. Die Grenze des Eingriffs ist jedoch bereits dann überschritten, wenn diese Netzwerkdaten für eine spätere Auswertung gespeichert werden[947] und ist insbesondere dann überschritten, wenn die so erhobenen Daten ausgewertet werden.[948]

Nichts Anderes kann dabei für die IP-Adressen-Ermittlung gelten, wenn hierzu die Verbindung über das *Tor-Netzwerk* verhindert wird.[949] Denn hierdurch ändert sich insoweit nur ein Umstand bei der Datenerhebung, und zwar, dass die Verwendung des *Tor-Netzwerkes* verhindert wird.[950] Die Auswertungsmethode als solches bleibt dagegen bestehen.[951]

Ähnliches gilt, soweit die technischen Eigenheiten des *Tor-Netzwerks* dahingehend ausgenutzt werden, dass der so übermittelte Datenverkehr ausgewertet wird.[952] Allenfalls dürfte die bloße Kenntnisnahme des so übermittelten Datenverkehrs keinen Eingriff begründen, da der Betroffene diesen durch Nutzung des *Tor-Netzwerks* insoweit bewusst preisgegeben

946 Siehe zu dieser Auswertungsmöglichkeit oben unter Kap. 3, B.I.
947 *Reid/Harrigan*, SPSN 2013, 197 (214) m.w.N. Siehe hierzu bereits Kap. 3, B.I.
948 *Reid/Harrigan*, SPSN 2013, 197 (214) m.w.N. Siehe hierzu bereits Kap. 3, B.I.
949 Siehe zu dieser Auswertungsmöglichkeit oben unter Kap. 3, B.II.
950 Siehe hierzu bereits unter Kap. 3, B.II.2.
951 Siehe hierzu bereits unter Kap. 3, B.II.2.
952 Siehe zu dieser Auswertungsmöglichkeit oben unter Kap. 3, B.II.3.

hat, wenn auch mit einer anderen Intention. Jede weitere Auswertung der so erhobenen Daten begründet dagegen einen Eingriff in das RiS.

Darüber hinaus stellt auch die IP-Adressen-Ermittlung mittels *Bloom-Filter-Attacks*[953] einen Eingriff nach den hergeleiteten Grundsätzen dar. Denn der Betroffene hinterlegt zwar bewusst seinen *Bloom-Filter* beim auswertenden *Full-client,* von dieser bewussten Preisgabe ist jedoch nicht die systematische Auswertung der hinterlegten *Bloom-Filter* in Form eines Durchsuchens nach Treffern erfasst, um so *Bitcoin-Adressen* IP-Adressen zuordnen zu können.

(3) Auswertung anderweitig verfügbarer Daten

Soweit mittels *Internet-Crawler* das Internet nach der Zeichenstruktur von *Bitcoin-Adressen* durchsucht wird[954], stellt dies ebenfalls einen entsprechenden Eingriff in das RiS dar, da insoweit ein über die bloße Kenntnisnahme von selbstveröffentlichten Daten hinausgehendes systematisches und zielgerichtetes Durchsuchen öffentlich verfügbarer Daten vorliegt.

Je nach konkreter Ausgestaltung von Auswertung von Dritt-Anbieter-Cookies und den Standortdaten von IoT-Anwendungen, dürfte in der Regel auch bei diesen ein entsprechender Eingriff in das RiS anzunehmen sein, da die Auswertungsmethoden wohl in der Regel über die bloße Kenntnisnahme der veröffentlichten Daten hinausgehen werden.

d) Zwischenergebnis

Nach den vorstehend herausgearbeiteten Kriterien für einen Eingriff in das RiS bei öffentlich verfügbaren Daten stellen alle in Kap. 3 dargestellten Auswertungsmethoden einen Eingriff in das RiS dar.

3. Zwischenergebnis

Alle in Kap. 3 dargestellten Auswertungsmethoden begründen einen rechtfertigungsbedürftigen Eingriff in das RiS.

953 Siehe zu dieser Auswertungsmöglichkeit oben unter Kap. 3, B.III.
954 Siehe zu dieser Auswertungsmöglichkeit oben unter Kap. 3, C.I.

III. Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme – „IT-Grundrecht"

Außerdem könnte durch die Anwendung der in Kap. 3 dargestellten Auswertungsmethoden jeweils ein Eingriff in das vom BVerfG aus dem allgemeinen Persönlichkeitsrecht entwickelte Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (nachfolgend als „IT-Grundrecht" bezeichnet[955]) vorliegen.

Ein wesentliches Problem in diesem Zusammenhang ist die Abgrenzung zwischen einer reinen nicht in den Schutzbereich des IT-Grundrechts fallenden Internetaufklärung[956] und dem vom Schutzbereich des IT-Grundrechts erfassten Zugriff auf geschützte informationstechnische Systeme. Denn das BVerfG hat im grundlegenden Urteil zum IT-Grundrecht[957] vorgegeben, dass die reine Internetaufklärung das IT-Grundrecht nicht berühre, da sich die Internetaufklärung auf Datenerhebungen beschränke, „die der Inhaber des Systems – beispielsweise der Betreiber eines Webservers – für die Internetkommunikation vorgesehen [habe]"[958] und er daher nicht darauf vertrauen könne, dass diese Daten nicht erhoben würden.[959] Für die Auswertungsmethoden bei Blockchain-Systemen ist dies insoweit problematisch, als dass die dargestellten Auswertungsmethoden zwar in vergleichbarer Art und Weise lediglich auf Daten zugreifen, die öffentlich verfügbar sind[960]. Anders als die herkömmliche Internetaufklärung sind dagegen die Blockchain-Daten als einheitlicher, umfangreicher Datensatz verfügbar.[961] Die Notwendigkeit des Schutzes durch das IT-Grundrecht wird aber gerade auch damit begründet, dass beim Zugriff auf informationstechnische Systeme, die Möglichkeiten zur Datenerhebung weit umfangreicher sind, als bei einzelnen Datenerhebungen.[962] Insoweit stellt sich die Frage, ob bei den dargestellten Auswertungsmethoden eine nicht geschützte Internetaufklärung vorliegt oder der Zugriff auf ein vom IT-Grundrecht geschütztes informationstechnisches System.

955 Zur Begrifflichkeit kritisch siehe BeckOK-InfoMedienR/*Gersdorf,* GG Art. 2 Rn. 22, der den Begriff des IT-Grundrechts als irreführend bezeichnet.
956 Siehe hierzu unter BVerfGE 120, 274 (344).
957 BVerfGE 120, 274ff.
958 BVerfGE 120, 274 (344).
959 BVerfGE 120, 274 (344).
960 Siehe hierzu bereits ausführlich unter Kap. 4, B.II.2.c).
961 Vgl. hierzu bereits ausführlich unter Kap. 4, B.II.1.c).
962 BVerfGE 120, 274 (313). Siehe hierzu ausführlich sogleich.

Um diese Frage zu beantworten, wird nachfolgend zunächst die Herleitung des IT-Grundrechts (hierzu unter 1.) dargestellt, anschließend der Schutzbereich des IT-Grundrechts herausgearbeitet (hierzu unter 2.) und dann auf die Frage eingegangen, ob bei der Anwendung der Auswertungsmethoden der Schutzbereich des IT-Grundrechts betroffen ist (hierzu unter 3.).

1. Herleitung und Begründung des IT-Grundrechts

Das in der Entscheidung des BVerfG zum VSG NRW[963] entwickelte IT-Grundrecht schützt Grundrechtsträger vor dem unberechtigten Zugriff auf informationstechnische Systeme und geht insoweit über den Schutz vor einem Zugriff auf einzelne Kommunikationsvorgänge oder gespeicherte Daten hinaus.[964]

Die Notwendigkeit und den Schutzbereich dieses IT-Grundrechts begründet das BVerfG einerseits mit der zunehmenden Verbreitung derartiger „informationstechnischer Systeme" und andererseits mit der besonderen Persönlichkeitsrelevanz, die diese auf Grund ihrer allgegenwärtigen Nutzung entfalten können.[965]

Da das allgemeine Persönlichkeitsrecht auch eine lückenschließende Funktion habe, müsse es neuartigen Gefährdungen begegnen, die sich im „Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse"[966] ergäben. Solche Gefährdungen könnten sich daraus ergeben, dass von informationstechnischen Systemen sowohl bewusst vom Nutzer erzeugte personenbezogene Daten als auch unbewusst selbsttätig erzeugte Daten gespeichert und verarbeitet würden.[967] Beim Zugriff durch Dritte auf diese Systeme und deren Daten wären daher umfassende und „weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung"[968] möglich. Derartige Gefährdungen seien bei der Vernetzung solcher Systeme mit dem Internet noch vertieft, da einerseits eine noch größere Datenmenge anfallen könne und andererseits eine erhöhte

963 BVerfGE 120, 274ff.
964 BVerfGE 120, 274 (313).
965 BVerfGE 120, 274 (302f.).
966 BVerfGE 120 274 (303).
967 BVerfGE 120, 274 (305).
968 BVerfGE 120, 274 (305).

Gefahr eines unberechtigten Zugriffs bestehen würde.[969] Aus diesen Persönlichkeitsgefährdungen folge ein erhebliches grundrechtliches Schutzbedürfnis, dem die bisherigen grundrechtlichen Gewährleistungen aus Art. 10, Art. 13 GG und dem allgemeinen Persönlichkeitsrecht nicht hinreichend Rechnung trügen.[970]

Insbesondere das RiS gewährleiste zwar im Grundsatz den Schutz vor Persönlichkeitsgefährdungen, die sich aus Datenerhebungen und anderen Datenverarbeitungsmaßnahmen ergäben.[971] Dieser Schutz reiche allerdings dahingehend nicht aus, dass Dritte sich durch den Zugriff auf informationstechnische Systeme „einen potentiell äußerst großen und aussagekräftigen Datenbestand [verschafften], ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff [gehe] in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung [schütze], weit hinaus."[972]

Daher trage das allgemeine Persönlichkeitsrecht in seiner lückenfüllenden Funktion diesem Schutzbedarf dahingehend Rechnung, dass es die „Integrität und Vertraulichkeit informationstechnischer Systeme"[973] gewährleiste. Das bedeute, dass es den Grundrechtsträger „vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit [bewahre], als auf das informationstechnische System insgesamt zugegriffen werde und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten."[974]

Das IT-Grundrecht soll insoweit vor Gefährdungen für die Persönlichkeit des Einzelnen schützen, die sich daraus ergeben können, dass Dritte unberechtigterweise auf informationstechnische Systeme zugreifen, die einen großen Datenbestand personenbezogener Daten erheben, speichern und verarbeiten und vor denen andere grundrechtliche Gewährleistungen keinen ausreichenden Schutz bieten.[975]

969 BVerfGE 120, 274 (305f.).
970 BVerfGE 120, 274 (306). Siehe zur ausführlichen Begründung und Darstellung der Schutzlücken von Art. 10, 13 GG und dem allgemeinen Persönlichkeitsrecht ausführlich BVerfGE 120, 274 (306ff.).
971 BVerfGE 120, 274 (312).
972 BVerfGE 120, 274 (313).
973 BVerfGE 120, 274 (313).
974 BVerfGE 120, 274 (313).
975 BVerfGE 120, 274 (306, 313).

2. Schutzbereich des IT-Grundrechts

Ob der Schutzbereich des IT-Grundrechts eröffnet ist, hängt nach dem BVerfG zunächst davon ab, ob ein geschütztes informationstechnisches System vorliegt.[976]

a) Schutzgegenstand – Informationstechnische Systeme

Ein informationstechnisches System kann grundsätzlich nach dem BVerfG jeder Rechner und jeder Verbund von Rechnern und Rechnernetzwerken sein.[977] So stellt bereits das Internet selbst ein solches informationstechnisches System dar.[978] Nach weitgehend vertretener Auffassung ist der Begriff des informationstechnischen Systems weit zu verstehen, sodass sämtliche informationstechnische Systeme erfasst sind, die Daten verarbeiten können.[979] Erfasst sind dabei auch Netze, die aus mehreren „räumlich getrennten Komponenten bestehen [...], wenn die verbundenen Geräte funktional eine Einheit bilden."[980]

Ob ein solches informationstechnisches System vom Schutzbereich des IT-Grundrechts erfasst sei, hänge nach der Rechtsprechung des BVerfG zunächst davon ab, ob die vom informationstechnischen System gespeicherten und verarbeiteten Daten qualitativ über den Datenbestand anderer Datenerhebungen hinausgingen.[981] Dies sei etwa dann nicht der Fall, wenn „ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen [enthalte] – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik"[982].

Dagegen sei der Schutzbereich des IT-Grundrechts für informationstechnische Systeme eröffnet, die „allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und

976 BVerfGE 120, 274 (313).
977 BVerfGE 120, 274 (276).
978 BVerfGE 120, 274 (276). So auch *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 203.
979 *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 126; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 92; *Michael/Morlok*, Grundrechte, Rn. 427.
980 *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 126; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 92 mit Verweis auf BVerfG NJW 2008, 822 Rn. 203.
981 BVerfGE 120, 274 (313).
982 BVerfGE 120, 274 (313).

in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten."[983] Als Beispiele für derartige informationstechnische Systeme nennt das BVerfG etwa „Personalcomputer […] Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können."[984]

b) Schutz der Vertraulichkeit verarbeiteter Daten und der Integrität des informationstechnischen Systems

Der Schutz des IT-Grundrechts umfasst dabei zwei Varianten des Schutzes: so soll einerseits die Vertraulichkeit der vom informationstechnischen System erzeugten, gespeicherten und verarbeiteten Daten gewährleistet bleiben und andererseits die Integrität des informationstechnischen Systems als solches bereits vor dem unberechtigten Zugriff durch Dritte geschützt werden.[985] Schutzdimensionen des IT-Grundrechts sind insoweit einerseits die Vertraulichkeit der Daten und andererseits die Integrität des Systems als solches.[986]

Dabei soll der Schutz der Integrität des informationstechnischen Systems nicht davon abhängen, ob der Zugriff „leicht oder nur mit erheblichem Aufwand möglich ist"[987]. Erforderlich für den Schutz ist 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."[988]

Der Schutzbereich des IT-Grundrechts sei allerdings dann nicht berührt, wenn Daten auf dem technisch dafür vorgesehenen Weg erhoben werden, die der Inhaber des Systems für die Internetkommunikation vorgesehen hat.[989]

983 BVerfGE 120, 274 (314).
984 BVerfGE 120, 274 (314).
985 BVerfGE 120, 274 (314).
986 *Böckenförde*, JZ 2008, 925 (928).
987 BVerfGE 120, 274 (315).
988 BVerfGE 120, 274 (315).
989 BVerfGE 120, 274 (344). Siehe hierzu bereits einleitend unter Kap. 4, B.III.

c) Literaturauffassungen zum Schutzbereich des IT-Grundrechts

In der Literatur wurde diese Rechtsprechung des BVerfG insbesondere für die Frage der Grundrechtsrelevanz sog. Online-Streifen[990] und -Ermittlungen[991] in sozialen Netzwerken aufgegriffen.[992]

So nimmt etwa *Bauer* an, dass auf Grund der Rechtsprechung des BVerfG bei strafprozessualen Ermittlungen in sozialen Netzwerken kein Eingriff in das IT-Grundrecht vorliege, da sich Daten in sozialen Netzwerken an die Netzwerköffentlichkeit richteten, sodass die Nutzer keine berechtigte Vertraulichkeitserwartung haben könnten.[993]

Ähnlich arbeitet *Eisenmenger* heraus, dass im Grundsatz zwar bei sozialen Netzwerken gerade die für die Herleitung des IT-Grundrechts erforderliche Datenmenge vorliege, vor dem „Hintergrund des Entscheidungskontextes"[994] des BVerfG jedoch eine gewisse „hardwareäquivalente"[995] Auslegung geboten sei, sodass für das Vorliegen eines informationstechnischen Systems mindestens eine gewisse „gerätegleiche Ersatzfunktion"[996] erforderlich sei. Diese läge bei sozialen Netzwerken gerade nicht vor, sodass der Schutzbereich des IT-Grundrechts beim Zugriff auf soziale Netzwerke nicht eröffnet sei.[997]

d) Zwischenergebnis

Vom Schutzbereich des IT-Grundrechts erfasst sind technische Gegenstände, die Daten verarbeiten können und deren Datenverarbeitung derart

990 Siehe hierzu etwa *Eisenmenger,* Grundrechtsrelevanz virtueller Streifenfahrten.
991 Siehe hierzu etwa *Bauer*, Soziale Netzwerke, S. 108.
992 Auf die wesentliche Kritik in der Literatur, dass der Schutz des IT-Grundrechts auf Grund eines ausreichenden Schutzes des RiS entbehrlich sei, wird nicht weiter eingegangen, da dies für die Frage nach der Grundrechtsrelevanz der Auswertung von Blockchain-Systemen nicht relevant ist. Siehe zur Kritik in der Literatur im Überblick *Bäcker*, Linien der Rechtsprechung Bd. 1, S. 120 m.w.N., der die Notwendigkeit des IT-Grundrechts über den Schutz des RiS hinaus insbesondere damit begründet, dass nicht nur die Vertraulichkeit der Daten von IT-Systemen geschützt sei, sondern insbesondere auch die Integrität des IT-Systems selbst. Siehe hierzu auch Dreier Bd. 1/*Dreier,* Art. 2 Abs. 1 Rn. 84 m.w.N.
993 *Bauer*, Soziale Netzwerke, S. 108.
994 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 204.
995 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 204.
996 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 204.
997 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 203. Ähnlich insoweit auch *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 92f.

über einen lediglich punktuellen Lebensbereich hinausgehen, dass ihr Datenbestand qualitativ über andere Datenerhebungen hinausgeht und so einen Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglichen. Geschützt sind einerseits die Vertraulichkeit der Daten des informationstechnischen Systems und andererseits die Integrität des informationstechnischen Systems soweit der Betroffene alleine oder zusammen mit bestimmten anderen über das informationstechnische System verfügen kann.

Vom Schutzbereich ausgeschlossen sind dagegen Daten von informationstechnischen Systemen, die für die Internetkommunikation vorgesehen sind, sodass insoweit öffentlich verfügbare Daten nicht vom Schutzbereich erfasst sind.

3. Blockchain-Systeme als geschützte informationstechnische Systeme?

Insoweit stellt sich die Frage, ob nach diesen Maßstäben bei der Anwendung der in Kap. 3 dargestellten Auswertungsmethoden der Schutzbereich des IT-Grundrechts eröffnet ist. Soweit die unterschiedlichen Auswertungsmethoden unterschiedliche Datengrundlagen nutzen, ist für die rechtliche Bewertung hiernach zu differenzieren. So stellt sich zunächst die Frage, ob der Zugriff auf ein Blockchain-System in den Schutzbereich des IT-Grundrechts fällt (hierzu unter a))[998]. Daran anschließend stellt sich die Frage, ob sich eine abweichende rechtliche Bewertung dadurch ergeben kann, dass die Netzwerkverbindungen eines Blockchain-Systems ausgewertet werden (hierzu unter b))[999] und insbesondere, ob der Schutzbereich des IT-Grundrechts betroffen ist, wenn die Verbindung mit dem Blockchain-System über das *Tor-Netzwerks* verhindert wird (hierzu unter c))[1000] bzw. mittels dem *Tor-Netzwerk* der Datenverkehr ausgewertet wird (hierzu unter d)). Zusätzlich stellt sich die Frage, wie die Auswertung von *Bloom-Filtern*[1001] zu bewerten ist (hierzu unter e)). Abschließend stellt sich die Frage, ob der Schutzbereich des IT-Grundrechts bei der Auswertung anderweitig verfügbarer Daten betroffen ist (hierzu unter f))[1002].

998 Maßgebliche Auswertungsmethoden sind hier die in Kap. 3, A. dargestellten.
999 Maßgebliche Auswertungsmethoden sind hier die in Kap. 3, B.I.,III. dargestellten.
1000 Maßgebliche Auswertungsmethoden sind hier die in Kap. 3, B.II. dargestellten.
1001 Siehe hierzu oben unter Kap. 3, B.III.
1002 Maßgebliche Auswertungsmethoden sind hier die in Kap. 3, C. dargestellten.

a) Auswertung der Blockchain-Daten

Dementsprechend stellt sich zunächst die Frage, ob ein Blockchain-System bereits ein vom IT-Grundrecht erfasstes informationstechnisches System ist.

Problematisch ist in diesem Zusammenhang zunächst, ob das IT-Grundrecht überhaupt betroffen sein kann, wenn bereits ein Eingriff in das RiS vorliegt.[1003] Im grundlegenden Urteil des BVerfG zum IT-Grundrecht[1004] stellt das BVerfG darauf ab, dass das IT-Grundrecht vor „Eingriffen in informationstechnische Systeme [schütze], soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist"[1005]. Auch auf Grund der lückenfüllenden Schutzfunktion[1006] ist insoweit von einem Spezialitätsverhältnis dahingehend auszugehen, dass das IT-Grundrecht subsidiär zum Schutz anderer Grundrechte ist.[1007] Da bei den dargestellten Auswertungsmethoden von Blockchain-Inhalten jeweils ein Eingriff in das RiS vorliegt[1008], kann bei ihrer Anwendung insoweit auf Grund der Subsidiarität des IT-Grundrechts dessen Schutzbereich nicht betroffen sein. Daher kommt allenfalls die Eröffnung des Schutzbereichs für die nicht vom RiS erfasste staatliche Beteiligung an einem Blockchain-System[1009] in Betracht, durch die insbesondere die Datengrundlage der jeweiligen Blockchain für die weiteren Ausführungen heruntergeladen und damit verfügbar gemacht wird.[1010]

Wie oben bereits dargestellt[1011] ist ein Blockchain-System ein Zusammenschluss mehrerer Rechner zu einem *Peer-to-Peer-Netzwerk,* durch das die Nutzer gemeinsam eine bestimmte Datenbank fortschreiben.

Da der Begriff des informationstechnischen Systems weit auszulegen ist und auch den Verbund von Rechnern erfasst, liegt in dem Zusammen-

1003 Siehe hierzu ausführlich oben unter Kap. 4, B.II.2.c).
1004 BVerfGE 120, 274ff.
1005 BVerfGE 120, 274 (302).
1006 BVerfGE 120, 274 (303).
1007 So auch BeckOK-InfoMedienR/*Gersdorf,* GG Art. 2 Rn. 24; *Michael/Morlok*, Grundrechte, Rn. 427. Vgl. SHH-GG/*Hofmann,* Art. 2 Rn. 17; vgl. insoweit auch Specht/Mantz-HdB DSR/*Brethauer,* § 2 Rn. 8.
1008 Siehe hierzu ausführlich unter Kap. 4, B.II.2.c).
1009 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c).(1).
1010 Siehe hierzu bereits ausführlich unter Kap. 4, B.II.2.c).(1), Kap. 3, A.
1011 Siehe hierzu ausführlich unter Kap. 2, A.II.,III.

schluss der Rechner durch eine Blockchain-Technologie im Grundsatz ein informationstechnisches System vor. Die in einer Blockchain enthaltenen Daten hängen zwar von der jeweiligen konkreten Anwendung ab[1012], sie dürften auf Grund ihrer umfassenden Inhalte – etwa über Transaktionen von Kryptowährungen[1013] – über lediglich punktuelle Lebensbereiche, wie nicht vernetzte Haushaltstechnik, hinausgehen.

Der Schutzbereichseröffnung für Blockchain-Systeme stehen jedoch zwei wesentliche Voraussetzungen des IT-Grundrechts entgegen: die Vertraulichkeit der Daten und die Integrität des informationstechnischen Systems. Denn anders als bei der an Personalcomputern orientierten Rechtsprechung des BVerfG kann bei einem Blockchain-System, deren Grundvoraussetzung ihre öffentliche Einsehbarkeit ist, keine Vertraulichkeitserwartung der beteiligten Nutzer in die in der Blockchain enthaltenen Daten bestehen. Außerdem ist bei einem staatlichen Zugriff auf ein Blockchain-System nicht die Integrität des Systems verletzt, da die hier gegenständlichen Blockchains als offene Netzwerke ausgestaltet sind. Die beteiligten Nutzer können insoweit nicht davon ausgehen, dass sie im Sinne des Schutzbereichs des IT-Grundrechts über das Blockchain-System verfügen können. Denn ein Blockchain-System zeichnet ja gerade aus, dass alle beteiligten Rechner die Datenbank gemeinsam fortschreiben und insoweit gemeinsam über sie verfügen. Dabei sind Blockchain-Systeme nicht auf bestimmte Nutzer beschränkt. Deshalb gibt es auch keine Nutzer, die alleine oder gemeinsam mit anderen Nutzern über das informationstechnische System verfügen können. Insoweit kann die Integrität eines Blockchain-Systems nicht betroffen sein, wenn eine staatliche Stelle sich hieran beteiligt.

Zwar ließe sich argumentieren, dass bei einer staatlichen Beteiligung an einem Blockchain-System gerade der Sinn und Zweck für den Schutz des IT-Grundrechts betroffen ist, da insoweit der Zugriff auf eine einheitlich verfügbare, umfangreiche Datenquelle vorliegt, der ein umfassendes Bild über die Persönlichkeit der Nutzer ermöglichen kann. Dementsprechend ließe sich annehmen, dass die staatliche Beteiligung an einem Blockchain-System auf Grund der Masse der einheitlich erhebbaren Daten über den bloßen Aufruf von Internetseiten hinausgeht, der nach dem BVerfG nicht vom Schutzbereich des IT-Grundrechts erfasst sein solle.

1012 Siehe hierzu und zu den über Kryptowährungen hinausgehenden Anwendungsmöglichkeiten bereits ausführlich oben unter Kap. 2, B.

1013 Siehe hierzu bereits ausführlich oben unter Kap. 2, A.II.7.,8.

Dem steht jedoch entgegen, dass der Hintergrund für den Schutz des IT-Grundrechts die Gefährdungen für die Persönlichkeit des Betroffenen sind, die sich daraus ergeben, dass eine staatliche Stelle auf einen umfangreichen Datenbestand informationstechnischer Systeme zugreift, die der Betroffene dem informationstechnischen System anvertraut hat. Eine derartige Vertraulichkeits- und Integritätserwartung des Betroffenen in ein informationstechnisches System kann jedoch dann nicht bestehen, wenn das System als offenes Netzwerk ausgestaltet ist und jeder auf die Inhalte zugreifen kann. Daher ist auch ein Blockchain-System im Sinne der Rechtsprechung des BVerfG als für die Internetkommunikation vorgesehen.

Dementsprechend ist der Schutzbereich des IT-Grundrechts bei der staatlichen Beteiligung an Blockchain-Systemen und der damit einhergehenden Erhebung der Blockchain-Daten nicht eröffnet.

b) Auswertung des Netzwerkverhaltens

Dies muss insoweit in vergleichbarer Weise auch für die Auswertung des Netzwerkverhaltens und der Netzwerkverbindungen gelten, da sich die Auswertungsmethoden insoweit nur zu Nutze machen, dass das Blockchain-Netzwerk als offenes Netzwerk ausgestaltet ist und die dort ablaufende Kommunikation von jedermann zur Kenntnis genommen werden kann.

Fraglich könnte diese rechtliche Bewertung allerdings dahingehend sein, dass für die Auswertung des Netzwerkverhaltens nicht nur eine bloße staatliche Beteiligung an einem Blockchain-System erforderlich ist, sondern darüber hinaus eine Verbindung mit allen *Full-nodes* erforderlich ist, um zu ermitteln von welcher IP-Adresse eine Transaktionsnachricht zuerst versandt wurde.[1014] Insoweit geht diese Auswertungsmethode über eine bloße staatliche Beteiligung – wie sie auch bei jedem anderen Nutzer vorliegt – hinaus. In diesem Sinne könnte hierin die vom BVerfG angesprochene Infiltration eines informationstechnischen Systems vorliegen, vor der das IT-Grundrecht gerade auch schützen soll.[1015] Dem steht allerdings wiederum die notwendige Vertraulichkeitserwartung der Nutzer entgegen. Denn der grundrechtliche Schutz hängt zwar nicht davon ab, ob der Zugriff

1014 Siehe hierzu bereits ausführlich unter Kap. 3, B.I.; *Reid/Harrigan*, SPSN 2013, 197 (218); *Feld/Schönfeld/Werner*, PCS. 2014, 1121 (1122f.); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).

1015 Siehe insbesondere BVerfGE 120, 274 (Ls. 2, 306).

leicht oder nur mit erheblichem Aufwand möglich ist[1016], erforderlich ist aber, dass eine „Vertraulichkeits- und Integritätserwartung besteht"[1017], die nur dann vorliegen kann, wenn der Betroffene das „informationstechnische System als eigenes nutzt"[1018]. Eine derartige Vertraulichkeits- und Integritätserwartung kann wiederum nicht bei einem offenen Netzwerk bestehen.[1019]

Daher ist der Schutzbereich des IT-Grundrechts auch nicht betroffen, wenn das Netzwerkverhalten ausgewertet wird.

c) Verhinderung der Verbindung über das Tor-Netzwerk

Fraglich ist allerdings, ob der Schutzbereich des IT-Grundrechts betroffen ist, wenn zur soeben dargestellten Auswertung des Netzwerkverhaltens verhindert wird, dass Nutzer sich über das *Tor-Netzwerk* mit dem Blockchain-System verbinden, in dem zunächst selbst eine Verbindung über das *Tor-Netzwerk* zum Blockchain-System aufgebaut wird und so faktisch die Verbindung über das *Tor-Netzwerk* verhindert wird.[1020]

Insoweit könnte man annehmen, dass hierdurch die Grenze zur Infiltration eines informationstechnischen Systems überschritten ist, da bewusst bestimmte technische Eigenheiten ausgenutzt werden – insbesondere, da das *Tor-Netzwerk* ja gerade zum Zweck der Verschleierung von IP-Adressen eingesetzt wird. Insoweit könnte man auf den ersten Blick annehmen, dass hierin ein Zugriff auf informationstechnische Systeme vorliegt, der nicht auf dem technisch dafür vorgesehenen Weg stattfindet. Problematisch hieran ist allerdings, dass sowohl der Zugriff auf das Blockchain-System als auch auf das *Tor-Netzwerk* auf dem technisch dafür vorgesehenen Weg stattfindet. Beide sind als offene Netzwerke ausgestaltet, sodass ein Zugriff von einem unbestimmten Adressatenkreis möglich ist. Zwar verwenden die Nutzer des *Tor-Netzwerk* dieses gerade zu ihrer Vertraulichkeit, das kann aber nicht dazu führen, dass dies in den Schutzbereich des IT-Grundrechts fällt. Denn einerseits kann bei einem offenen Netzwerk eine derartige Ver-

1016 BVerfGE 120, 274 (315).
1017 BVerfGE 120, 274 (315).
1018 BVerfGE 120, 274 (315).
1019 Siehe hierzu bereits soeben unter Kap. 4, B.III.3.a).
1020 Siehe zur technischen Funktionsweise ausführlich unter Kap. 3, B.II.

traulichkeitserwartung nicht bestehen.[1021] Andererseits erfolgt ohnehin kein Zugriff auf das informationstechnische System als solches. Denn Ziel der gegenständlichen Auswertungsmethode ist es ja gerade, dass das *Tor-Netzwerk* nicht mehr für die Verbindung zu einem Blockchain-System genutzt werden kann. Hierzu wird zwar eine Verbindung über das *Tor-Netzwerk* hergestellt, es erfolgt aber keinerlei Zugriff auf Daten auf einem technisch nicht vorgesehenen Weg.

Daher können etwaige Vertraulichkeits- oder Integritätserwartungen der Nutzer nicht bestehen, sodass auch für diese Auswertungsmethode der Schutzbereich des IT-Grundrechts nicht eröffnet ist.

d) Auswertung des Datenverkehrs mittels Tor-Netzwerk

Vergleichbar gilt dies auch insoweit, wenn darüber hinaus der Datenverkehr dadurch zur Kenntnis genommen wird, dass eine staatliche Stelle selbst einzelne oder mehrere *Relays* für das *Tor-Netzwerk* bereitstellt. Denn der Nutzer des *Tor-Netzwerks* nutzt dieses bewusst, damit die Telekommunikation über mehrere *Relays* weitergeleitet wird, um so seine Kommunikationsspur zu verschleiern. Er kann aber nicht darauf vertrauen, dass diese *Relays* die weitergeleiteten Telekommunikationsdaten nicht zur Kenntnis nehmen. Da für die Bereitstellung von *Relays* oder der Teilnahme am *Tor-Netzwerk* auch keine Zugangsbeschränkungen bestehen, kann insoweit keine berechtigte Vertraulichkeitserwartung der Nutzer bestehen. Hinzukommt, dass das *Tor-Netzwerk* im Kern nur zur Weiterleitung von Telekommunikation zu ihrer Verschleierung verwendet wird und nicht zur „Erfassung und Speicherung" von umfangreichen Datenmengen.

Daher ist der Schutzbereich des IT-Grundrechts auch nicht betroffen, wenn der Datenverkehr mittels *Tor-Netzwerk* ausgewertet wird.

e) Bloom-Filter-Attacks

Ähnliches gilt für die oben dargestellten *Bloom-Filter-Attacks*[1022], da insoweit wiederum kein unberechtigter Zugriff auf ein informationstechnisches System vorliegt, soweit lediglich die Inhalte des bei einem *Full-node* von

1021 Siehe hierzu bereits die Argumentation unter Kap. 4, B.III.3.a), b).
1022 Siehe hierzu bereits unter Kap. 3, B.III.

einem *SPV-Client* hinterlegten *Bloom-Filter* abgefragt werden. Diese Abfrage ist aber grundsätzlich gerade das Ziel der Anwendung derartiger *Bloom-Filter*.[1023]

f) Auswertung anderweitig verfügbarer Daten

Soweit mittels *Internet-Crawler*[1024] das Internet nach veröffentlichten *Bitcoin-Adressen* durchsucht wird, liegt hierin zwar eine systematische Durchsuchung des Internets, diese geht aber insoweit nicht über die reine Internetaufklärung, die nicht vom Schutzbereich des IT-Grundrechts erfasst ist, hinaus.

Soweit darüber hinaus Dritt-Anbieter-Cookies oder Standortdaten bei *IoT-Blockchain-Systemen* ausgewertet werden, hängt die rechtliche Bewertung wiederum von der konkreten Ausgestaltung ab, sodass hierzu wiederum keine rechtliche Bewertung vorgenommen werden kann. Sofern allerdings bei der von *Shahid et.al.*[1025] dargestellten Auswertungsmethode Gegenstand der Auswertungen nur die über die Blockchain vermittelte Kommunikation der Fahrzeuge untereinander ist[1026], liegt hierin kein unberechtigter Zugriff auf ein informationstechnisches System auf einem technisch nicht dafür vorgesehenen Weg. Soweit darüber hinaus die Zuordnung von *public keys* zu einer natürlichen Person mittels Abfrage bei einer zentralen Stelle[1027] stattfindet, stellt dies ebenfalls keinen Zugriff auf einem unberechtigten und technisch nicht dafür vorgesehenen Weg dar. Sodass für diese Auswertungsmöglichkeit der Schutzbereich des IT-Grundrechts nicht eröffnet ist.

4. Zwischenergebnis

Der Schutzbereich des IT-Grundrechts ist bei keiner Anwendung der in Kap. 3 dargestellten Auswertungsmethoden eröffnet.

1023 Siehe hierzu bereits unter Kap. 3, B.III.
1024 Siehe hierzu bereits oben unter Kap. 3, C.I.
1025 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 1 (4).
1026 Einschließlich deren Standortdaten, vgl. *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 1 (4).
1027 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous 2019, 1 (4).

IV. Zwischenergebnis

Bei der Anwendung der in Kap. 3 dargestellten Auswertungsmethoden liegt lediglich ein Eingriff in das RiS vor und auch erst, wenn über die bloße staatliche Beteiligung an einem Blockchain-System und dem damit verbundenen Herunterladen der Blockchain-Inhalte hinaus, die so erhobenen Daten ausgewertet werden, dass sich eine über die einzelnen Daten hinausgehende Information hieraus ergibt.

C. Zusammenfassung

Bei der Auswertung von Blockchain-Inhalten und der damit in Zusammenhang stehenden Daten[1028] liegt lediglich ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor und auch erst, wenn über die bloße Kenntnisnahme bzw. das Herunterladen der Daten hinaus weitergehende Datenverarbeitungen vorgenommen werden.

Zu berücksichtigen ist jedoch, dass jede über die Kenntnisnahme hinausgehende Datenverarbeitungsmaßnahme einen eigenständigen Grundrechtseingriff darstellt. Dies ist insbesondere relevant, da die dargestellten Auswertungsmethoden zu Strafverfolgungszwecken wohl in der Praxis nicht einzeln und unabhängig voneinander stattfinden werden, sondern gerade miteinander kombiniert werden, um so nach Möglichkeit Informationen zur Strafverfolgung zu erhalten. Für die nachfolgend zu beantwortende Frage der verfassungsrechtlichen Rechtfertigung ist daher insbesondere zu berücksichtigen, dass einerseits jede Datenverarbeitungsmaßnahme für sich genommen auf eine ausreichende Ermächtigungsgrundlage gestützt werden muss und andererseits auch für die Kombination der Datenverarbeitungsmaßnahmen eine ausreichende Ermächtigungsgrundlage erforderlich ist. Hierbei ist insoweit auch bei den Anforderungen an eine Ermächtigungsgrundlage für die jeweils einzelne Datenverarbeitungsmaßnahme zu berücksichtigen, ob und unter welchen Voraussetzungen deren Ergebnisse mit den Ergebnissen anderer Auswertungen verknüpft werden können, um so weitergehende Rückschlüsse und Informationen zu erhalten.

1028 Insbesondere der Daten über das Netzwerkverhalten und ähnliche in Kap. 3 dargestellte Daten.