Studien zum Strafrecht 120

Michael Koenen

Auswertung von Blockchain-Inhalten zu Strafverfolgungszwecken

Nomos

DIKE

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Studien zum Strafrecht Band 120

Herausgegeben von
Prof. Dr. Martin Böse, Universität Bonn
Prof. Dr. Gunnar Duttge, Universität Göttingen
Prof. Dr. Dr. h.c. mult. Urs Kindhäuser, Universität Bonn
Prof. Dr. Dr. h.c. Dr. h.c. Claus Kreß, LL.M., Universität zu Köln
Prof. Dr. Hans Kudlich, Universität Erlangen-Nürnberg
Prof. Dr. Dr. h.c. Lothar Kuhlen, Universität Mannheim
Prof. Dr. Ursula Nelles, Universität Münster
Prof. Dr. Dres. h.c. Ulfrid Neumann, Universität Frankfurt a. M.
Prof. Dr. Henning Radtke, Universität Hannover
Prof. Dr. Klaus Rogall, Freie Universität Berlin
Prof. Dr. Frank Saliger, Universität München
Prof. Dr. Helmut Satzger, Universität München
Prof. Dr. Brigitte Tag, Universität Zürich
Prof. Dr. Thomas Weigend, Universität Köln
Prof. Dr. Wolfgang Wohlers, Universität Basel
Prof. Dr. Rainer Zaczyk, Universität Bonn

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Michael Koenen

Auswertung von Blockchain-Inhalten zu Strafverfolgungszwecken

Nomos

DIKE

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dekan: Prof. Dr. Jürgen von Hagen
Erstreferent: Prof. Dr. Martin Böse
Zweitreferent: Prof. Dr. Thorsten Verrel

Die Open-Access-Veröffentlichung dieses Titels wurde durch die Dachinitiative „Hochschule.digital Niedersachsen“ des Landes Niedersachsen ermöglicht.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Bonn, Univ., Diss., 2023

1. Auflage 2023

© Michael Koenen

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-1099-8
ISBN (ePDF): 978-3-7489-4124-8

ISBN 978-3-03891-614-7 (Dike Verlag Zürich/St. Gallen)

DOI: https://doi.org/10.5771/9783748941248

Onlineversion
Nomos eLibrary

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Meiner Mutter

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2021/22 von der Rechts- und Staatswissenschaftlichen Fakultät der Rheinischen-Friedrich-Wilhelms-Universität Bonn als Dissertation angenommen. Literatur und Rechtsprechung wurden bis zur Abgabe im Januar 2022 berücksichtigt.

Besonders danke ich meinem Doktorvater Prof. Dr. Martin Böse für seine außerordentlich intensive Betreuung – ohne ihn wäre diese Arbeit nicht möglich gewesen. Prof. Böse hat mich einerseits in allen Abschnitten dieser Arbeit mit außerordentlich hilfreicher Kritik unterstützt und mich dabei andererseits meine ganz eigene Arbeit schreiben lassen.

Außerdem danke ich Herrn Prof. Dr. Torsten Verrel für das zügige Erstellen des Zweitgutachtens. Weiterhin gilt mein Dank Prof. Dr. Carl-Friedrich Stuckenberg, LL.M. (Harvard) für das sehr freundliche Prüfungsgespräch.

Auf dem Weg dieser Dissertation haben mich viele Menschen begleitet und in ihrer ganz eigenen Form dabei unterstützt, sie schlussendlich fertigzustellen. Ein besonderer Dank gilt dabei meiner Familie – Stefan, Barbara, Kathrin und Martin Koenen – und meiner Lebensgefährtin Anne Schlickenrieder. Sie alle hatten stets ein offenes Ohr, Anregungen und Kritik für diese Arbeit und haben es geschafft, mich auch in den schwierigen Phasen zu motivieren, an dieser Arbeit dranzubleiben.

Köln, im März 2023 *Michael Koenen*

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:34
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Inhaltsverzeichnis

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Abkürzungsverzeichnis

a.A.	Andere Ansicht
ACSAC '14	Proceedings of the 30th Annual Computer Security Applications Conference
Art.	Artikel
Auernhammer	*Esser, Martin/ Kramer, Philipp/ Lewinski, Kai* (Hrsg.): Auernhammer DSGVO BDSG, 7. Auflage, Köln 2020
Bd.	Band
BeckOK-DSR	*Brink, Stefan/ Wolff, Heinreich Amadeus* (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 38. Edition, München 2021
BeckOK-GG	*Epping, Volker/ Hillgruber, Christian* (Hrsg.): Beck'scher Online-Kommentar Grundgesetz, 49. Edition, München 2021
BeckOK-GwG	*Frey, Tobias/ Pelz, Christian* (Hrsg.): Beck'scher Online-Kommenrtar GwG, 7. Edition, München 2021
BeckOK-InfoMedienR	*Gersdorf, Hubertus/ Paal, Boris P.* (Hrsg.): Beck'scher Online-Kommentar Informations- und Medienrecht, 27. Edition, München 2020
BeckOK-StPO	*Graf, Jürgen* (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 41. Edition, München 2021
BGH	Bundesgerichtshof
BMF	Bundesministerium für Finanzen
BMWi	Bundesministerium für Wirtschaft und Energie
Breidenbach-Glatz RhdB-Legal-Tech	*Breidenbach, Stephan/ Glatz, Florian* (Hrsg.): Rechtshandbuch Legal Tech, 2. Auflage, München 2021
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CCZ	Corporate Compliance Zeitschrift
CR	Computer und Recht
DANA	Datenschutz Nachrichten
DÖV	Die Öffentliche Verwaltung

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dreier Bd. 1	*Dreier, Horst* (Hrsg.): Grundgesetz-Kommentar Band 1, 3. Auflage, Tübingen 2013
DStR	Deutsches Steuerrecht
DuD	Datenschutz und Datensicherheit
Dürig/Herzog/Scholz	*Herzog, Roman/ Herdegen, Matthias/ Scholz, Rupert/ Klein, Hans H.* (Hrsg.): Grundgesetz Kommentar begründet von Theodor Maunz und Günter Dürig, 95. Ergänzungslieferung, München 2021
Ehmann-Selmayr	*Ehmann, Eugen/ Selmayr, Martin* (Hrsg.): DS-GVO Datenschutzgrundverordnung Kommentar, 2. Auflage, München 2018
EuGH	Europäischer Gerichtshof
FC2013, LNCS 7859	*Sadeghi, Ahmad-Reza* (Hrsg.): Financial Cryptography and Data Security, 17th International Conference, FC2013, Revised Selected Papers, Lecture Notes in Computer Science, vol 7859, Berlin Heidelberg 2013
FC2014, LNCS 8437	*Christin, Nicolas/ Safavi, Reihaneh* (Hrsg.): Financial Cryptography and Data Security, 18th International Conference, FC2014, Revised Selected Papers, Lecture Notes in Computer Science, vol 8437, Berlin Heidelberg 2014
GA	Goltdammer's Archiv für Strafrecht
GCIG	Global Commission on Internet Governance
GDPR	General Data Protection Regulation
Gercke/Julius/Temming/ Zöller	*Gercke, Björn/ Julius, Karl-Peter/ Temming, Dieter/ Zöller, Mark A.* (Hrsg.): Strafprozessordnung, 6. Auflage, Heidelberg 2019
Ggf.	Gegebenenfalls
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
Hdb-StA	*Vordermayer, Helmut/ von Heintschel-Heinegg, Bernd/ Schnabl, Robert* (Hrsg.): Handbuch für den Staatsanwalt, 6. Auflage, Köln 2018
Herzog-GwG	*Herzog, Felix/ Achtelik, Olaf* (Hrsg.): Geldwäschegesetz (GwG), 4. Auflage, München 2020
HGR Bd. III	*Merten, Detlef/ Papier, Hans-Jürgen* (Hrsg.): Handbuch der Grundrechte in Deutschland und Europa, 1. Auflage, Heidelberg 2009
HGR Bd. IV	*Merten, Detlef/ Papier, Hans-Jürgen* (Hrsg.): Handbuch der Grundrechte in Deutschland und Europa, 1. Auflage, Heidelberg 2009

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

HICSS	Proceedings of the 51st Hawaii International Conference on System Sciences 2018
Hrsg.	Herausgeber
HStR Bd. V	*Isensee, Josef/ Kirchhof, Paul* (Hrsg.): Handbuch des Staatsrechts, Band V, 3. Auflage, Heidelberg 2003
ICITST	International Conference for Internet Technology and Secured Transactions
IEEE CST	IEEE Communications Surveys and Tutorials
IMC '13	IMC '13: Proceeding of the 2013 conference on Internet measurement Conference
i.S.d.	im Sinne des
ISSA	2016 Information Security for South Africa
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
JuS	Juristische Schulung
JZ	JuristenZeitung
Kap.	Kapitel
KMR-StPO	*Von Heintschel-Heinegg, Bernd/ Bockemühl, Jan* (Hrsg.): KMR – Kommentar zur Strafprozessordnung, Loseblattsammlung, Stand: 107. Ergänzungslieferung, Köln 2021
KriPoZ	Kriminalpolitische Zeitschrift
Kühling-Buchner	*Kühling, Jürgen/ Buchner, Benedikt* (Hrsg.): Datenschutz-Grundverordnung/BDSG Kommentar, 3. Auflage, München 2020
Löwe-Rosenberg	*Becker, Jörg-Peter/ Erb, Volker/ Esser, Robert/ Graalmann-Scheerer, Kirsten/ Hilger, Hans/ Ignor, Alexander* (Hrsg.): Löwe/Rosenberg Die Strafprozeßordnung und das Gerichtsverfassungsgesetz Großkommentar, 27. Auflage, Berlin 2018
m.w.N.	mit weiteren Nachweisen
Maume/Maute Kryptowerte HdB	*Maume, Philipp/ Maute, Lena/ Fromberger, Mathias* (Hrsg.): Rechtshandbuch Kryptowerte, 1. Auflage, München 2020
Meyer-Goßner/Schmitt	*Schmitt, Bertram/ Köhler, Marcus:* Meyer-Goßner/ Schmitt Strafprozessordnung, 64. Auflage, München 2021
MMR	Multimedia und Recht

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

MMR-Beil.	Multimedia und Recht, Beilage
MobiQuitous '19	MobiQuitous '19: Proceedings of 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2019
MüKo-StPO	*Knauer, Christoph/ Kudlich, Hans/ Schneider, Hartmut* (Hrsg.): Münchener Kommentar zur StPO, 1. Auflage, München 2014
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ	Neue Strafrechtszeitschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
NZKart	Neue Zeitschrift für Kartellrecht
NZWiSt	Neue Zeitschrift für Wirtschaftsstrafrecht
Paal-Pauly	*Paal, Boris P./ Pauly, Daniel A.* (Hrsg.): Beck'sche Kompakt-Kommentare Datenschutzgrundverordnung, 3. Auflage, München 2021
PCS	Procedia Computer Science
RFS	The Review of Financial Studies
RiS	Recht auf informationelle Selbstbestimmung
Rn.	Randnummer
Rücker-Kugler	*Rücker, Daniel/ Kugler, Tobias* (Hrsg.): New European General Data Protection Regulation, A Practitioners's Guide, 1. Auflage, München 2018
Sachs-GG	*Sachs, Michael* (Hrsg.): Grundgesetz Kommentar, 8 Auflage, München 2018
SHH-GG	*Schmidt-Bleibtreu, /Hofmann/Henneke* (Hrsg.): GG Grundgesetz, 14. Auflage, Köln 2017
Simitis-Hornung-Spieker	*Simitis, Spiros/ Hornung, Gerrit/ Spiecker genannt Döhmann, Indra* (Hrsg.): Datenschutzrecht, 1. Auflage, Baden-Baden 2019
SK-StPO	*Wolter, Jürgen* (Hrsg.): Systematischer Kommentar zur Strafprozessordnung, Mit GVG und EMRK, 5. Auflage, Köln 2016
Sog.	Sogenannte

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Specht/Mantz-HdB DSR	*Specht, Louisa/ Mantz, Reto* (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht, Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor
SPSN	*Altshuler, Yaniv/ Elovici, Yuval/ Cremers, Armin B./ Aharony, Nadav/ Pentland, Alex* (Hrsg.): Security and Privacy in Social Networks, New York, 2013
SSW-StPO	*Satzger, Helmut/ Schluckebier, Wilhelm* (Hrsg.): Satzger, Schluckebier, Widmaier Strafprozessordnung Mit GVG und EMRK Kommentar, 4. Auflage, Köln 2020
Stern-Becker-GG	*Stern, Klaus/ Becker, Florian* (Hrsg.): Grundrechte-Kommentar, 3. Auflage, Köln 2019
StV	Der Strafverteidiger
Sydow-DSGVO	*Sydow, Gernot* (Hrsg.): Europäische Datenschutzgrundverordnung Handkommentar, 2. Auflage, Baden-Baden 2018
WM	Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen
ZBB	Zeitschrift für Bankrecht und Bankwirtschaft
ZD	Zeitschrift für Datenschutz
ZGR	Zeitschrift für Gesellschaftsrecht
ZIS	Zeitschrift für internationale Strafrechtsdogmatik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Kapitel 1 – Einleitung

Die weltweite Finanzkrise ab 2007 hatte nicht nur drastische ökonomische Auswirkungen, sondern zog auch einen enormen Vertrauensverlust in staatliche Währungen nach sich. Vor diesem Hintergrund veröffentlichte *Satoshi Nakamoto* Ende 2008 sein White-Paper zur ersten praxistauglichen Kryptowährung Bitcoin.[1] Bitcoin sollte als erstes Zahlungsmittel unabhängig vom Vertrauen in (Zentral-)Banken funktionieren.

Mittlerweile ist Bitcoin die bekannteste Kryptowährung und die Kryptowährung mit der größten Marktkapitalisierung.[2] Bekannt ist sie aber auch wegen ihrer Verbindung zu illegalen Aktivitäten und als Spekulationsobjekt.

Technische Grundlage von Bitcoin ist die sog. *Blockchain*-Technologie, der in der öffentlichen Diskussion ein enormes Entwicklungspotenzial über die Anwendung bei Kryptowährungen hinaus zugeschrieben wird. So hat auch die Bundesregierung bereits im September 2019 eine Blockchain-Strategie vorgestellt, in der sie annimmt, dass die Blockchain-Technologie ein Baustein für das Internet der Zukunft ist.[3]

Eine wesentliche Eigenschaft der Blockchain-Technologie ist, dass die Daten, die durch sie verwaltet werden, in der Regel öffentlich verfügbar sind.[4] Dementsprechend ist es für Strafverfolgungsbehörden praktisch ohne weiteres möglich, diese Daten zu erheben und zu Strafverfolgungszwecken auszuwerten. Zwar kann auf Grund der dezentralen Datenverwaltung nicht unmittelbar ein Personenbezug hergestellt werden, jedoch bieten systematische Analysen der Transaktionsdaten Anhaltspunkte, um einerseits Straftaten aufzudecken und andererseits die jeweiligen Personen zu identifizieren.[5]

---

1 Hierzu im Einzelnen unter Kap. 2, A.I. Ausführlich zur Entstehungsgeschichte auch *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 28ff; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 6ff.

2 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz*, Kap. 4.1 Rn. 6, der als Wert der Marktkapitalisierung über hundert Milliarden US-Dollar angibt, in diesem Kontext aber auch angibt, dass dieser Wert auf Grund der hohen Volatilität von Bitcoin starken Schwankungen unterliegt.

3 *BMWi/BMF*, Blockchain-Strategie der Bundesregierung, S. 3.

4 Hierzu im Einzelnen unter Kap. 2, A.IV., B.IV.

5 Zu den einzelnen technischen Auswertungsmöglichkeiten ausführlich unter Kap. 3.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Aus rechtlicher Sicht stellt sich aber die Frage, ob diese Erhebungen und Auswertungen der Blockchain-Daten zulässig sind. Denn auch bei Daten, die in einer Blockchain enthalten und damit öffentlich verfügbar sind, kann ihre Erhebung und Auswertung einen Grundrechtseingriff darstellen. So entschied das BVerfG ebenfalls im Jahr 2008 in seinem Urteil zur Online-Durchsuchung des Verfassungsschutzgesetz Nordrhein-Westfalen, dass auch bei der Auswertung öffentlich verfügbarer Daten ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen könne. Dies sei der Fall, „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“[6].

Insoweit stellt sich die hier zu untersuchende Frage, ob der Einsatz von systematischen Auswertungsmethoden bei Blockchains zu Strafverfolgungszwecken grundsätzlich nach der bisher geltenden Rechtslage zulässig sein kann.

Um diese Frage zu untersuchen, wird nachfolgend zunächst in Kapitel 2 die technische Funktionsweise von Blockchains dargestellt und anschließend in Kapitel 3 auf die technische Funktionsweise von systematischen Auswertungsmethoden im Zusammenhang mit Blockchains eingegangen.

Nach dieser Betrachtung der tatsächlichen Gegebenheiten wird in Kapitel 4 untersucht, ob ein Eingriff in Grundrechte durch den Einsatz dieser Auswertungsmethoden vorliegt. Dabei kommt neben dem bereits angesprochenen Recht auf informationelle Selbstbestimmung das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, ebenfalls nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, in Betracht.

Da beim Vorliegen eines Grundrechtseingriffs eine verfassungsrechtliche Rechtfertigung erforderlich wäre, wird in Kapitel 5 untersucht, ob die StPO eine entsprechend ausreichende Ermittlungsbefugnis enthält, auf die die Auswertungsmethoden gestützt werden könnten.

Darüber hinaus wird in Kapitel 6 in einem kurzen Exkurs eine mögliche, datenschutzrechtliche Bewertung auf Grund der engen thematischen Nähe vorgenommen, um zu prüfen, ob sich aus dem Datenschutzrecht der DSGVO weitergehende Erkenntnisse für die hier gegenständliche Untersuchung ableiten lassen.

6 BVerfGE 120, 274, 345.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Schließlich werden in Kapitel 7 die wesentlichen Erkenntnisse dieser Untersuchung zusammengefasst.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Kapitel 2 – Die Blockchain-Technologie

Die Blockchain-Technologie ist eine neue Technologie zur Datenverwaltung, deren wesentliches Merkmal ist, dass Daten dezentral verwaltet werden. Erstmalig trat sie im Zusammenhang mit der virtuellen Kryptowährung Bitcoin in Erscheinung. Sie ist allerdings keinesfalls auf Kryptowährungen beschränkt, sondern kann zur Datenverwaltung insgesamt verwendet werden.

Zur Vereinfachung der komplizierten, technischen Darstellung wird im Folgenden zunächst die Blockchain-Technologie anhand des Bitcoin-Systems dargestellt (hierzu unter A.).

Daran anschließend wird die Blockchain-Technologie mit ihren Funktionen auf einer abstrakteren Ebene als Datenverwaltungsstruktur unabhängig vom Bitcoin-Kontext dargestellt (hierzu unter B.), um abschließend zu erörtern, welche weiteren Anwendungsmöglichkeiten es für die Blockchain-Technologie noch gibt (hierzu unter C.).

A. Die Blockchain-Technologie anhand des Bitcoin-Systems

Die Blockchain-Technologie kann als dezentrale Datenverwaltungsstruktur verstanden werden, die bei Bitcoin eingesetzt wird, um ein Register über die virtuelle Kryptowährung unabhängig von einem zentralen Intermediär dezentral zu führen.

Was das bedeutet, wird im Folgenden zunächst dadurch erläutert, dass der historische Hintergrund von Bitcoin dargestellt wird (hierzu unter I.). Daran anschließend wird dargestellt, wie Nutzer das Bitcoin-System verwenden können (hierzu unter II.). Abschließend wird erörtert, was die Blockchain-Technologie hierfür leisten muss und wie diese Anforderungen technisch erfüllt werden und ablaufen (hierzu unter III.).

I. Historischer Hintergrund von Bitcoin und Blockchain-Technologie

Ende 2008 veröffentlichte eine bisher unbekannte Person unter dem Pseudonym *Satoshi Nakamoto* die technische Abhandlung „Bitcoin: A Peer-to-

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Peer Electronic Cash System"[7]. Diese Abhandlung enthielt die technische Bauanleitung zur ersten praxistauglichen „virtuellen Kryptowährung"[8]. Zwar gab es auch schon vor Bitcoin Konzepte zur Entwicklung virtueller Kryptowährungen, diese konnten aber entweder praktisch gar nicht umgesetzt werden, oder enthielten noch derartige Umsetzungsschwierigkeiten, dass sie sich nicht durchsetzen konnten.[9]

Die Abhandlung von *Nakamoto* erschien im Zusammenhang mit der weltweiten Finanzkrise und kann als Antwort auf den Vertrauensverlust der Menschen in das weltweite Banken- und Finanzsystem verstanden werden.[10] So referenziert Bitcoin im sog. „Genesis-Block"[11] ihrer Blockchain[12] den Artikel einer britischen Tageszeitung mit dem Titel „Chancellor on Brink of Second Bailout for Banks".[13] Vor diesem historischen Hintergrund war es also Ziel von *Nakamoto* ein Zahlungsmittel zu schaffen, das losgelöst von staatlich regulierten Banken funktionieren sollte.[14] Anders als bei staatlich regulierten Finanz- und Währungssystemen soll bei Bitcoin die Integrität des Systems bzw. das Vertrauen in das System nicht durch eine staatliche Regulierung erreicht werden, sondern durch den Algorithmus des Systems selbst.[15] Diese Integrität liefert die Blockchain-Technologie.[16] Deshalb wird Bitcoin häufig als „Trustless Trust"[17] bezeichnet. Denn anders als konventionelle Buch- und E-Geld-Systeme generiert Bitcoin das

7 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 6; *Hofert*, Regulierung der Blockchains, S. 1.

8 Zur Einordnung des Begriffs ausführlich: *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 25ff.

9 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 7; Grzywotz, Virtuelle Kryptowährungen und Geldwäsche, S. 28 m.w.N. zu vorherigen Versuchen von virtuellen Währungen.

10 *Simmchen*, MMR 2017, 162 (162).

11 Der Genesis-Block ist der erste berechnete Datensatz im Bitcoin-Netzwerk, vgl. *Hofert*, Regulierung der Blockchains, S. 1.

12 Zur Vereinfachung kann der Begriff „Blockchain" zunächst als Datenbank verstanden werden. Ausführlich werden Inhalte und Funktionsweise der Blockchain unter A.II.7, III. dargestellt.

13 *Hofert*, Regulierung der Blockchains, S. 1 m.w.N.

14 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 6f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 28f.

15 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1; *Hofert*, Regulierung der Blockchains, S. 2.

16 *Hofert*, Regulierung der Blockchains, S. 2.

17 *Hofert*, Regulierung der Blockchains, S. 2 m.w.N.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Vertrauen der Nutzer lediglich durch seine technische Funktionsweise – ein Vertrauensverhältnis zwischen Kunden und Bank bzw. Bürger und Staat ist gerade nicht mehr erforderlich.[18] Dementsprechend ist der technische Ablauf der Blockchain besonders wichtig dafür, dass das Konzept von Bitcoin funktioniert.

II. Funktionsweise und Anwendung von Bitcoin für Nutzer – wie verwendet ein Nutzer Bitcoin?

Bitcoin soll als alternatives Zahlungsmittel fungieren, das für jeden Interessierten zugänglich ist (hierzu unter 1.). Die Nutzer agieren unter den Pseudonymen der *public keys* (hierzu unter 2.) bzw. den *Bitcoin-Adressen* (hierzu unter 3.).[19] Hierbei sind die *Bitcoin-Adressen* die Ergebnisse von Hashfunktionen der *public keys* (hierzu unter 4.).[20]

Anders als bei herkömmlichen Zahlungssystemen bestehen bei Bitcoin keine „Konten" als solches (hierzu unter 5.)[21], denn Bitcoin sind keine digitalen Geldmünzen, sondern lediglich Einträge von Wertzuweisungen in ein Register (hierzu unter 6.)[22]. Diese Wertzuweisungen können „übertragen" werden, indem die Wertzuweisung durch eine Transaktion verändert wird (hierzu unter 7.)[23]. Derartige Transaktionen werden in das Register des Systems, also in die Blockchain, eingetragen (hierzu unter 8.).[24]

18 So insbesondere *Hofert*, Regulierung der Blockchains, S. 2.
19 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Pesch/Böhme*, DuD 2017, 93 (93).
20 *Pesch/Böhme*, DuD 2017, 93 (93f.); *Börner*, NZWiSt 2018, 48 (48). Im Folgenden werden die Begriffe public key und Bitcoin-Adresse synonym verwendet, da die Differenzierung nur eine technische Besonderheit ist, die unter A.II.2. dargestellt wird.
21 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33f.
22 *Kütük/Sorge*, MMR 2014, 643 (643).
23 *Safferling/Rückert*, MMR 2015, 788 (790); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Kaulartz*, CR 2016, 474 (474ff.); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
24 *Pesch/Böhme*, DuD 2017, 93 (94).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

1. Keine Zugangsbeschränkung

Das Bitcoin-System ist als offenes Netzwerk[25] ausgestaltet, an dem sich jeder Interessierte beteiligen kann – unabhängig von Standort, Bankkonto oder Herkunft, erforderlich ist nur ein Internetzugang.[26] Um sich am Netzwerk zu beteiligen ist außerdem keinerlei Angabe von personenbezogenen Daten erforderlich.[27]

2. Private Key und Public Key

Zur Beteiligung muss sich der Interessierte ein Schlüsselpaar aus sog. *private key* und *public key* generieren lassen.[28] Hiermit können die Nutzer im Bitcoin-Netzwerk aktiv werden. Dabei dient der *public key* als eine Art Adresse bzw. Kontonummer[29] und der *private key* als eine Art Signatur und Authentifizierung von Transaktionen – vergleichbar mit der PIN einer EC- bzw. Kreditkarte oder der Unterschrift auf einem (Bar-) Scheck. [30]

Hintergrund von *private key* und *public key* ist das sog. asymmetrische Verschlüsselungsverfahren. Verständlich wird dieses Verschlüsselungsverfahren durch einen Vergleich zur symmetrischen Verschlüsselung. Bei der symmetrischen Verschlüsselung existiert nur ein einziger Schlüssel zum Verschlüsseln einer Nachricht – Absender und Empfänger müssen beide diesen Schlüssel kennen.[31] Hierdurch kann aber nicht gewährleistet werden, dass keine andere Person den Schlüssel kennt, bzw. der Empfänger kann nicht mit Sicherheit wissen, dass die Nachricht auch tatsächlich vom genannten Absender stammt.[32]

---

25 Im Folgenden meint der Begriff des (Bitcoin-)Netzwerkes das *Peer-to-Peer*-Netzwerk, in dem alle Nutzer des Bitcoin-Systems zusammengeschlossen sind. Siehe hierzu insbesondere die Ausführungen zum *Peer-to-Peer*-Netzwerk unter A.III.1.b).

26 *Boehm/Pesch*, MMR 2014, 75 (75); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 1f.; *Safferling/Rückert*, MMR 2015, 788 (793); *Kaulartz*, CR 2016, 474 (475).

27 *Boehm/Pesch*, MMR 2014, 75 (76).

28 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.

29 Der Vergleich mit einer Kontonummer ist ungenau (hierzu unter A.II.5), er soll hier nur zur Veranschaulichung dienen.

30 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 61; *Hofert*, Regulierung der Blockchains, S. 18. Auch dieser Vergleich ist stark vereinfacht und dient lediglich der Veranschaulichung.

31 *Kaulartz/Matzke*, NJW 2018, 3278 (3282).

32 *Kaulartz*, CR 2016, 474 (475); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (31f).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Im Fall von asymmetrischer Verschlüsselung gibt es dagegen zwei Schlüssel – bei Bitcoin den sog. *private key* und den sog. *public key*.[33]

Im Fall von Bitcoin wird zunächst der *private key* als eine zufällige alphanummerische Zahlenfolge erzeugt.[34] *Grzywotz* vergleicht die Funktion des *private keys* mit einem Schlüssel zu einem öffentlichen Briefkasten, in den jeder Nachrichten einwerfen, aber nur derjenige mit dem *private key* sie auch lesen kann.[35] Über diese Funktion des öffentlichen Briefkastens, den nur der Inhaber des *private keys* lesen kann, hinaus, dient der *private key* allerdings auch zum Verschlüsseln von Nachrichten bzw. wird durch die Verschlüsselung mit dem *private key* die Nachricht „signiert" (hierzu sogleich).[36]

Aus dem *private key* wird über eine rechnerische Funktion der *public key* erzeugt.[37] Der *public key* ist jedem Netzwerkteilnehmer bekannt. Er ist, wie der Name schon sagt, öffentlich.[38] Im oben dargestellten bildlichen Vergleich des öffentlichen Briefkastens, kann er als der Standort des Briefkastens verstanden werden, den der Absender von Nachrichten kennen muss, um sie an den Empfänger zu übermitteln.

Außerdem dient er zur Überprüfung der soeben erwähnten Signatur.[39] Wird eine Nachricht mit dem *private key* verschlüsselt, kann durch den dazugehörigen *public key* überprüft werden, ob sie auch tatsächlich mit dem zugehörigen *private key* verschlüsselt wurde.[40] Der Empfänger der Nachricht kann also überprüfen, ob der genannte Absender auch tatsächlich die Nachricht versendet hat – so kann der Absender seine Nachricht signieren.[41]

Das Schlüsselpaar aus *private key* und *public key* ist dabei zufällig generiert und lässt insgesamt keinerlei Rückschlüsse auf die Identität des dahinterstehenden Nutzers zu, insbesondere auch, da die Teilnahme am Netzwerk keinerlei Angabe von personenbezogenen Daten erfordert.[42]

---

33 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 2; *Kaulartz*, CR 2016, 474 (475); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.
34 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 64f.
35 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.
36 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32.
37 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32 m.w.N.
38 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.
39 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.
40 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.
41 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.
42 *Boehm/Pesch*, MMR 2014, 75 (76).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

3. Bitcoin Adresse – als Ergebnis einer Hashfunktion

Die *Bitcoin-Adresse* ist der sog. *Hashwert* des *public keys*. Er wird verwendet, um die Datenmenge im Bitcoin-System zu verringern.[43] Ein solcher *Hashwert* entsteht, wenn eine Ziffern- und Zahlenfolge (im Folgenden als „Zeichenfolge" bezeichnet) durch eine sog. *Hashfunktion* abgebildet wird.[44]

4. Hashfunktionen

Einfachstes Beispiel einer solchen *Hashfunktion* ist die Quersumme – die Quersumme von 17 ist 8, die Quersumme von 23 ist 5.[45] Ziel solcher Funktionen ist es, eine beliebig lange Zeichenfolge „durch eine kurze Zeichenfolge fester Länge"[46] darzustellen, um schnell abgleichen zu können, ob mehrere lange Zeichenfolgen gleich sind, denn wird auch nur ein Zeichen beim Eingabewert verändert[47], verändert sich der gesamte *Hashwert.*[48] Im Fall von langen Nachrichten[49] bzw. großen Datensätzen ermöglichen die *Hashfunktionen* also den schnellen Vergleich, ob etwas an der Nachricht verändert wurde.[50] Aus diesem Grund wird der *Hashwert* eines Datensatzes häufig auch als sein digitaler Fingerabdruck bezeichnet.[51]

Damit die Nachrichten im Bitcoin-System nicht zu lang werden, werden an verschiedenen Stellen *Hashfunktionen* eingesetzt, u.a. beim *public key* – konkret wird die Funktion SHA-256 verwendet, bei der eine Zeichenfolge

43 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33. Denn dadurch, dass mit jedem Weiterleiten einer Transaktion jeweils der *public key* des neuen Empfängers der Transaktion angehängt wird, verlängert sich die Datenmenge einer Transaktionsnachricht mit jeder Transaktion.

44 Im Bitcoin-System wird die Hashfunktion SHA-256 verwendet, *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 3. Die Zeichenfolge, die in die Hashfunktion eingegeben wird und aus der der Hashwert ermittelt wird, wird im Folgenden als „Eingabewert" bezeichnet.

45 *Kaulartz*, CR 2016, 474 (475).

46 *Kaulartz*, CR 2016, 474 (475).

47 Bzw. sogar die Veränderung von Groß- und Kleinschreibung im Eingabewert wirkt sich aus.

48 *Kaulartz*, CR 2016, 474 (475).

49 Gemeint sind hiermit die Transaktionsnachrichten, die die Nutzer an das Netzwerk aussenden.

50 *Kaulartz*, CR 2016, 474 (475).

51 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193; *Kaulartz*, CR 2016, 474 (475).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

mit einer Länge von 64 Zeichen erzeugt wird.[52] Entsprechend wird aus dem *public key* eine 64 Zeichen lange Zeichenfolge erzeugt – die *Bitcoin Adresse*. Sie kann am ehesten mit einer Kontonummer im herkömmlichen Banken- und Finanzsystem verglichen werden, denn an sie adressieren Nutzer ihre Zahlungen.[53]

Die SHA-256 *Hashfunktion* wird insbesondere auch bei der Verkettung der Datenblöcke der Blockchain eingesetzt und ermöglicht damit insbesondere ihre Fälschungssicherheit (hierzu im Einzelnen unter A.III.2.).

5. Konten

Anders als der Vergleich des *public keys* bzw. der *Bitcoin-Adresse* mit einer Kontonummer vermuten lässt, bestehen im Bitcoin-System keine „Konten" im Sinne des herkömmlichen Banken- und Finanzsystems.[54] Anbieter von sog. *Wallets* und anderen Diensten im Zusammenhang mit Bitcoin stellen für ihre Nutzer zwar eine derartige Saldenansicht bereit, diese beruht allerdings nur auf der eigenen Darstellung der Anbieter.[55] Im Bitcoin-System bzw. konkret in der *Blockchain* – gibt es dagegen keine Saldenansichten von Konten.

Denn bei Bitcoin gibt es lediglich sog. *unspent transaction outputs (=UTXO),* wörtlich übersetzt „nicht ausgegebene Transaktionen" bzw. „nicht weitergeleitete Transaktionen".[56] Denn das Bitcoin-Netzwerk lebt von sog. Transaktionen – vergleichbar mit herkömmlichen Überweisungen.[57] Der „Kontostand" eines Pseudonyms ergibt sich aus allen Transaktionen, die er empfangen, aber nicht ausgegeben hat – über die er also noch verfügen kann.[58]

52 *Kaulartz*, CR 2016, 474 (475); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33.
53 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33.
54 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Kaulartz*, CR 2016, 474 (475f.); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33f.
55 Auch andere Anbieter wie etwa blockchain.org stellen eine derartige Saldenansicht für alle Bitcoin-Adressen bereit.
56 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Kaulartz*, CR 2016, 474 (475).
57 *Kaulartz*, CR 2016, 474 (475).
58 *Kaulartz*, CR 2016, 474 (475f).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dies können einerseits Transaktionen sein, die darauf beruhen, dass das Pseudonym sie von einem anderen Pseudonym empfangen hat, oder auf dem sog. *Bitcoin-Mining* (vereinfacht = Bereitstellen von Rechenleistung zur Funktionsweise des Netzwerks)[59]. All diese Transaktionen des gesamten Netzwerks werden in chronologischer Reihenfolge in der Blockchain gespeichert.[60] Die Transaktionen eines bestimmten, einzelnen Pseudonyms können also über den gesamten Datenbestand der Blockchain verteilt sein.[61] Entsprechend kann eine Salden-Ansicht der „Konten" von einzelnen *public keys* nur abgeleitet werden, indem alle vorherigen Transaktionen ausgewertet werden.[62]

Da es also kein Konto als solches bzw. keine Saldenansicht gibt, wird bei einer Transaktion im Bitcoin-Netzwerk lediglich eine bereits empfangene Transaktion „weitergeleitet".[63]

Zu berücksichtigen ist in diesem Kontext, dass eine empfangene Transaktion nur als Ganzes weitergeleitet werden kann – ähnlich wie beim Bargeld, bei dem eine Münze bzw. ein Schein nur als Ganzes übergeben wird und der zu viel gezahlte Betrag als Wechselgeld herausgegeben wird.[64] In jeder Transaktionsnachricht muss deshalb bereits enthalten sein, an welche *Bitcoin-Adresse* das „Wechselgeld" transferiert werden soll, da es sonst als Transaktionsgebühr eingezogen wird.[65]

6. Bitcoin

Anders als der Begriff „Bitcoin" suggeriert, gibt es keine derartige „digitale Geldmünze".[66] Denn bei digitalen Gütern besteht immer das Problem, dass sie nicht rivalisierend sind.[67] Das bedeutet, dass digitale Güter, anders als materielle Güter, gleichzeitig von verschiedenen Nutzern ge- und

59 Das *Bitcoin-Mining* wird ausführlich unter A.III.1.c) beschrieben.
60 *Martini/Weinzierl*, NVwZ 2017, 1251 (1251); *Schrey/Thalhofer*, NJW 2017, 1431 (1431).
61 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114.
62 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114.
63 *Kaulartz*, CR 2016, 474 (475f).
64 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
65 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
66 *Kütük/Sorge*, MMR 2014, 643 (643).
67 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz*, Kap. 4.1 Rn. 8; *Kütük/Sorge*, MMR 2014, 643 (643); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754). Der Begriff „rivalisierend" wird hier nicht im ökonomischen Sinne verwendet, sondern bedeutet lediglich, dass die Nutzung eines Gutes die Nutzungsmöglichkeit eines anderen nicht ausschließt.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

verbraucht werden können, ohne, dass dadurch die Nutzungsmöglichkeit Anderer eingeschränkt wird.[68]

Was bereits seit Jahren ein Problem der Film- und Musikindustrie ist, würde genauso bei virtuellem Geld auftreten, wenn die virtuellen Geldmünzen einfach kopiert werden könnten.[69] Deshalb ist ein Bitcoin kein bestimmtes, digital kopierbares „Datum", sondern ein Bitcoin ist die Zuschreibung eines Wertes zu einem Pseudonym.[70] Diese Zuweisung erfolgt durch Transaktion an einen *public key*. Ein Bitcoin wird also transferiert bzw. überwiesen, indem die Zuweisung einer Transaktion zu einem Pseudonym verändert wird.[71]

Zu beachten ist, dass ein Bitcoin bis zu acht Nachkommastellen geteilt werden kann – ähnlich einem Euro, der auch bis zu zwei Nachkommastellen geteilt werden kann (Cents).[72] Die kleinste Einheit von Bitcoin heißt *Satoshi*.[73]

7. Transaktionen

Um eine Transaktion im Bitcoin-System auszuführen, muss also die Zuweisung einer noch nicht weitergeleiteten Transaktion verändert werden.[74]

a) „Transaktion 01"

Hierzu erstellt der Bitcoin-Nutzer die Nachricht an das Netzwerk, dass eine ursprünglich seinem *public key* zugewiesene Transaktion an einen anderen *public key* weitergeleitet werden soll.[75] Diese Nachricht verschlüsselt der Absender mit seinem *private key*.[76]

---

68 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8f.
69 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8.
70 *Safferling/Rückert*, MMR 2015, 788 (790); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
71 So bezeichnen bereits *Safferling/Rückert*, MMR 2015, 788 (789)„Bitcoin als Kette digitaler Signaturen".
72 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
73 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
74 *Kaulartz*, CR 2016, 474 (476); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
75 *Kaulartz*, CR 2016, 474 (475f.).
76 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Hiermit signiert er sie und weist gegenüber dem Netzwerk nach, dass er dazu berechtigt ist, Transaktionen weiterzuleiten, die dem zugehörigen *public key* zugewiesen ist[77] – vereinfacht: er weist nach, dass er über den *public key* verfügen kann.[78] In der Nachricht enthalten ist auch der *public key* des Empfängers.[79]

Das Netzwerk nimmt diese Nachricht zur Kenntnis, überprüft sie und bestätigt sie, sodass nun die Transaktion dem *public key* des Empfängers zugewiesen ist.[80]

b) „Transaktion 02"

Will nun der Empfänger der Transaktion 01, die Transkation weiterleiten, muss auch er eine derartige Nachricht an das Netzwerk versenden und einen neuen Empfänger als *public key* definieren.[81] Ebenfalls muss er nun die Nachricht mit seinem *private key* signieren. Das Netzwerk kann so überprüfen, ob Absender der Transkation 02 auch tatsächlich der Empfänger der Transkation 01 ist.[82]

c) Gültigkeit einer Transaktion

Eine Transaktion gilt allerdings erst als erfolgt, wenn sie in die Blockchain aufgenommen wurde – vereinfacht bedeutet das, dass sie als gültig von den anderen Nutzern bestätigt wurde.[83]

8. Blockchain

Um die Gültigkeit einer Transaktion zu überprüfen, muss das Bitcoin-Netzwerk einerseits die Berechtigung mittels *public key* und *private key* überprüfen und andererseits überprüfen, ob die gegenständliche Transaktion

77 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
78 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 63.
79 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
80 Zum Ablauf dieser Bestätigung innerhalb des Netzwerkes unter A.III.1.c).
81 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
82 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
83 Im Einzelnen hierzu unter A.III.1.c).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nicht bereits zuvor anderweitig ausgegeben bzw. weitergeleitet wurde (sog. *double spending*).[84]

Hierzu dient die Blockchain (wörtlich übersetzt als „Blockkette") als „zentrales"[85], chronologisches Transaktionsregister, in das alle Transaktionen aller Nutzer fortlaufend eingetragen werden.[86] Die Blockchain ist insoweit vergleichbar mit einem Kontobuch, das alle Transaktionen aller Kunden einer Bank aufzeichnet.[87] Da der Begriff des „Kontobuchs" allerdings widersprüchlich zu den fehlenden Konten[88] ist, wird im Folgenden der von *Grzywotz* verwendete Begriff des „Hauptbuchs" verwendet.[89]

Anhand dieses vom Netzwerk erzeugten Hauptbuchs können die Nutzer abgleichen, ob die Transaktion, die weitergeleitet werden soll, nicht bereits zuvor ausgegeben bzw. weitergeleitet wurde.[90]

III. Funktionsweise der Blockchain-Technologie – wie wird die Blockchain fortgeschrieben?

Der besondere technologische Fortschritt der Blockchain-Technologie liegt darin, wie dieses Hauptbuch erzeugt wird. Denn das Hauptbuch wird – anders als im herkömmlichen Bankensystem – von allen Nutzern gemeinsam fortgeschrieben, anstatt von einer zentralen Verwaltungsinstanz.[91]

Im herkömmlichen Banken- und Finanzsystem führt jede Bank ein solches Hauptbuch für ihre Nutzer[92] – also ein zentraler Intermediär.[93]

---

84 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1f.; *Safferling/Rückert*, MMR 2015, 788 (790); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 25ff.

85 „Zentral" meint in diesem Kontext, nicht die Form der Datenverwaltung, sondern stellt darauf ab, dass die Blockchain als Transaktionsregister die Grundlage der Überprüfung von Transaktionen ist.

86 *Martini/Weinzierl*, NVwZ 2017, 1251 (1251); *Schrey/Thalhofer*, NJW 2017, 1431 (1432).

87 *Börner*, NZWiSt 2018, 48 (49).

88 Siehe oben unter B.II.3.

89 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 41.

90 *Safferling/Rückert*, MMR 2015, 788 (790); *Kaulartz*, CR 2016, 474 (476).

91 *Safferling/Rückert*, MMR 2015, 788 (789f.).

92 *Kaulartz*, CR 2016, 474 (476). Im Folgenden wird der Begriff „Nutzer" synonym zum Begriff „Kunde" verwendet, auch um den Vergleich zwischen Bitcoin und herkömmlichen Zahlungsverkehr zu unterstreichen.

93 *Hofert*, Regulierung der Blockchains, S. 18; Breidenbach-Glatz RhdB-Legal-Tech/*Sandner/Voigt/Fries,* Kap. 5.4 Rn. 15f. S. 150f.; *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2254f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Die Bank überprüft vor einer Überweisung, ob der Überweisende bzw. Absender[94] das überwiesene Vermögen überhaupt hat und führt nach der Überweisung sein Konto mit einem entsprechenden Eintrag fort.[95]

Ziel von Bitcoin war es aber gerade, die zentrale Verwaltung von „Konten" zu vermeiden und die Verwaltung dezentral zu ermöglichen.[96] Allerdings müssen die (Verwaltungs-)Aufgaben, die sonst Banken bzw. zentrale Intermediäre übernehmen, auch bei einer dezentralen Verwaltungsstruktur gewährleistet werden.[97] Dies ermöglicht die Blockchain-Technologie. Mit diesem Instrument schreiben alle Nutzer das gemeinsame Hauptbuch fort.[98]

Dazu muss die Blockchain-Technologie folgende zwei Funktionen erfüllen:

1. Alle Nutzer des Bitcoin-Systems müssen einen Konsens über den Inhalt des Hauptbuchs bzw. seine Fortschreibung erreichen (hierzu unter 1.).
2. Das Hauptbuch bzw. die Blockchain muss fälschungssicher sein – darf also nicht durch einen Angriff von außen verändert werden können (hierzu unter 2.).

1. Konsensmechanismus – Governance

a) Konnektivität durch Internet und Peer-to-Peer-Netzwerk

Um einen Konsens der Nutzer zu erreichen, müssen die Nutzer zunächst miteinander kommunizieren. Die Kommunikation der Bitcoin-Nutzer erfolgt über das Internet. Das Internet stellt als Netzwerkprotokoll die Konnektivität aller Nutzer sicher.[99]

94 Im Folgenden wird der Begriff „Absender" synonym zum Begriff des „Überweisenden" verwendet, auch um den Vergleich zwischen Bitcoin und herkömmlichem Zahlungsverkehr zu unterstreichen.
95 *Kaulartz*, CR 2016, 474 (476).
96 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1f.; *Kaulartz*, CR 2016, 474 (476).
97 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 40f.
98 *Hofert*, Regulierung der Blockchains, S. 21.
99 *Böhme/Pesch*, DuD 2017, 473 (475); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Durch das Internet werden alle Nutzer, die die Bitcoin-Software[100] nutzen, zu einem sog. *Peer-to-Peer-Netzwerk* zusammengeschlossen.[101] Das *Peer-to-Peer-Netzwerk* ist ein Netzwerkprotokoll, das ein dezentrales Kommunikationsnetzwerk erzeugt.[102] Die Kommunikation der Netzwerkteilnehmer findet hier unmittelbar – also direkt – zwischen den einzelnen Nutzern, ohne den Umweg über einen zentralen Knotenpunkt statt – deshalb werden die Nutzer auch als *nodes* (=Knoten) bezeichnet.[103] Regelmäßig findet Kommunikation im Internet nämlich über zentrale Diensteanbieter und deren Server statt – wie etwa bei Facebook, WhatsApp oder auch beim E-Mail-Postfach bei einem E-Mail-Diensteanbieter. Bei einem *Peer-to-Peer*-Netzwerk werden die Nutzer unmittelbar, ohne den Umweg über den Server eines Dritten, zusammengeschlossen – deshalb ist auch jeder Beteiligte Rechner selbst Server.[104]

Bildlich ausgedrückt gleicht das *Peer-to-Peer*-Netzwerk also einem persönlichen Gespräch in Abgrenzung zu einem Telefonat – die Kommunikation findet beim persönlichen Gespräch unmittelbar zwischen den Teilnehmern des Gesprächs statt, beim Telefonat dagegen wird die Kommunikation zwischen den Gesprächsteilnehmern vom Telefonanbieter vermittelt.

Wichtig ist in diesem Zusammenhang, dass die Teilnehmer eines *Peer-to-Peer*-Netzwerks gleichberechtigte Nutzer des Netzwerks sind, also alle den gleichen Einfluss auf das Netzwerk haben.[105]

b) Nodes im Peer-to-Peer Netzwerk – wer schreibt die Blockchain fort?

Jeder dieser *nodes* hält fortlaufend die gesamte Blockchain auf seinem lokalen Rechner vor und hält sie auf dem aktuellen Stand.[106] Hierzu steht

100 Zur Differenzierung der verschiedenen Bitcoin-Software sogleich unter A.III.1.b).
101 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12.
102 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12; *Hofert*, Regulierung der Blockchains, S. 17.
103 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Hofert*, Regulierung der Blockchains, S. 17.
104 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 139.
105 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 139; *Hofert*, Regulierung der Blockchains, S. 17.
106 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17ff.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

er im ständigen Austausch mit den anderen *nodes* im Netzwerk, um den aktuellen Stand abzugleichen.[107]

Bei Bitcoin ist zwischen drei verschiedene Varianten von *nodes* zu differenzieren[108]:

i. Sog. *Full-Node* als umfassendstes Endnutzerprogramm. Der Full-Node speichert fortlaufend die gesamte Blockchain, kann selbst im Netzwerk mit einer *Bitcoin-Adresse* bzw. *public key* agieren und schreibt die Blockchain fort.[109]
ii. Sog. *Solo-Miner*, die die Blockchain fortschreiben und sie fortlaufend lokal speichern, aber selbst nicht im Netzwerk mit einer *Bitcoin-Adresse* aktiv werden können.[110]
iii. Sog. *Full-Blockchain-Nodes,* die die gesamte Blockchain zwar fortlaufend lokal vorhalten, sie aber weder selbst fortschreiben oder mit einer *Bitcoin-Adresse* aktiv werden können, sondern lediglich „gültige Blöcke an andere Knoten weiterleiten".[111]

Die ersten beiden Varianten schreiben selbst die Blockchain fort, sie sind sog. *miner.*[112] Begrifflich wird deshalb zwischen *minern* und *nodes* differenziert. *Nodes* sind diejenigen Netzwerkteilnehmer, die sich an der Kommunikation im Netzwerk beteiligen – also alle der drei genannten. *Miner* sind dagegen nur solche *nodes* die selbst die Blockchain fortschreiben.

c) Fortschreiben der Blockchain bzw. Bitcoin-Mining – wie wird die Blockchain fortgeschrieben?

Wenn eine Transaktion erfolgen soll, erstellt der Nutzer eine entsprechende Nachricht und sendet diese an die *nodes*.[113] Die *miner* überprüfen diese

107 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17ff.
108 Hierzu ausführlich *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
109 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 140f.
110 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 140f.
111 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche; ausführlich hierzu *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 149ff.
112 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 4; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
113 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43. Siehe auch oben unter A.II.7.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Nachricht und leiten sie an weitere *nodes* weiter.[114] Die Transaktionsnachricht gelangt durch ständiges Weiterleiten der *nodes* an andere *nodes* ins Netzwerk.

Daraufhin gelangt die Nachricht in den sog. *memory-pool*.[115] Im *memory-pool* befinden sich alle Transaktionsnachrichten aller Nutzer, die noch nicht in die Blockchain aufgenommen wurden und aus denen sich die *miner* beim Erstellen eines neuen Blocks bedienen können.

Die *miner* entnehmen diesem *memory-pool* geeignete[116] Transaktionsnachrichten und berechnen hieraus einen neuen sog. *candidate-block*.[117]

(1) Überprüfung der Transaktionen – Verhinderung von „Double Spending"

Geeignet sind dabei nur solche Transaktionsnachrichten, die spezifische Kriterien einer Checkliste erfüllen.[118] Zu diesen Kriterien gehört u.a. auch, dass die Transaktion sich nicht bereits mit einem anderen Empfänger im *memory-pool* befindet (*double spending*) – dann wird sie nicht in den *candidate-block* aufgenommen.[119] Außerdem darf sie nicht der bisherigen Transaktionshistorie widersprechen – konkret: die weitergeleitete Transaktion darf nicht bereits zuvor vom gleichen Absender an einen anderen Empfänger weitergeleitet worden sein.[120]

Hierdurch wird gewährleistet, dass nur „gültige" Transaktionen in die Blockchain aufgenommen werden und das Problem des *double spending* wird hierdurch gelöst.[121]

114 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
115 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
116 Die miner können aus den Transaktionsnachrichten auswählen, abhängig von der Höhe der Transaktion, der Höhe der Transaktionsgebühr und der Länge der Wartezeit, *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43f.
117 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
118 Siehe zur genauen Darstellung dieser Checkliste *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182f.
119 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182.
120 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 183.
121 Siehe ausführlich hierzu: *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 49f.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(2) Proof-of-Work

Der *miner* muss dem *candidate-block* außerdem noch den sog. *Proof-of-Work*[122] beifügen – ein Nachweis darüber, dass er Rechenleistung für die Berechnung des Blocks aufgewendet hat.[123] Dies erfolgt wiederum durch eine *Hashfunktion*[124]. Allerdings muss diesmal nicht der *Hashwert* eines Eingabewertes durch die *Hashfunktion* berechnet werden, sondern der *miner* muss den *Hashwert* des *candidate-blocks* berechnen und dabei zu einem bestimmten, vom System vorgegebenen Ergebnis gelangen – bspw. muss die erste Ziffer des *Hashwerts* des *candidate-blocks* 0 sein.[125] Da sich aber bei *Hashfunktionen* der *Hashwert* vollständig verändert, wenn sich der Eingabewert nur um ein Zeichen verändert, kann dieses Ziel nur durch ausprobieren erreicht werden.[126] Der *miner* muss also den Inhalt des *candidate-blocks* anpassen – regelmäßig wird er immer eine weitere Transaktion hinzufügen. Dabei muss er jedes Mal den *Hashwert* neuberechnen, bis er den vorgegebenen Zielwert erreicht – je nachdem, wie genau das zu erzielende Ergebnis vorgegeben ist, ist diese Rechenoperation sehr aufwändig.[127] Findet der *miner* einen *candidate-block*, der den vorgegebenen *Hashwert* erreicht, kann das Netzwerk einfach überprüfen, ob die Berechnung richtig ist, denn hierfür muss nur berechnet werden, ob der vom *miner* gefundene Block tatsächlich den vorgegebenen *Hashwert* ergibt.

Insoweit ist der Rechenprozess, um einen *Proof-of-Work* zu finden, für den *miner* sehr aufwändig, kann aber vom Netzwerk durch eine einzige Rechenoperation überprüft werden.[128] So können die anderen *nodes* sicher-

122 Das sog. *Proof-of-Work*-Verfahren wird bei Bitcoin verwendet, ein anderes Verfahren ist das sog. *Proof-of-Stake*-Verfahren, hierzu sogleich.

123 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 3; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 44.

124 Zur Funktionsweise einer Hashfunktion siehe oben unter A.II.4.

125 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Hofert*, Regulierung der Blockchains, S. 20f.

126 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Kaulartz*, CR 2016, 474 (475); *Hofert*, Regulierung der Blockchains, S. 20f.

127 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 195; *Hofert*, Regulierung der Blockchains, S. 20f.

128 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

stellen, dass der *miner*, der den Block gefunden hat, auch entsprechende Rechenleistung aufgewendet hat.[129]

d) Konsens über Gültigkeit der längsten Kette

Der so gefundene Block wird im Anschluss mit dem entsprechend berechneten *Hashwert* an die anderen *nodes* im Netzwerk verteilt und hierdurch an die Blockchain angehängt. Dabei beinhaltet ein neuer Block auch immer den *Hashwert* des vorhergehenden Blocks. So entsteht eine Kette aus Datenblöcken (= „Blockchain").

Da aber die *miner* die Blockchain gleichzeitig fortschreiben, besteht das Problem, dass sie sich einigen müssen, wer nun die „richtige" bzw. gültige Kette berechnet hat. Von den anderen *minern* wird deshalb nur die längste Kette als die gültige Kette anerkannt.[130] Dass eine Kette als die gültige anerkannt wird, kommuniziert nun der weitere *miner* dadurch, dass er sie als Ausgangspunkt für seine weitere Kette annimmt und diese dann wiederum an das Netzwerk kommuniziert.[131]

e) Exkurs – Andere Konsensmechanismen

Problematisch ist das *Proof-of-Work*-Verfahren u.a., weil es sehr rechenintensiv ist und damit auch einen sehr hohen Energieverbrauch hat – insbesondere da der Rechenaufwand immer höher wird.[132] Aus diesen Gründen werden verschiedene alternative Konsensverfahren diskutiert – insbesondere der sog. *„Proof-of-Stake"* und der sog. *„Proof-of-Authority"*.[133]

Bei dem *Proof-of-Stake*-Verfahren wird im Wesentlichen die erforderliche Rechenkraft durch die Währung der jeweiligen Blockchain-Netzwerke

129 *Kütük/Sorge*, MMR 2014, 643 (643).
130 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 45; *Hofert*, Regulierung der Blockchains, S. 19.
131 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 45; *Hofert*, Regulierung der Blockchains, S. 17f.
132 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 33; *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2100f.).
133 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 34; *Janicki/Saive*, ZD 2019, 251 (251f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

selbst ersetzt.[134] Die *miner* müssen ihre jeweiligen Werteinheiten einsetzen, um einen neuen Block zu finden, je höher dabei der Einsatz, desto höher ist auch die Wahrscheinlichkeit, dass sie einen neuen Block finden.[135]

Eine andere Alternative ist das sog. *Proof-of-Authority*, bei dem die *miner* vom System auf Grund eines überprüften Vertrauens dazu autorisiert werden, die Blockchain fortzuschreiben.[136]

Beide Alternativen sehen sich allerdings der Kritik ausgesetzt, dass hierdurch der ursprüngliche Gedanke einer dezentralisierten Währung verfehlt wird.[137]

2. Unveränderlichkeit der Blockchain

Damit die *miner* die zu validierende Transaktion verifizieren können – insbesondere abgleichen können, ob die zu bestätigende Transaktion bereits vormals an einen anderen Absender transferiert wurde (*double spending*) – muss die Blockchain eine vollständige Historie aller bisher getätigten Transaktionen enthalten und diese Transaktionshistorie muss fälschungssicher bzw. unveränderlich sein.[138]

Dabei wird die erforderliche Unveränderlichkeit durch eine „Verkettung" der Datenblöcke erreicht.[139] Die Verkettung wird – wie oben bereits kurz beschrieben – dadurch gewährleistet, dass jeder neue Block den *Hashwert* des vorhergehenden Blocks referenziert.[140] Insoweit wird die Verkettung der Blockchain als Weiterentwicklung verketteter Listen beschrieben.[141]

Denn von einer einfach verketteten Liste spricht man, wenn in einer Datenstruktur jeder neue Block auf „die Adresse der ersten Speicherzelle des vorhergehenden Elements" verweist.[142] In diesem Fall können Elemente

134 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 34.
135 *King/Nadal*, PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, S. 2; *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2102).
136 *Janicki/Saive*, ZD 2019, 251 (251f).
137 *Schlund/Pongratz*, DStR 2018, 598 (599).
138 *Schrey/Thalhofer*, NJW 2017, 1431 (1432); *Martini/Weinzierl*, NVwZ 2017, 1251 (1255); *Hofert*, Regulierung der Blockchains, S. 21.
139 *Hofert*, Regulierung der Blockchains, S. 21.
140 *Hofert*, Regulierung der Blockchains, S. 19f; *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2257).
141 *Böhme/Pesch*, DuD 2017, 473 (474).
142 *Böhme/Pesch*, DuD 2017, 473 (474).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

der Speicherkette aber einfach ausgetauscht werden und durch Änderung lediglich eines Elements verändert bzw. eingefügt oder gelöscht werden.[143]

Eine schwieriger zu verändernde Datenstruktur erhält man, wenn der neue Block in einer Datenstruktur auf den *Hashwert* eines vorhergehenden Speicherelements verweist.[144] In diesem Fall müssen die gesamten *Hashwerte* neu berechnet werde, die dem veränderten Element nachfolgen.[145] Entsprechend aufwändiger ist die Veränderung der Datenstruktur.

Die Technologie der Blockchain geht hierüber noch hinaus. Denn, wenn ein Element eines Blocks verändert werden soll, müssen nicht nur die *Hashwerte* neu berechnet werden, sondern es muss jeweils ein bestimmter neuer *Hashwert* eines nachfolgenden Blocks, entsprechend dem oben[146] beschriebenen Verfahren, gefunden werden.[147] Möchte ein Angreifer also den Inhalt der Blockchain nachträglich verändern, müsste er mehr Rechenkapazität aufwenden als alle Rechner, die die Blockchain zuvor berechnet haben – sog. 51%-Angriff.[148]

Dass ein solcher Angriff äußerst unwahrscheinlich ist, beruht auf dem Grundgedanken, dass mit der so aufgewendeten Rechenkapazität wirtschaftlich sinnvoller neue Blocks berechnet werden könnten und damit auf dem von *John F. Nash* entwickelten spieltheoretischen Prinzip des sog. *Nashgleichgewichts*.[149] Denn den *minern* des Bitcoin-Systems wird ein „pekuniärer Anreiz" geboten.[150] Sie erhalten für die Berechnung neuer Blöcke einerseits die Transaktionsgebühren der neuberechneten Blöcke und andererseits werden mit jedem neuen, gültigen Block, der an die Blockchain angehängt wird, neue Bitcoin geschaffen, die demjenigen, der den neuen Block berechnet hat, gutgeschrieben werden.[151]

143 *Böhme/Pesch*, DuD 2017, 473 (474).
144 *Böhme/Pesch*, DuD 2017, 473 (474).
145 *Böhme/Pesch*, DuD 2017, 473 (474).
146 Siehe hierzu unter A.III.1.c)(2).
147 *Hofert*, Regulierung der Blockchains, S. 21.
148 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 2; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Böhme/Pesch*, DuD 2017, 473 (95); *Hofert*, Regulierung der Blockchains, S. 21.
149 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 27.
150 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46f.; *Hofert*, Regulierung der Blockchains, S. 22.
151 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 47; *Hofert*, Regulierung der Blockchains, S. 22.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

So gewährleistet das Bitcoin-System, dass es wirtschaftlich sinnlos ist, die Blockchain nachträglich zu verändern, sodass es eine fälschungssichere Transaktionshistorie gibt.[152]

IV. Öffentliche Verfügbarkeit der Blockchain-Daten als Folge dieser Funktionsweise der Blockchain-Technologie

Aus diesem Verfahren der Konsensfindung zwischen allen Beteiligten Nutzern ergibt sich mittelbar, dass alle Transaktionsdaten öffentlich verfügbar sein müssen, soweit ein öffentliches Blockchain-Netzwerk verwendet wird.[153]

Denn Kerngedanke der Blockchain-Technologie ist eine Datenverwaltungsstruktur, für die kein Vertrauen in eine zentrale Instanz notwendig ist. Stattdessen soll die Funktion der Währung dadurch gewährleistet werden, dass alle Beteiligten gleichberechtigt die Verwaltungsaufgaben des Systems übernehmen.[154] Entsprechend kontrolliert nicht eine zentrale Verwaltungsinstanz die Gültigkeit der Transaktionen, sondern das Kollektiv der Nutzer selbst überprüft dies.[155] Das setzt allerdings auch voraus, dass alle Nutzer die notwendigen Informationen haben müssen, um die Transaktionen zu kontrollieren. Entsprechend muss die Transaktionshistorie, anhand derer der Abgleich vorgenommen wird, allen Nutzern zur Verfügung stehen.[156]

Da bisher die virtuellen Kryptowährungen gerade nicht zugangsbeschränkt sind und sich jeder Interessierte sowohl am Handel wie auch am *mining* beteiligen kann, sind die Daten der Transaktionshistorie entsprechend transparent und damit auch öffentlich verfügbar.[157]

V. Zwischenergebnis

Vorstehend wurde dargestellt, wie Bitcoin und die dahinterstehende Blockchain-Technologie funktionieren. Hieraus ist Folgendes festzuhalten:

152 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 27.
153 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6; *Safferling/Rückert*, MMR 2015, 788 (793); *Pesch/Böhme*, DuD 2017, 93 (94).
154 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 20ff.
155 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 20f.
156 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 40f.
157 *Safferling/Rückert*, MMR 2015, 788 (793); *Pesch/Böhme*, DuD 2017, 93 (93).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Nutzer des Bitcoin-Systems können im Netzwerk mit sog. *private* und *public key* aktiv werden und sog. Bitcoin transferieren. Eine Transaktion bedeutet, dass die Zuweisung eines Wertes zu einem *public key* verändert wird. Solche Veränderungen der Wertzuweisungen werden in die sog. Blockchain eingetragen – das Hauptbuch des Bitcoin-Systems. Der Eintragungsprozess erfolgt dabei durch alle Nutzer gemeinsam und setzt insoweit voraus, dass sich alle Nutzer auf einen entsprechenden Konsens einigen. Dieser Konsens wird dadurch erreicht, dass nur die längste Blockchain fortgeschrieben wird, denn für sie wurde bisher am meisten Rechenleistung aufgewendet. Eingetragen werden außerdem nur Transaktionen, die der vorhergehenden Transaktionshistorie nicht widersprechen bzw. die einer noch einzutragenden Transaktion nicht widersprechen. Da die Bitcoin-Blockchain als offenes Netzwerk ausgestaltet ist, an dem sich jeder beteiligen kann, sind die Transaktionsdaten in der Blockchain auch für jeden Nutzer verfügbar und damit insgesamt öffentlich verfügbar.

B. Die Blockchain-Technologie außerhalb des Bitcoin- und Kryptowährungskontextes

Auch wenn die Blockchain-Technologie am Anwendungsbeispiel von Bitcoin erklärt wurde, ist sie gerade nicht auf die Verwaltung von Kryptowährungen beschränkt – ihr Anwendungsbereich ist sehr viel umfassender.[158]

I. Nicht die „eine" Blockchain

So ist für das Verständnis zunächst wichtig, dass es nicht die „eine" Blockchain gibt, sondern die oben im Zusammenhang mit Bitcoin dargestellte Technologie kann auf beliebige andere Vorgänge angewendet werden.[159] Hierzu muss der Programmcode der Blockchain natürlich entsprechend angepasst werden. Das „Grundkonzept" bleibt aber gleich. Denn die Blockchain-Technologie zeichnet sich durch:

158 *Kaulartz*, CR 2016, 474 (474); *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Simmchen*, MMR 2017, 162 (162f.).

159 *Kaulartz*, CR 2016, 474 (474); *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

– einen Zusammenschluss gleichberechtigter Rechner zu einem Netzwerk aus,
– die auf der Grundlage eines vorher festgelegten Netzwerkprotokolls
– eine gemeinsame, verteilte Datenbank (die Blockchain) fortschreiben,
– indem sie sich in einem vorher festgelegten Verfahren auf einen Konsens der fortzuschreibenden Daten einigen.[160]

II. Transaktions- und Dokumentationsfunktion

Aus dem Bitcoin-Kontext werden aber bereits die beiden wesentlichen Funktionen der Blockchain-Technologie ersichtlich: einerseits eine Transaktionsfunktion und andererseits eine Dokumentationsfunktion.[161]

1. Transaktionsfunktion

Im Bitcoin-System dient die Blockchain-Technologie zur Führung des dezentral geführten Transaktionsregisters.[162] Dabei führt sie selbst Transaktionen aus, indem sie die Zuweisung von Werten dadurch verändert, dass das Transaktionsregister entsprechend fortgeschrieben wird.[163] Bei Bitcoin und anderen virtuellen Kryptowährungen werden hierdurch die jeweiligen Werteinheiten transferiert.[164]

Anders als im Fall von Bitcoin und anderen virtuellen Kryptowährungen, muss sich die Transaktionsfunktion der Blockchain-Technologie aber nicht auf die Transaktion der jeweiligen Werteinheiten beschränken, sondern die Transaktionsfunktion kann umfassend dahingehend verstanden werden, dass die transferierten Werteinheiten alles repräsentieren können, worauf Menschen sich einigen können.[165] Die Transaktionsfunktion kann

160 *Kaulartz*, CR 2016, 474 (476f.); *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff). So auch Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 15ff.
161 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255).
162 *Börner*, NZWiSt 2018, 48 (48).
163 Siehe hierzu oben unter A.II.7., III.1.c). Hierzu insbesondere auch *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255).
164 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8f.
165 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 41.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

sich also gerade auch auf Umstände erstrecken, die außerhalb der Blockchain liegen.[166]

So könnte die Blockchain-Technologie etwa für das Grundbuchamt, das Handelsregister[167], sog. *Smart Contracts*[168], Musiklizensierung, Versicherungen und gesellschaftsrechtliche Organisationen[169] dienen (zu diesen Anwendungsmöglichkeiten im Einzelnen sogleich unter C.).

2. Dokumentationsfunktion

Daneben bietet die Blockchain-Technologie auch eine Dokumentationsfunktion, da sie auf Grund ihrer Unveränderlichkeit[170] in besonderem Maße fälschungssicher ist.[171] Deshalb kann sie gerade auch zur Dokumentation von (Transaktions-)Vorgängen verwendet werden.[172] Sie dokumentiert insoweit die soeben beschriebene Transaktionsfunktion. Insoweit ist sie Integritätssicherung von Daten.[173]

III. Blockchain-Technologie ist dezentrale Datenverwaltungsstruktur

Daraus ergibt sich, dass die Blockchain-Technologie nicht einmal auf die Anwendung zur Transaktion von Werteinheiten beschränkt ist. Sie kann deshalb allgemein im technischen Sinne als Protokoll zur dezentralen Datenverwaltung verstanden werden.[174]

166 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255f.); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz*, Kap. 4.1 Rn. 43f.
167 Siehe hierzu etwa *Knaier/Wolf*, Betriebs-Berater 2018, 2253.
168 Siehe hierzu etwa *Kaulartz/Heckmann*, CR 2016, 618.
169 Siehe hierzu etwa *Mann*, NZG 2017, 1014.
170 Siehe hierzu oben unter Kap. 2, A.III.2. m.w.N.
171 *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Kaulartz/Matzke*, NJW 2018, 3278 (3282); *Spindler*, ZGR 2018, 17 (49).
172 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256).
173 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256); *Sattler*, Betriebs-Berater 2018, 2243 (2245).
174 *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; *Böhme/Pesch*, DuD 2017, 473 (474); Breidenbach-Glatz RhdB-Legal-Tech/*Krall*, Kap. 5.7 Rn. 11; *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

IV. Differenzierung von Blockchain-Technologien und thematische Beschränkung

Diese Datenverwaltung kann in unterschiedlicher Weise erfolgen. So ist zwischen verschiedenen Ausprägungen der Blockchain-Technologien zu differenzieren.

1. Ausgangspunkt: Offene, genehmigungsfreie, pseudonymisierte Blockchain

Ausgangspunkt ist die von *Satoshi Nakamoto* entwickelte Blockchain-Technologie. Sie wurde als Netzwerk, das für jeden zugänglich ist (=offen)[175] und in dem jeder Teilnehmer gleichzeitig auch *miner* bzw. *nodes* sein kann (=genehmigungsfrei) und die Blockchain fortschreiben kann, angelegt. Außerdem handeln die Nutzer im Netzwerk nur unter den Pseudonymen der *public keys* bzw. den *Bitcoin-Adressen* (=Pseudonymität).[176]

2. Abweichung 1: geschlossene Blockchain

Mittlerweile haben insbesondere Finanzdienstleister, aber auch andere Unternehmen[177] das Potenzial der Blockchain-Technologie entdeckt.[178] Allerdings insbesondere wegen ihrer Datenverwaltungsstruktur.[179] Sie haben Blockchain-Technologien entwickelt, auf die nur bestimmte Beteiligte – wie etwa die Unternehmen[180] – Zugriff haben.[181] Hier dient die Blockchain-

175 *Kaulartz*, CR 2016, 474 (475); *Schlund/Pongratz*, DStR 2018, 598 (599).
176 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1.
177 Wie zum Beispiel die AXA-Versicherung.
178 So beschreibt Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 51ff. ausführlich, für welche Wirtschaftsbereiche und Anwendungsfälle die Blockchain-Technologie angewendet werden könnte.
179 So etwa Breidenbach-Glatz RhdB-Legal-Tech/*Regierer,* Kap. 5.2 Rn. 3, der darstellt, dass die dezentrale Verwaltungsstruktur besondere Vorteile für die Abwicklung von Lieferketten hat. Außerdem ist die Blockchain-Technologie gerade auch mit Blick auf die Integrität der in ihre enthaltenen Daten für Unternehmen interessant.
180 Oder etwa Unternehmenskonsortien, wie etwa das sogleich genannte R3-Bankenkonsortium.
181 So etwa das R3-Bankenkonsortium, das sich zu einem weltumspannenden Transaktionsnetzwerk zusammengeschlossen hat, vgl. *Glatz*, DGRI Jahrbuch 2016, Rn. 7.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Technologie nur als interne Datenverwaltungsstruktur.[182] Weiteren Nutzern steht diese Blockchain nicht zur Verfügung (= geschlossene Blockchain).

3. Abweichung 2: genehmigungsbedürftige Blockchain

Wie oben bereits erwähnt hat das beschriebene *Proof-of-Work*-Konsensverfahren insbesondere den Nachteil, dass es sehr viel Rechenleistung benötigt.[183] Eine oben kurz angedeutete Alternative ist das sog. *Proof-of-Authority*-Verfahren, bei dem nur diejenigen Netzwerkteilnehmer die Blockchain fortschreiben, die vom Algorithmus hierzu autorisiert wurden.[184] Das Fortschreiben der Blockchain setzt also eine Genehmigung voraus (= genehmigungsbedürftige Blockchain).[185]

4. Abweichung 3: Blockchain mit unmittelbarem Personenbezug

Soweit die Blockchain-Technologie lediglich für interne Datenverwaltungsstrukturen verwendet wird, ist die durch den *public key* gewährleistete Pseudonymität bzw. Anonymität nicht mehr erforderlich. Eine Blockchain, die mit „Klarnamen" funktioniert erscheint insoweit möglich.[186]

5. Beschränkung der Untersuchung auf offene Blockchains

Die nachfolgende Untersuchung der rechtlichen Zulässigkeit von Blockchain-Auswertungen zu Strafverfolgungszwecken beschränkt sich auf die Inhalte in offenen Blockchains. Denn soweit die Blockchain-Technologie lediglich zur internen Datenverwaltung im Unternehmen bzw. in der internen öffentlichen Verwaltung verwendet wird und die Blockchain-Daten nicht öffentlich zugänglich sind, ergibt sich aus der Verwendung der Blockchain-Technologie für strafprozessuale Ermittlungen keine Besonderheit.

182 *Glatz*, DGRI Jahrbuch 2016, Rn. 7f.; *Hofert*, Regulierung der Blockchains, S. 14, 22; *Janicki/Saive*, ZD 2019, 251 (254).
183 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 30.
184 *Janicki/Saive*, ZD 2019, 251 (251f.).
185 *Janicki/Saive*, ZD 2019, 251 (251f.); siehe hierzu auch die Differenzierung von *Martini/Weinzierl*, NVwZ 2017, 1251 (1253f.), die zwischen zulassungsfreien und zulassungsbeschränkten Blockchains differenzieren. So etwa die im Folgenden dargestellte virtuelle Kryptowährung "Libra".
186 So etwa eine von *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2257) dargestellte Möglichkeit zur Führung des Handelsregisters.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Da auch genehmigungsbedürftige Blockchains als offenes Netzwerk ausgestaltet sein können[187], werden auch sie Gegenstand der nachfolgenden Untersuchung sein. Außerdem können sich in der rechtlichen Bewertung Unterschiede dadurch ergeben, dass die Inhaltsdaten in der Blockchain pseudonymisiert bzw. anonymisiert sind, sodass auch diese Abweichung Gegenstand der Untersuchung sein wird.

C. Weitere blockchain-basierte Anwendungen

Welche Daten dann durch die Blockchain-Technologie verwaltet werden, hängt davon ab, wie sie konkret eingesetzt und ausgestaltet wird. Hierzu gibt es sowohl von Seiten der Bundesregierung wie auch von privaten Unternehmen verschiedene Ideen, die teilweise bereits umgesetzt wurden.[188] Da die Anwendungsfälle der Blockchain-Technologie fast täglich wächst[189], kann eine vollumfassende Darstellung der Anwendungsfälle von Blockchain-Technologien im Folgenden nicht geleistet werden. Um aber einen Überblick zu geben, wie weitreichend die Anwendungsfälle sein können, werden nachfolgend verschiedene Beispielsanwendungen dargestellt.

Zu differenzieren ist hier zwischen den klassischen virtuellen Kryptowährungen (hierzu unter I.), den sog. *Smart Contract*-Anwendungen (hierzu unter II.) und Anwendungen im Bereich der öffentlichen Verwaltung (hierzu unter III.).

I. Virtuelle Kryptowährungen

Bereits vor dem rasanten Bekanntheitsgrad und dem Kursgewinn von Bitcoin in den vergangenen Jahren hatten sich bereits weitere virtuelle Kryptowährungen herausgebildet – im Dezember 2021 wurden auf der

187 Vgl. insoweit etwa die nachfolgend dargestellte virtuelle Kryptowährung „Libra".

188 Siehe hierzu u.a. die Antwort der Bundesregierung auf die kleine Anfrage, welche Anwendungsmöglichkeiten es für sog. *Distributed-Ledger-Technologien* gibt, BT-Drs. 19/3817. Einen Überblick über mögliche Anwendungsfelder geben auch: *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 51ff.

189 Siehe hierzu etwa die Offenlegungsschriften des Deutschen Patentamtes, die nach dem Stichwort „Blockchain" gefiltert werden können; so auch *Glatz*, DGRI Jahrbuch 2016, Rn. 7ff.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Website „coinmarktecap" 15.838 virtuelle Kryptowährungen gelistet.[190] Im Folgenden werden nur drei Beispiele weiterer virtueller Kryptowährungen in ihren technischen Abweichungen dargestellt.

1. Bitcoin-Cash

Bitcoin-Cash ist eine Abspaltung aus dem ursprünglichen Bitcoin-Netzwerk, die am 01. August 2017 stattfand.[191] Hintergrund war, dass die Datenmenge der Blöcke im Bitcoin-System begrenzt war und deshalb nur etwa 7 Transaktionen pro Sekunde durchgeführt werden konnten.[192] Bitcoin-Cash erweiterte die Datenmenge der Blöcke, sodass im Bitcoin-Cash-System etwa 8-mal so viel Transaktionen pro Sekunde möglich sind.[193]

2. Litecoin

Litecoin wurde im Oktober 2011 als Open-Source-Software veröffentlicht und wird, wie Bitcoin, dezentral über ein *Peer-to-Peer-Netzwerk* verwaltet.[194] Die virtuelle Kryptowährung unterscheidet sich zu Bitcoin technisch darin, dass die Blöcke etwa alle 2,5 Minuten erzeugt werden[195] und auch in diesem kürzeren Zeitabstand jeweils neue Litecoin durch das *mining* erzeugt werden. Dementsprechend ist auch die verfügbare Gesamtmenge der Litecoin ca. 84 Millionen.[196] Außerdem verwendet Litecoin eine andere *Hashfunktion* in ihrem *Proof-of-Work* Algorithmus, der das *mining* gleichmäßig auf die beteiligten Nutzer verteilen soll.[197]

---

190 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 27f.; https://coinmarketcap.com/currencies/views/all/ (letzter Abruf: 20. Dezember 2021).

191 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46. Siehe hierzu auch: https://www.bitcoincash.org (letzter Abruf: 20. Dezember 2021).

192 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46. Hierzu insbesondere auch: https://bchfaq.com/faq/whats-the-difference-between-bitcoin-cash-and-bitcoin/ (letzter Abruf: 20. Dezember 2021).

193 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46.

194 Siehe hierzu: https://litecoin.org/de/ (letzter Abruf: 20. Dezember 2021).

195 Statt wie bei Bitcoin etwa alle 10 Minuten, *Kaulartz*, CR 2016, 474 (474); *Hofert*, Regulierung der Blockchains.

196 Vgl. hierzu https://litecoin.info/index.php/Main_Page und https://litecoin.org (letzter Abruf jeweils: 20. Dezember 2021).

197 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 28; Hierzu ebenfalls https://litecoin.info/index.php/Main_Page und https://litecoin.org (letzter Abruf jeweils: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

3. Libra / Diem – FacebookCoin

Im Juni 2019 veröffentlichte die LibraAssociation das Whitepaper der Kryptowährung „Libra" – eine virtuelle Kryptowährung in Kooperation mit Facebook.[198] Mittlerweile hat sich das Projekt in „Diem" umbenannt.[199] Das vordergründig gemeinnützige Ziel, den 1,7 Milliarden Menschen auf der Welt, die bisher noch keinen Zugang zu einem Konto haben, aber ein Smartphone besitzen, Zahlungen über ein alternatives Finanzsystem zu ermöglichen, soll ab 2020 durch ein blockchain-basiertes alternatives Zahlungssystem erreicht werden.[200] Grundlage soll zwar auch hier die Blockchain-Technologie sein, in diesem Fall aber in der modifizierten Form, dass die Transaktionen von sog. *validator-nodes* (= Mitglieder der LibraAssociation) bestätigt werden.[201] *Miner*[202] und damit diejenigen, die die Blockchain fortschreiben, sind zum Zeitpunkt des Starts des Systems nur diejenigen, die von der LibraAssociation eine entsprechende Genehmigung erhalten haben (= genehmigungsbedürftige Blockchain).[203] Obwohl die Verwaltung insoweit nicht von allen Nutzern gleichberechtigt vorgenommen wird, sollen alle Nutzer Zugriff auf die Inhaltsdaten der Blockchain haben mit dem vordergründigen Ziel eine offene, transparente und verlässliche virtuelle Kryptowährung zu schaffen.[204]

198 Siehe hierzu etwa: https://www.tagesschau.de/wirtschaft/facebook-digitale-weltwaehrung-101.html (letzter Abruf: 20. Dezember 2021)

199 Vgl. https://www.diem.com/en-us/white-paper/#cover-letter (letzter Abruf: 20. Dezember 2021)

200 So das erklärte Ziel im Whitepaper der *LibraAssociation*, Cover Letter, White Paper v2.0, S. 4.

201 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 8.

202 Die LibraAssociation spricht in ihrem White-Paper zwar von *validator-nodes,* hier wird allerdings an der oben angegebenen Differenzierung zwischen *nodes,* die lediglich Kommunikationsknoten sind, und *minern,* die die Blockchain selbst aktiv fortschreiben, festgehalten.

203 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 8. Allerdings soll die Libra Blockchain im weiteren Verlauf als genehmigungsfreie Blockchain ausgestaltet werden. Siehe zur Differenzierung der Blockchain-Technologien oben unter B.IV.2.

204 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 22f. Deshalb wird Libra in der öffentlichen Debatte aktuell scharf kritisiert, vgl. hierzu etwa *Menges*, Datenschützer äußern Bedenken zu Facebooks Libra.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

II. Smart Contracts

Ähnlich wie die virtuellen Währungen, ist auch der Begriff der sog. *Smart Contracts* bereits aus den 90er Jahren bekannt.[205] *Nick Szabo* veröffentlichte 1997 erstmals seine Theorie von Verträgen, die sich selbst ausführen.[206] Zentrales Problem zu dieser Zeit war allerdings, dass ein zentraler Intermediär weiterhin erforderlich war um die Verträge abzuwickeln.[207] Deshalb konnten sich die *Smart Contracts* zu diesem Zeitpunkt noch nicht durchsetzen.[208] Die Idee gewann deshalb mit Einführung der Blockchain-Technologie wieder an Interesse, da diese gerade ohne eine zentrale Verwaltungsinstanz auskommt.[209]

1. Was ist ein Smart Contract und wie funktioniert er?

a) Ziel und Funktion eines Smart Contracts

Smart Contracts sollen Vertragsbeziehungen programmieren und automatisieren.[210] Das bedeutet, dass das synallagmatische Verhältnis von Verträgen automatisch ausgeführt wird, indem es in die Programmlogik eines Computers implementiert wird.[211]

Vielfach zitiertes Beispiel ist der Leasingvertrag eines Autos.[212] In den *Smart Contracts* werden die Vertragsbedingungen wie die Höhe der Leasingraten und die Fälligkeit der Raten und der Leasinggegenstand implementiert.[213] Der Bordcomputer des Autos ist mit dem *Smart Contract*

205 *Kaulartz/Heckmann*, CR 2016, 618 (618); *Glatz*, DGRI Jahrbuch 2016, Rn. 19; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 13.
206 *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2092); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3, Rn. 13; *Heckelmann*, NJW 2018, 504 (504).
207 *Kaulartz/Heckmann*, CR 2016, 618 (618).
208 *Kaulartz/Heckmann*, CR 2016, 618 (618); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 17ff.
209 *Kaulartz/Heckmann*, CR 2016, 618 (618f.); Vgl. insoweit auch *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2092).
210 *Kaulartz/Heckmann*, CR 2016, 618 (618f); *Mann*, NZG 2017, 1014 (1015); *Heckelmann*, NJW 2018, 504 (504).
211 *Kaulartz/Heckmann*, CR 2016, 618 (618f.); *Mann*, NZG 2017, 1014 (1015); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 14f.; *Heckelmann*, NJW 2018, 504 (504).
212 Hierzu ausführlich *Kaulartz/Heckmann*, CR 2016, 618 (618).
213 *Kaulartz/Heckmann*, CR 2016, 618 (618).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

verknüpft und kann so selbständig überprüfen, ob die Leasingraten zum vereinbarten Zeitpunkt gezahlt wurden, und kann davon abhängig machen, ob die Zündung des Autos funktioniert.[214]

In diesem Kontext ist eine Instanz notwendig, die das Vorliegen der Vertragsbedingungen überprüft und der beide Vertragspartner vertrauen – durch die Blockchain-Technologie kann diese Funktion nun das Netzwerk der Blockchain-Teilnehmer übernehmen.[215]

b) (Versuch einer) Definition eines Smart Contracts

Den ersten Versuch einer Definition von *Smart Contracts* nehmen *Kaulartz/Heckmann* vor und arbeiten die folgenden wesentlichen Merkmale von *Smart Contracts* anhand des Beispiels eines Leasingvertrags über ein Auto heraus:[216]

- „ein digital überprüfbares Ereignis
- ein Programmcode, welcher das Ereignis verarbeitet
- eine rechtlich relevante Handlung, welche auf Grundlage des Ereignisses ausgeführt wird"[217]

Dementsprechend soll ein *Smart Contract* eine Software sein, „die rechtlich relevante Handlungen […] in Abhängigkeit von digital überprüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert"[218].

c) Die Blockchain-Technologie bei Smart Contracts

Im Kontext der *Smart Contracts* übernimmt die Blockchain-Technologie die Funktion der Überprüfung der Transaktionen.[219]

---

214 *Kaulartz/Heckmann*, CR 2016, 618 (618).

215 *Kaulartz/Heckmann*, CR 2016, 618 (618); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 18f.

216 *Kaulartz/Heckmann*, CR 2016, 618 (618).

217 *Kaulartz/Heckmann*, CR 2016, 618 (618), der auf die von *Nick Szabo* verwendete Definition *„A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.*" verweist. Ähnlich auch: *Heckelmann,* NJW 2018, 504 (504).

218 *Kaulartz/Heckmann*, CR 2016, 618 (618).

219 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 19. Siehe zur Transaktionsüberprüfung ausführlich oben unter A.III.1.c).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Denn im Bitcoin-System überprüfen die *miner* die Transaktionen des *memory-pools* anhand einer Checkliste, bevor sie sie in den *candidate-block* aufnehmen.[220] Bei Bitcoin umfasst die Überprüfung der Transaktionen insbesondere das Kriterium, dass die zu verifizierende Transaktion der bisherigen Blockchain nicht widerspricht und auch keine weitere widersprechende Transaktion im *memory-pool* enthalten ist.[221] Bei der Transaktionsprüfung können aber beliebig viele weitere Kriterien enthalten sein.[222] Hierzu ist aber eine Modifizierung der oben beschriebenen Funktionsweise der Blockchain-Technologie erforderlich, und zwar dahingehend, dass in der Blockchain die zu überprüfenden Bedingungen abgelegt werden müssen.[223]

2. Die „Ethereum"-Blockchain als Grundlage von Smart Contracts

Eine Plattform, die dies ermöglicht, bietet die bislang in diesem Bereich erfolgreichste Blockchain „Ethereum".[224] Genauso wie die Bitcoin-Blockchain erfolgt ein Zusammenschluss der Rechner über das Internet zu einem *Peer-to-Peer-Netzwerk,* das gemeinsam die zugrundeliegende Blockchain fortschreibt.[225]

Anders als bei Bitcoin ist es im Etherum-Netzwerk möglich, nicht nur sog. *Ether* (= die von Etherum verwendete virtuelle Kryptowährung) zu transferieren, sondern die *nodes* können auf der Blockchain eigene *Smart Contracts* ablegen*,* nach deren Bedingungen Transaktionen ablaufen.[226] Die Ethereum-Blockchain ist insoweit entwicklungsoffen und kann deshalb als Weiterentwicklung der Bitcoin-Blockchain verstanden werden.[227]

Ein *Smart Contract* ist in diesem Zusammenhang ein automatisierter Agent, der im Ethereum-Netzwerk lebt, eine eigene Ethereum-Adresse und

220 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182f.
221 Siehe hierzu bereits oben unter A.III.1.c). *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies.
222 *Kaulartz/Heckmann*, CR 2016, 618 (619).
223 *Kaulartz/Heckmann*, CR 2016, 618 (619).
224 *Kaulartz/Heckmann*, CR 2016, 618; *Heckelmann*, NJW 2018, 504 (505); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 21.
225 *Buterin*, Ethereum White Paper, S. 1; *Kaulartz/Matzke*, NJW 2018, 3278 (3278).
226 *Hoffer/Mirtchev*, NZKart 2019, 239 (241). Siehe hierzu insbesondere auch die Darstellung auf https://www.ethereum.org/beginners/ (letzter Abruf: 20. Dezember 2021).
227 *Mann*, NZG 2017, 1014 (1015).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

-Guthaben hat und selbst Transaktionen senden und empfangen kann.[228] Dieser Agent wird jedes Mal „aktiviert", wenn jemand eine Transaktion an ihn richtet, dann führt er seinen Code aus. So ist es möglich, dass in einer Blockchain die Bedingungen eines Vertrages abgelegt werden können, der sich selbst automatisch ausführt.[229]

So könnte das oben angesprochene Beispiel des Leasingvertrages in die Ethereum-Blockchain abgelegt werden.[230] Eine Transaktion an den *Smart Contract* wäre dann etwa das Drehen des Zündschlüssels, bei dem der Code des *Smart Contracts* ausgelöst würde und überprüfen könnte, ob eine Zahlung auf einem bestimmten Konto eingegangen ist und im Anschluss die Nachricht an den Bordcomputer des Autos sendet, dass der Motor gestartet werden darf.[231]

Werden mehrere dieser sich selbst ausführenden Verträge miteinander verbunden, spricht das Netzwerk von sog. *DApps* – Decentralized Apps.[232] Solche DApps können sehr komplex gestaltet werden, sodass sie etwa

228 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 48, der insoweit auf *Buterin*, Ethereum White Paper verweist.

229 *Glatz*, DGRI Jahrbuch 2016, Rn. 17ff.; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 48.

230 Ähnlich auch *Glatz*, DGRI Jahrbuch 2016, Rn. 17ff., der als Beispiel einen Kauf im Internet erläutert, bei dem der Kaufpreis an einen dritten public key gesendet wird, von dem der Kaufpreis erst an den Verkäufer überwiesen werden kann, wenn sowohl Käufer wie auch Verkäufer die Transaktion mit ihren private keys signiert haben.

231 *Kaulartz/Heckmann*, CR 2016, 618 (618). Das bedeutet jedoch nicht, dass jeder blockchain-basierte Smart Contract auch jede Transaktion in der Blockchain ablegt, denn – wie bereits dargestellt – sind für die Datenverwaltung von Blockchains große Rechenkapazitäten erforderlich. Bei kommerziellen Anbietern wird deshalb wohl die Blockchain praktisch nicht zu Verwaltung aller Daten eingesetzt werden, sondern lediglich zur Verfügung über Berechtigungen. Im Fall des Leasingvertrages könnte entsprechend auch nur die Verfügung über die Berechtigung an den Leasingnehmer in die Blockchain eingetragen werden – alle weiteren Daten könnten in einer „herkömmlichen" Datenverwaltungsstruktur erfasst werden. Allerdings sind auch durchaus Anwendungsfälle denkbar, in denen es erforderlich ist, sämtliche Daten in die Blockchain einzutragen – namentlich dann, wenn es keinen zentralen Diensteanbieter gibt. Ein Beispiel könnte etwa ein dezentraler Carsharing Smart Contract sein, bei dem jeder Interessierte sein Auto zur Verfügung stellen kann und selbst auch die Autos aller anderer Nutzer mieten kann. Soweit hier wiederum auf einen zentralen Diensteanbieter verzichtet werden soll, wäre es erforderlich, alle notwendigen Daten (wie Zeitpunkt der Anmietung, Ort der Anmietung, Zeitpunkt der Rückgabe und Ort der Rückgabe, sowie die „Vertragsparteien") in die Blockchain einzutragen.

232 *Buterin*, Ethereum White Paper, S. 1, 33; *Hoffer/Mirtchev*, NZKart 2019, 239 (241).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:35
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Gesellschaftsverträge, Shareholder-Agreements und verschiedene Finanzinstrumente abbilden können.[233]

Die Blockchain-Technologie liefert dabei wiederum die Funktion der Verifikationsstelle. Die Teilnehmer des *Peer-to-Peer-Netzwerkes* überprüfen, ob die Bedingungen eingetreten sind, die Voraussetzungen für die Ausführungen bzw. Verifikation der Transaktion sind.[234]

3. Was sind ICOs – „Initial Coin Offerings"?

Über die Ethereum-Blockchain werden mittlerweile vermehrt sog. *ICOs (= „Initial Coin Offerings")* abgewickelt, die eine bestimmte Form des Crowdfundings darstellen.[235] Hierbei veröffentlichen Entwickler ihre Ideen und verkaufen sog. *tokens* über *Smart Contracts* an Kapitalgeber.[236] Mit dem eingenommenen Kapital wird dann die Idee des Entwicklers ausgearbeitet.[237] Den *token* kommt insoweit eine mit Unternehmensanteilen vergleichbare Funktion zu.[238]

4. Smart-Contract-Beispiele

a) The DAO

Das wohl wichtigste Beispiel der *Smart Contracts* dürfte die im Jahr 2016 auf der Etherum-Blockchain abgelegte sog. *„The DAO"* – The Decentralized Autonomus Organisation – sein, die innerhalb kürzester Zeit Kapital in

233 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 49; *Sattler*, Betriebs-Berater 2018, 2243 (2249).

234 *Kaulartz/Heckmann*, CR 2016, 618 (619); *Mann*, NZG 2017, 1014 (1015).

235 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 24ff.; *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (90).

236 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 25f.

237 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 27ff.

238 Dieser Vergleich dient lediglich zum Verständnis und ist vereinfacht. Lediglich die sog. *Investment Tokens* haben tatsächlich mit Unternehmensanteilen vergleichbare Funktionen, vgl. *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (92). Hierzu sogleich am Beispiel der „The DAO". Diese gesellschaftsrechtliche Differenzierung ist allerdings für die Frage nach den Auswertungsmöglichkeiten von Strafverfolgungsbehörden irrelevant.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Höhe von ca. 160 Mio. $ aufnahm und damit das damals größte Crowdfunding Projekt aller Zeiten war.[239]

Die *DAO* besteht aus mehreren *Smart Contracts,* die *Christopher Jentzsch* 2016 in seinem White Paper als Programmcode veröffentlichte.[240] Die DAO soll nach Ablage auf der *Ethereum-Blockchain* Kapital aufnehmen, indem Nutzer *Ether* an ihre *Ethereum-Adresse* senden.[241] Im Gegenzug erhalten die kapitalgebenden Nutzer frei weiterveräußerliche Eigentümer- und Stimmrechte (sog. *token*), mit denen sie im Anschluss Vorschläge über die Verwendung des Kapitals machen könnten.[242] Sobald sich eine bestimmte Mehrheit aus den *token* gebildet hätte, sollte die entsprechend gewählte Verwendung ausgeführt werden.[243]

Mann beschreibt die *DAO* als „eine auf Dauer angelegte Organisation, die aus einem Programmcode besteht, der dezentralisiert in der digitalen Welt verwahrt und ausgeführt wird; ihr wird eigenes Kapital überwiesen, das die Gesamtheit der Kapitalgeber gemäß den selbstausführenden Regeln des Programmcodes unmittelbar verwaltet."[244]

Auch wenn die juristische Einordnung dieses Programmcodes bisher nicht eindeutig geklärt ist[245], gleicht sie einer gesellschaftsrechtlichen Organisation und verdeutlicht dadurch insbesondere, welches Ausmaß *Smart Contracts* haben können.[246]

b) Lition

Das 2018 an den Markt gegangene Start-Up „Lition", das mittlerweile im Oktober 2021 Insolvenz anmelden musste[247], bezeichnete sich selbst als ers-

239 *Mann*, NZG 2017, 1014 (1014, 1016); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91).
240 *Mann*, NZG 2017, 1014 (1015); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
241 *Mann*, NZG 2017, 1014 (1015); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91); *Sattler*, Betriebs-Berater 2018, 2243 (22250).
242 *Mann*, NZG 2017, 1014 (1015); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
243 *Mann*, NZG 2017, 1014 (1015); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
244 *Mann*, NZG 2017, 1014 (1015).
245 Vgl. insoweit zur Diskussion der rechtlichen Einordnung ausführlich *Mann*, NZG 2017, 1014 (1019f.).
246 *Sattler*, Betriebs-Berater 2018, 2243 (2250f.).
247 Vgl. https://lition.de/goodbye-lition (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ter blockchain-basierter Energieversorger.[248] Sein Ziel war es, dass Kunden am Strommarkt selbst agieren können und den Strom von Produzenten direkt beziehen können.[249]

Auf der von Lition angebotenen Plattform konnten Kunden einen Stromerzeuger auswählen und dann bilanziell von diesem Erzeuger ihren Strom erwerben. Die Abwicklung übernahm dabei die Plattform Lition, die selbst am Strommarkt auftrat und den jeweils von Kunden abgenommenen Strom am Markt kaufte. Eine direkte Vertragsbeziehung zwischen Produzent und Konsument war laut Unternehmensangaben auf Grund gesetzlicher Vorgaben noch nicht möglich.

Dabei verwendete das Unternehmen die Ethereum-Blockchain zur Abwicklung der Verträge. Gemeint waren hiermit wohl die konkreten Verträge zwischen Lition und den Stromerzeugern, da Lition angab, den Strom für seine Kunden entweder als Beauftragte des Kunden am Markt zu beschaffen oder den Kunden die Aktivität am Markt selbst über die Ethereum-Blockchain zu ermöglichen.

c) Fizzy – Flugverspätungsversicherung

Ein ähnliches Projekt war die von der AXA entwickelte Flugverspätungsversicherung, die im Versicherungsfall (eine Flugverspätung von mehr als 2 Stunden) eine automatische Auskehrung der Versicherungssumme versprach. Hierzu wurde wiederum die Ethereum-Blockchain verwendet, in der der *Smart Contract* über die Flugversicherung niedergelegt wurde.[250] Wenn das Flugzeug nun landete, glich der *Smart Contract* die Zeitdaten ab und zahlte im Fall einer Verspätung automatisch die Versicherungssumme

248 Vgl. hierzu ein Interview mit dem Unternehmensgründer, abrufbar unter: https://www.energate-messenger.de/news/190680/ha-erloes-ist-etwa-zehn-prozent-hoeher-als-ueblich- (letzter Abruf: 20. Dezember 2021).

249 So das erklärte Ziel des Unternehmens, abrufbar unter. Vgl. auch die Podiumsdiskussion mit dem CEO von Lition im Fachgespräch „#leben2030" der Unionsfraktion vom 03. April 2019, abrufbar unter: https://www.cducsu.de/veranstaltungen/leben2030-blockchain-chancen-nutzen (letzter Abruf: 20. Dezember 2021).

250 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

an den Versicherungsnehmer aus.[251] Dabei wurden allerdings die persönlichen Daten des Kunden nicht in der Ethereum-Blockchain niedergelegt.[252]

d) „Bitsong" und „KodakOne" – Musik- und Fotoindustrie

Auch im Bereich der Musik- und Fotoindustrie gibt es mittlerweile erste blockchain-basierte Anwendungen.

So gibt es mittlerweile mit „Bitsong" einen ersten blockchain-basierten Musik-Streaming-Anbieter, bei dem Künstler ihre Musik in einer Blockchain veröffentlichen können und diese von Kunden dann mittels *Smart Contract* gehört werden kann.[253]

Für den Bereich der Fotoindustrie hat Kodak mit „KodakOne" eine ähnliche Anwendung geschaffen. Über die „blockchain-basierte Foto-Rechte-Management Plattform"[254] können Fotografen Lizenzen ihrer Fotos anbieten.[255]

e) Zwischenergebnis

Die vorstehenden Beispiele für blockchain-basierte *Smart Contracts* verdeutlichen wie weit der mögliche Anwendungsbereich der Blockchain-Technologien ist. Kernpunkt aller Anwendungen ist dabei, dass durch die Blockchain-Technologie hohe Verwaltungskosten wegfallen sollen, da sich die Anwendungen durch die Technologie selbst abwickeln sollen. Dabei sind die Inhaltsdaten der Blockchains überwiegend öffentlich einsehbar. Uneinheitlich bleibt in diesem Zusammenhang die tatsächliche konkrete Ausgestaltung der Anwendungen – insbesondere, welche Daten in die jeweiligen Blockchains geschrieben werden.

251 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

252 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

253 Vgl. hierzu das White-Paper des Streaming-Anbieters, *Recca/Ricli/Anghelin/Farruggio*, The first decentralized music streaming platform a new era in music streaming.

254 So die wörtliche Übersetzung der Unternehmensangabe, abrufbar unter: https://www.kodakone.com (letzter Abruf: 28. August 2019).

255 Vgl. https://vkool.com/kodakone/ (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

III. Öffentliche Verwaltung

Auch im Bereich der öffentlichen Verwaltung bzw. der öffentlichen Registerführung wird mittlerweile intensiv diskutiert, ob und inwieweit die Blockchain-Technologie hier zum Einsatz kommen kann[256] – teilweise gibt es in anderen Ländern bereits blockchain-basierte Bereiche der öffentlichen Verwaltung.[257] Diskutiert wird in Deutschland aktuell vor allem der Einsatz beim Handelsregister und Grundbuchamt.[258] In anderen Europäischen Ländern – wie etwa Estland – kommt die Blockchain-Technologie bereits für verschiedene Register – wie etwa das „Healthcare Registry" und das „Property Registry" – zum Einsatz, allerdings nur zur Absicherung der Daten.[259]

D. Zwischenergebnis

Die Blockchain-Technologie geht zurück auf die virtuelle Kryptowährung Bitcoin aus dem Jahr 2008 und fungiert in diesem Zusammenhang als dezentral geführtes Transaktionsregister. Ihr Ziel besteht darin, ein Register zu führen, das losgelöst von zentralen Intermediären funktioniert und für das kein Vertrauen mehr in eine zentrale Instanz notwendig ist.

Wesentlicher technologischer Fortschritt der Blockchain-Technologie ist ihre dezentrale Verwaltungsstruktur, die davon geprägt ist, dass sich alle Nutzer bzw. Teilnehmer des Netzwerks auf einen Konsens einigen und diesen in ihrer zentralen Datenbank fortschreiben. Dies ist deshalb ein wesentlicher Fortschritt, weil auch im Zeitalter des World Wide Web die meisten Online-Anwendungen von einer jeweils zentralen Instanz verwal-

256 Vgl. insoweit die intensive Diskussion von *Knaier/Wolf*, Betriebs-Berater 2018, 2253., der sich ausführlich mit der Frage auseinandersetzt, wie die Blockchain-Technologie für das Handelsregister und das Grundbuch eingesetzt werden können.

257 Vgl. insoweit die Einführung der sog. *E-ID* in der Schweiz und das darauf aufbauende blockchain-basierte Wahlsystem, abrufbar unter: https://www.heise.de/newsticker/meldung/Schweiz-Blockchain-Identitaet-fuer-Zug-E-ID-fuers-ganze-Land-3892220.html; https://www.heise.de/newsticker/meldung/Schweizer-Crypto-Valley-E-Voting-auf-Blockchain-Basis-in-Zug-4092661.html (letzter Abruf jeweils: 20. Dezember 2021).

258 *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Schrey/Thalhofer*, NJW 2017, 1431 (1432); *Knaier/Wolf*, Betriebs-Berater 2018, 2253.

259 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256). Vgl. auch: https://e-estonia.com/blockchain-healthcare-estonian-experience/ (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

tet werden. So verwalten Facebook, Google, Amazon und andere Online-Dienstanbieter die Daten ihrer Nutzer in zentralen Rechenzentren. Im Fall der Blockchain-Technologie sind dagegen die Nutzer des Netzwerks bzw. des Online-Angebotes selbst diejenigen, die die Daten des Netzwerks verwalten – hier existieren keine zentralen Knoten, über die die Kommunikation abgewickelt wird, sondern alle Nutzer sind selbst die Knoten.[260]

Der Anwendungsbereich der Blockchain ist allerdings nicht auf das Register von Kryptowährungen beschränkt, sondern die Technologie kann insgesamt als eine dezentral verwaltete Datenverwaltungsstruktur verstanden werden, in der Daten unabhängig von ihrem Inhalt dokumentiert und verwaltet werden können.

So können durch die Blockchain *Smart Contracts* abgebildet und ausgeführt werden, über die etwa Stromhandel, Musikstreaming, Fotolizensierung und auch gesellschaftsrechtliche Strukturen abgewickelt werden können. Dementsprechend weit können auch die Inhaltsdaten der verschiedenen Blockchains sein.

Als mittelbare Folge dieser technologischen Architektur sind jegliche Inhaltsdaten der Blockchain öffentlich verfügbar, soweit die jeweilige Blockchain als offenes Netzwerk ausgestaltet ist, da jeder Teilnehmer des Netzwerkes die Transaktionen der anderen Teilnehmer des Netzwerkes überprüfen können muss.

260 Dieser Architektur-Unterschied wird besonders deutlich anhand der Abbildung in Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 13.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Kapitel 3 – Technische Auswertungs- und Ermittlungsmöglichkeiten bei Blockchain-Systemen

Die Blockchain-Technologie ist vor allem aus dem Zusammenhang mit Kryptowährungen und deren Verwendung für illegale Aktivitäten bekannt. Denn da es keine zentrale Verwaltungsstelle gibt und die Nutzer nur unter den Pseudonymen der *public keys* miteinander agieren und diese einer Person nicht unmittelbar zugeordnet werden können[261], gelten Kryptowährungen als anonymes Zahlungsmittel.[262] Aus diesem Grund sind sie für illegale Aktivitäten besonders beliebt.[263] So geht eine aktuelle Studie davon aus, dass 46% der Bitcoin-Transaktionen im Zusammenhang mit illegalen Aktivitäten stehen.[264] Hierbei werden Kryptowährungen insbesondere eingesetzt, um Zahlungen zu illegalen Zwecken – wie etwa dem Kauf von Drogen oder Waffen oder zum Empfang von Erpressungszahlungen[265] – abzuwickeln oder um Geld zu waschen.[266]

Aus diesem Grund besteht ein hohes Interesse daran, illegale Aktivitäten, die im Zusammenhang mit Kryptowährungen oder Blockchains[267] stehen, aufzuklären. Dieses Interesse haben einerseits die Strafverfolgungsbehörden,[268] andererseits aber auch private Stellen/Personen, entweder, wenn sie

261 *Boehm/Pesch*, MMR 2014, 75 (76); *Safferling/Rückert*, MMR 2015, 788 (791); *Krause*, NJW 2018, 678 (679).

262 *Reid/Harrigan*, SPSN 2013, 197 (200f.); *Koshy/Koshy/McDaniel*, FC2014, LNCS 8437, 469 (469); *Krause*, NJW 2018, 678 (679).

263 *Safferling/Rückert*, MMR 2015, 788 (791); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1).

264 *Foley/Karlsen/Putnins*, RFS 2019, 1798 (1798).

265 *Safferling/Rückert*, MMR 2015, 788 (789). Ein Beispiel für eine Erpressung ist etwa Fall der Cyberattacke „WannaCry", bei der insgesamt 240.000 Computer gehackt und verschlüsselt wurden, bis eine Zahlung auf bestimmten Bitcoin-Adressen eingegangen waren, vgl. hierzu *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 22.

266 *Safferling/Rückert*, MMR 2015, 788 (789).

267 Siehe hierzu etwa bestimmte *Smart Contracts,* die auf der Ethereum-Blockchain abgelegt werden und als Schneeballsysteme einzuordnen sind, vgl. *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575).

268 Vgl. insoweit das vom BMBF geförderte Forschungsprojekt BITCRIME und dessen Abschlussbericht: *Böhme/Grzywotz/Pesch/Rückert/Safferling*, Prävention von Straftaten mit Bitcoins und Alt-Coins, Handlungsempfehlung zur Regulierung virtueller

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

bereits Opfer von Straftaten geworden sind und eine Aufklärung durch die Strafverfolgungsbehörden nicht ausreichend gewährleistet werden kann, oder – und vor allem – bevor sie in Crowdfunding-Projekte investieren, um deren Rechtschaffenheit vorab prüfen zu lassen.[269]

Welche Möglichkeiten es gibt, um illegale Aktivitäten im Zusammenhang mit Blockchains aufzudecken und zu verfolgen, wird im Folgenden dargestellt. Dabei wird danach differenziert, auf welcher Datengrundlage die Ermittlungen basieren, da die rechtliche Bewertung unter anderem davon abhängen wird.[270]

Denn derartige Ermittlungen können zunächst am Transaktionsregister der Blockchain ansetzen,[271] da dieses – wie bereits dargestellt[272] – öffentlich einsehbar ist und alle Transaktionen seit Beginn der jeweiligen Blockchain enthält. Insoweit ist es möglich, die Transaktionen der Blockchain auszuwerten und hierdurch bspw. zu verfolgen, wohin Zahlungen im Zusammenhang mit illegalen Aktivitäten geflossen sind. Oder die Transaktionen können systematisch dahingehend ausgewertet werden, ob es Transaktionsmuster gibt, die auf illegale Aktivitäten, wie Geldwäsche oder Betrug, hindeuten (hierzu im Einzelnen unter A.).

Ein weiterer Auswertungsansatz können die technischen Eigenschaften des *Peer-to-Peer-Netzwerks* zwischen den *nodes* sein, denn hieraus können etwa die IP-Adressen einzelner Bitcoin-Adressen ermittelt werden (hierzu im Einzelnen unter B.).

Kryptowährungen. Vgl. hierzu außerdem das EU-Forschungsprojekt TITANIUM, https://www.titanium-project.eu (letzter Abruf: 20 Dezember 2021).

269 So hat sich auch in Deutschland bereits ein Markt für derartige Untersuchungen entwickelt, vgl. insoweit die Dienste des in München ansässigen Anbieters https://www.immutableinsight.com (letzter Abruf: 20. Dezember 2021).

270 Siehe für eine abweichende Differenzierung *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1f.), die zwischen dem sog. *Clustering* und *Attribution Tagging* differenzieren. Hintergrund dieser abweichenden Differenzierung dürfte sein, dass die Autoren sich mit der Trefferwahrscheinlichkeit der dargestellten Auswertungsmöglichkeiten und deren Beweiswert im Strafverfahren auseinandersetzen.

271 Vgl. hierzu etwa *Safferling/Rückert*, MMR 2015, 788 (791).

272 Siehe hierzu oben unter Kap. 2, A.IV. m.w.N.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Darüber hinaus können die Blockchain-Daten, etwaige Auswertungsergebnisse und Daten aus dem Netzwerk mit Daten verknüpft werden, die anderweitig verfügbar sind[273] (hierzu im Einzelnen unter C.).

Zu beachten ist, dass die folgenden Auswertungs- und Ermittlungsmöglichkeiten auf Grund des schnellen technischen Wandels nicht abschließend sind. Außerdem beziehen sich die bisher entwickelten Auswertungsmöglichkeiten vorwiegend auf Bitcoin und können nicht zwangsläufig bei allen anderen Blockchain-Systemen angewendet werden. Die nachfolgenden Ausführungen dienen insoweit nur zur Darstellung, welche Auswertungen und Ermittlungen grundsätzlich möglich sind und wie diese technisch ablaufen.

A. Auswertung der Blockchain-Daten

Die unmittelbaren Blockchain-Daten können in verschiedener Art und Weise ausgewertet werden. So ist es zunächst möglich, mehrere Bitcoin-Adressen, die mit hoher Wahrscheinlichkeit von einer einzelnen Person oder Organisation kontrolliert werden, einem sog. *Entitäts-Cluster* zuzuordnen – sog. *Entitäts-Clustering*[274] (hierzu unter I.).

Außerdem kann etwa das typische Transaktionsverhalten innerhalb von Blockchains ermittelt werden, um Anomalien aufzudecken, die auf kriminelle Aktivitäten hindeuten können (hierzu unter II.).

Soweit darüber hinaus Informationen über die Hintergründe für ein bestimmtes Transaktionsverhalten bekannt sind (bspw., wenn eine bestimmte Transaktion bekanntermaßen im Zusammenhang mit Erpressungssoftware stand), kann dieses bekannte Transaktionsverhalten zunächst ausgewertet werden, um nach ähnlichen oder abweichenden Mustern innerhalb der Blockchain-Daten zu suchen (hierzu unter III.).

273 Etwa dadurch, dass ein Nutzer seine Bitcoin-Adresse in einem Forum selbst öffentlich preisgibt, indem er sie als Signatur verwendet, vgl. hierzu insbesondere *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3f.).

274 Der technische Begriff des *Clusterings* beschreibt Algorithmen, die zum Aufdecken von Ähnlichkeitsstrukturen in großen Datensätzen verwendet werden. Insoweit ist die Verwendung des Begriffs im hier benutzten Kontext nicht vollständig korrekt, wird aber im Folgenden verwendet, da die Entwickler derartiger *Clustering*-Methoden im Blockchain-Kontext diese jeweils als *Clustering* bezeichnen.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

I. Entitäts-Clustering

Eine der ersten, und die wohl am häufigsten zitierte, Möglichkeit[275] der Blockchain-Auswertungen ist das sog. *Clustering.*

Clustering ist in Informatik und Statistik zunächst einmal ein Verfahren zur Gruppierung von Daten mit ähnlichen Eigenschaften. Im Bereich des *Entitäts-Clusterings* ist es das Ziel, mehrere, verschiedene Bitcoin-Adressen zu einer sog. *Entität* zu gruppieren.[276]

Entität ist dabei eine Person oder Organisation, die eine oder mehrere Bitcoin-Adressen kontrolliert oder kontrollieren kann.[277] Zu beachten ist, dass das *Entitäts-Clustering* auf Grund von technischen Besonderheiten im Software-Protokoll bisher fast ausschließlich bei Bitcoin Anwendung findet. Entsprechende Anwendungen bei anderen Blockchains sind aktuell in Entwicklung, aber noch nicht ausgereift.[278]

Beim *Entitäts-Clustering* werden die folgenden Methoden (im Einzelnen unter 1. – 3.) unterschieden, wobei das sog. *Multi-Input-Clustering* (hierzu unter 1.) als das erfolgversprechendste im Bitcoin-Kontext gilt.[279]

1. Multi-Input-Clustering

Das sog. *Multi-Input-Clustering* beruht darauf, dass die Bitcoin-Nutzer Nutzer mehrere, verschiedene Bitcoin-Adressen haben – dies wird sogar zum Schutz der Privatsphäre von *Satoshi Nakamoto* empfohlen.[280] Aus diesem Grund haben Nutzer häufig mehrere, unterschiedliche Bitcoin-Adressen, auf denen sie jeweils Bitcoin (im Folgenden wird für die Bezeichnung

275 Siehe etwa: *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1); *Monamo/Marivate/Twala*, ISSA2016, 129 (130); *Pesch/Böhme*, DuD 2017, 93 (95); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (1f.).

276 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (127); *Pesch/Böhme*, DuD 2017, 93 (95).

277 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (3).

278 Vgl. etwa *Chan/Olmsted*, ICITST 2017, 498, die ein erstes Graphen-Modell entwickelt haben, um Transaktionen in der Ethereum-Blockchain nachzuvollziehen.

279 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

280 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6., und die Empfehlung auf: https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

der Einheit eines Bitcoin die Abkürzung „BTC“ verwendet) in unterschiedlicher Höhe empfangen haben. Will nun ein Nutzer eine Summe an BTC an eine andere Bitcoin-Adresse transferieren, deren Höhe er nur erreicht, wenn er sein Vermögen von verschiedenen Bitcoin-Adressen kombiniert, muss er von mehreren Bitcoin-Adressen, entsprechende Transaktionen weiterleiten.[281] Dabei haben dann aber unterschiedliche Absendeadressen den gleichen Empfänger.[282]

Als Beispiel:

Hat Nutzer A 20 verschiedene Bitcoin-Adressen A_1-A_{20}, die jeweils eine Transaktion mit 1 BTC erhalten haben und will Nutzer A an Nutzer B, insgesamt 2 BTC transferieren, muss er insgesamt zwei seiner empfangenen Transaktionen weiterleiten. Absendeadressen sind dann etwa A_1 und A_2, Empfangsadresse ist nur B_1. Die Absendeadressen werden als sog. *Inputs,* die Empfangsadressen als sog. *Outputs* bezeichnet. Wenn nun eine Transaktion erstellt werden soll, bei der mehrere *Inputs* kombiniert werden müssen, um eine bestimmte Höhe an BTC zu erreichen, wird regelmäßig eine einheitliche Transaktionsnachricht erstellt, in der als *Inputs* die beiden Bitcoin-Adressen A_1 und A_2 enthalten sind, als *Output* B_1.

Da der Absender dieser Transaktion über beide *private keys* – den für A_1 und A_2 – verfügen muss, um die Transaktionsnachricht zu signieren[283], kann man annehmen, dass zumindest eine Beziehung zwischen A_1 und A_2 besteht – wenn nicht sogar die gleiche Person oder Organisation hinter beiden Adressen steht.[284]

Dementsprechend ist es möglich, die Transaktionsdaten der Blockchain nach Transaktionen mit mehreren *Inputs* bei gleichem *Output* zu durchsuchen. So ist es im Beispiel möglich die Adressen A_1 und A_2 einer *Entität* zuzuordnen.[285] Wenn nun Nutzer A von den Adressen A_2 und A_3 jeweils 1

281 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

282 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

283 Siehe hierzu oben unter Kap.2, A.II.2.

284 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC ‘13 2013, 127 (133); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5; *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2).

285 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

BTC an die Adresse des Nutzers C transferiert, können auch die Adressen A_2 und A_3 der *Entität* des A zugeordnet werden.[286]

Die dieser Auswertung zugrundeliegende Annahme, dass bei mehreren *Inputs* einer Transaktion diese einer gemeinsamen *Entität* zugeordnet werden können, beruht insbesondere auch darauf, dass Nutzer von Bitcoin zur Verwaltung ihrer BTC und Bitcoin-Adressen häufig sog. *Wallets* verwenden. Dies können entweder sog. *Software-Wallets* sein oder *Online-Wallet-Anbieter*. Diese *Software-Wallets* oder *Online-Wallet-Anbieter* erleichtern die Verwaltung für die Nutzer, indem sie sowohl die Bitcoin-Adressen als auch die dazugehörigen *private keys* speichern und die Transaktionsnachrichten teilweise automatisch erstellen.[287] Bei der Erstellung der Transaktionsnachrichten verknüpft die Software dann automatisch mehrere Bitcoin-Adressen als absendende Adressen.[288]

Auf dieser Grundlage können durch die Transaktionsdaten der Blockchain mehrere Bitcoin-Adressen zu einer *Entität geclustert* werden.[289]

2. Change- und Shadow-Clustering

Zwei weitere *Entitäts-Clustering*-Methoden, die sich ebenfalls Besonderheiten der Verwendung und technische Eigenheiten von Bitcoin zu Nutze machen, sind die sog. *Change- und Shadow-Clustering*-Methoden.[290]

Wie oben dargestellt, werden im Bitcoin-System nur Transaktionen weitergeleitet.[291] Wichtig hieran ist, dass Transaktionen nur als Ganzes weitergeleitet werden können – sie können aber mehrere *Outputs* haben.[292] Da der Empfänger von BTC selten eine Transaktion in voller Höhe erhalten soll, werden häufig zwei *Outputs* definiert – einerseits der Empfänger, dem BTC tatsächlich transferiert werden sollen und eine weitere Bitcoin-Adresse, die den verbleibenden Teil – also das Wechselgeld / *Change* – erhalten

286 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).
287 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5.
288 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5.
289 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (132f.).
290 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (37).
291 Vgl. hierzu oben unter Kap.2, A.II.7 m.w.N.
292 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

soll.[293] Die sog. *Change-Adresse* ist dann die Adresse, an die das Wechselgeld transferiert wird.[294]

Hat also eine Transaktion mehrere *Outputs* kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass einer der beiden *Outputs* zur Entität des Absenders der Transaktion gehört.[295]

So kann das oben bereits erwähnte Beispiel wie folgt erweitert werden:

Wenn Nutzer A von seiner Adresse A_1 eine Transaktion an die Adressen B_1 und A_4 erstellt, kann man annehmen, dass die *Entität* hinter A_1 entweder auch über B_1 oder A_4 verfügen kann.[296] Transferiert nun die Bitcoin-Adresse A_1 häufiger BTC an die Bitcoin-Adresse A_4 und eine jeweils variierende Bitcoin-Adresse, kann man annehmen, dass A_1 und A_4 zu derselben Entität gehören.[297] So ist es möglich, mit Hilfe des sog. *Change-Clusterings*, die Adressen A_1 und A_4 der Entität des A zuzuordnen.

Die *Change-Clustering*-Methode kann wiederum auf Grund einer technischen Besonderheit der *Online- und Software-Wallets* um eine weitere Auswertungsmöglichkeit erweitert werden. Denn diese erzeugen für den Empfang von Wechselgeldtransaktionen regelmäßig jeweils neue Bitcoin-Adressen, die dem alleinigen Zweck dienen bei einer bestimmten Transaktion das Wechselgeld zu empfangen.[298] Der Nutzer bekommt hiervon teilweise gar nicht erst etwas mit. Diese Wechselgeld-Adressen, die nur zum einmaligen Empfang von Wechselgeld verwendet werden, werden als sog. *Shadow-Adressen* bezeichnet.[299]

Dementsprechend ist es zusätzlich möglich, die Blockchain-Daten nach entsprechenden Transaktionen zu durchsuchen, deren Empfänger Bitcoin-

293 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

294 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

295 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

296 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (43).

297 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (43).

298 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

299 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Adressen sind, die nur dem einmaligen Empfang von Transaktionen dienen – dies ist das sog. *Shadow-Clustering*.[300]

3. Behavioural Clustering

Eine dritte *Entitäts-Clustering*-Methode ist das sog. *Behavioural Clustering*, dessen Erfolgsaussichten bisher allerdings noch nicht ausreichend geklärt sind. Beim *Behavioural Clustering* werden die Blockchain-Daten nach Mustern in Form von zeitlichen Abläufen und Strukturen der Transaktionen durchsucht.[301] Hierdurch sollen Transaktionen mit ähnlichen Mustern gefunden werden, um diese einer *Entität* zuordnen zu können.[302] Hintergrund dieser Methode ist die Annahme, dass Bitcoin-*Wallets* mit einem herkömmlichen Bankkonto vergleichbar sind und insoweit nach Verhaltensmustern der dahinterstehenden natürlichen Personen durchsucht werden können.[303]

4. Probleme der Entitäts-Clustering-Methoden

Problematisch an den soeben dargestellten Methoden des *Entitäts-Clusterings* ist, dass sie jeweils immer auf Annahmen beruhen, wie Transaktionen typischerweise ablaufen.[304] Dabei kann der typische Ablauf von Transaktionen sowohl einen technischen als auch einen persönlichen Hintergrund haben.[305]

Problematisch ist dies deshalb, weil sich der typische Ablauf von Transaktionen ändern kann und die Annahmen insoweit nicht allgemeingültig sind – insbesondere vor dem Hintergrund, dass sich das typische Transaktionsverhalten gerade auch wegen der entwickelten Auswertungsmöglichkeiten ändert.[306]

---

300 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133f.); *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 5f.

301 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

302 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

303 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500).

304 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (3).

305 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (3).

306 So enthalten etwa die technischen Darstellungen der *Clustering* Methoden teilweise auch Empfehlungen, wie das Bitcoin-Protokoll angepasst werden kann, damit die

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

So gehen beispielsweise *Androulaki/ Karame/ Roeschlin/ Scherer/ Capkun*[307] beim *Change-Clustering* noch davon aus, dass Transaktionen, die mehrere *Outputs* haben, häufig darauf hindeuten, dass eine der beiden *Outputs* eine *Change*-Adresse ist, da Transaktionen mit mehreren Empfängern, bei denen alle *Outputs* gleichberechtigte Empfänger sind, sehr selten sind.[308]

Gerade diese Annahme wird bereits von *Meiklejohn/ Pomarole/ Jordan/ Levchenko/ McCoy/ Voelker/ Savage* dahingehend kritisiert, dass derartige Transaktionen mittlerweile keine Seltenheit mehr seien, da etwa sog. *Mining-Pools*[309] ihre Ausschüttungen in dieser Weise vornehmen würden.[310]

Ähnliches gilt für die *Multi-Input-Clustering*-Methode. Denn um die Transaktionsverläufe zu verschleiern und *Entitäts-Clustering*-Methoden zu verhindern, gibt es sog. *Mixing-Services* – wie etwa den bekanntesten *CoinJoin*.[311] Vereinfacht erstellen hierbei mehrere unterschiedliche Nutzer gemeinsam eine Transaktionsnachricht, in der sie ihre BTCs jeweils untereinander weiterversenden.[312] Hierdurch wird die Annahme des *Multi-Input-Clusterings* durchbrochen, dass bei einer Transaktion, die von mehreren unterschiedlichen Bitcoin-Adressen signiert wird, alle absendenden Adressen einer einheitlichen Entität zugeordnet werden können.[313]

Um derartige *CoinJoin*-Transaktionen identifizieren zu können, ist mittlerweile aber wiederum eine neue Auswertungsmethode entwickelt worden.[314] Diese Auswertungsmethode beruht nun auf der Eigenheit der *Coin-*

---

jeweils dargestellte Auswertung nicht mehr möglich ist, vgl. hierzu etwa *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (47ff.).

307 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42).

308 *Androulaki/Karame/Roeschlin/Scherer/Capkun*, FC2013, LNCS 7859, 34 (42); *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133).

309 *Mining-Pools* sind *Full-nodes*, die sich zum Fortschreiben der Blockchain zusammenschließen, um durch die so erhöhte Rechenkapazität eine höhere Ausschüttung an Bitcoin zu erreichen. Siehe hierzu ausführlich m.w.N. *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 48; *Hofert*, Regulierung der Blockchains, S. 150f.

310 *Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage*, IMC '13 2013, 127 (133). Ähnlich auch *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 6f., der insbesondere darauf abstellt, dass die Erfolgswahrscheinlichkeit immer auch davon abhängt, wie die verwendete Wallet technisch funktioniert.

311 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

312 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

313 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 7.

314 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3f.); *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (2f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Join-Transaktionen. Denn bei den *CoinJoin*-Transaktionen haben viele verschiedene Transaktionen die gleiche *In-* und *Output* Höhe und laufen ungefähr zu einer ähnlichen Zeit habe.[315] Auch diese Transaktionen weisen insoweit Besonderheiten auf, nach denen die Blockchain-Daten durchsucht werden können.[316]

5. Zwischenergebnis

Festzuhalten bleibt, dass es möglich ist, mehrere verschiedene Bitcoin-Adressen einer Person oder Organisation zuordnen zu können, indem die unmittelbaren Blockchain-Daten ausgewertet werden. Die jeweiligen Methoden nutzen dabei Eigenschaften von typischem Transaktionsverhalten aus. Dabei verändert sich zwar das Verständnis davon, wodurch sich typisches Transaktionsverhalten auszeichnet, diese Grundannahmen können aber von den technischen Auswertungsmethoden jeweils entsprechend angepasst werden.

II. Aufdecken von bestimmtem Transaktionsverhalten

Ähnlich funktioniert auch das Aufdecken von bestimmtem Transaktionsverhalten. Auch in diesem Kontext werden die Blockchain-Daten nach bestimmten Transaktionsmustern ausgewertet, die etwa auf Geldwäsche oder andere illegale Aktivitäten hindeuten (können).

So haben zum Beispiel *Hirshman/ Huang/ Macke* einen Algorithmus entwickelt, der auf maschinellem Lernen basiert und zunächst die Transaktionsdaten der Blockchain nach typischem und auffälligem Transaktionsverhalten analysiert.[317] In diesem Zusammenhang war etwa ein auffälliges Transaktionsverhalten, dass große Summen BTC, die anfänglich nur einer Bitcoin-Adresse zugeordnet waren, in einem ersten Schritt auf viele einzelne Bitcoin-Adressen verteilt werden und anschließend über viele Umwege wieder zu einer einzelnen Bitcoin-Adresse zusammengeführt wurden.[318]

315 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3f.).
316 *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (5).
317 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (1).
318 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (2).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Ein derartiges Transaktionsverhalten lässt den Rückschluss auf Geldwäsche zu.[319]

Ein ähnliches Ziel verfolgten *Pham/ Lee*, die ebenfalls die Transaktionsdaten der Blockchain nach auffälligen Transaktionen durchsuchten, da diese in herkömmlichen Finanzsystemen regelmäßig auf illegale Aktivitäten hindeuteten.[320]

Ein Problem dieser Methoden ist häufig, dass sie nur die Daten innerhalb der Blockchain auswerten und insoweit nicht vergleichen können, was typisches (bzw. typischerweise legales) und was auffälliges (bzw. typischerweise illegales) Transaktionsverhalten ist.[321]

III. Vergleich mit bekanntem Transaktionsverhalten

Dieses Problem kann überwunden werden, wenn die Hintergründe von einzelnen Bitcoin-Adressen/-Entitäten, Transaktionen oder Transaktionsmustern bekannt sind und diese bekannten Muster dann mit anderem Transaktionsverhalten verglichen werden können.

1. Betrugs-Transaktionen

So ist es etwa möglich, die Bitcoin-Blockchain nach Transaktionen zu durchsuchen, die im Zusammenhang mit Betrug stehen.[322]

Hierzu wertet ein sog. *Classifier* zunächst das typische Transaktionsverhalten von Transaktionen aus, die bekanntermaßen im Zusammenhang mit Betrug standen.[323] Der *Classifier* ermittelt auf dieser Grundlage dann Eigenschaften von typischem betrügerischem Transaktionsverhalten.[324] In einem zweiten Schritt durchsucht dann dieser *Classifier* die Blockchain-Daten nach Transaktionsmustern, die ähnliche Eigenschaften aufweisen.[325]

---

319 *Hirshman/Huang/Macke*, Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 1 (5).
320 *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1).
321 *Pham/Lee*, arXiv:1611.03941 [cs.LG] 2016, 1 (1).
322 *Monamo/Marivate/Twala*, ISSA 2016, 129 (129).
323 *Monamo/Marivate/Twala*, ISSA 2016, 129 (130f.). Ein *Classifier* ist ein Algorithmus, der typische Eigenschaften in einem Datensatz ermittelt.
324 *Monamo/Marivate/Twala*, ISSA 2016, 129 (130f.).
325 *Monamo/Marivate/Twala*, ISSA 2016, 129 (131).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Ein ähnliches Verfahren wurde auch verwendet, um bei der Ethereum-Blockchain betrügerische *Wallets* und Transaktionen zu ermitteln.[326] Hierzu wurden ebenfalls verschiedene *Classifier* eingesetzt, die in einem ersten Schritt das Transaktionsverhalten von bekannten[327] betrügerischen *Wallets* und Transaktionen auswerteten.[328] In einem zweiten Schritt wurde die Ethereum-Blockchain wiederum nach Transaktionsverhalten durchsucht, das den so ermittelten Eigenschaften ähnlich war.[329]

2. Transaktionen bei Schneeballsystemen

Ein ähnliches Modell entwarfen *Chen/ Zheng/ Ngai/ Zheng/ Zhou*[330], die eine Auswertungsmöglichkeit der Ethereum-Blockchain entwickelten, um Schneeballsysteme aufzudecken.

Da die Etherum-Blockchain – wie oben dargestellt[331] – nicht nur eine Kryptowährung ist, sondern eine entwicklungsoffene Blockchain, die gerade auch für die Entwicklung und Abwicklung von *Smart Contracts* genutzt werden kann, werden auf der Ethereum-Blockchain u.a. auch *Smart Contracts* von Schneeballsystemen abgelegt.[332] Diese laufen dann ähnlich wie herkömmliche Schneeballsysteme ab – nur automatisiert.[333]

Ziel der Methode von *Chen/ Zheng/ Ngai/ Zheng/ Zhou* war es, derartige *Smart Contracts* aufzudecken.[334] Hierzu wurden zunächst die Programmcodes von *Smart Contracts* ausgewertet, soweit diese verfügbar waren.[335] So konnte ermittelt werden, welche *Smart Contracts* nach einem Schneeball-

326 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (1).
327 Die Grundlage der „bekannten", betrügerischen *Wallets* und Transaktionen waren die Angaben von https://etherscan.io (letzter Abruf: 20. Dezember 2021), die u.a. Informationen zu einzelnen Ethereum-Adressen bzw. Ethereum-Wallets bereitstellen. Unklar ist in diesem Zusammenhang allerdings, auf welcher Grundlage diese Angaben basieren. Vgl. *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (4).
328 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (5ff.).
329 *Ostapowicz/Zbikowski*, arXiv:1908.07886 [cs.CR] 2019, 1 (6ff.).
330 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575ff.).
331 Vgl. hierzu oben unter Kap.2, C.II.2.
332 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37576)., die als Beispiel etwa den *Smart Contract* Rubixi benennen.
333 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37579)., die auch beispielhaft den Programmcode eines Schneeballsystems abbilden und darstellen.
334 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37575).
335 Es konnten nur solche Programmcodes ausgewertet werden, die öffentliche verfügbar waren, da eben nicht alle Programmcodes sog. *Open-Source-Codes* sind. Vgl. hierzu *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37579f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

system funktionieren.[336] Typischerweise legt etwa ein Schneeballsystem-Programmcode die Bedingung fest, dass Beträge an diejenigen ausgezahlt werden, die zuerst einen Betrag an den *Smart Contract* transferieren.[337]

Anschließend wurde wiederum das Transaktionsverhalten der so ermittelten *Schneeball-Smart Contracts* ausgewertet – insbesondere konnte in diesem Fall das Transaktionsverhalten eines *Schneeball-Smart Contracts* mit einem *Nicht-Schneeball-Smart Contract* verglichen werden und so Unterschiede und Eigenschaften des typischen Transaktionsverhaltens ermittelt werden.[338] Auffällige Eigenschaften eines *Schneeball-Smart Contracts* waren etwa, die Rücküberweisung an Nutzer, die zuerst einen Betrag an den *Smart Contract* transferiert hatten, oder ein Ungleichgewicht von Zahlungsein- und -ausgängen.[339]

Die so ermittelten, typischen Eigenschaften der Transaktionen von *Schneeball-Smart Contracts* wurden dann wiederum in einen *Classifier* implementiert, damit dieser dann die Ethereum-Blockchain nach vergleichbarem Transaktionsverhalten durchsuchen konnte.[340]

Auf Grund dieser Methode konnten insgesamt 394 *Smart Contracts* der Ethereum-Blockchain ermittelt werden, deren Transaktionsverhalten auf ein Schneeballsystem hindeutet.[341]

3. Kategorisierung von Entitäten – Labelling

Eine weitere Auswertungsmöglichkeit ist das sog. *Labelling*. Ziel des *Labellings* ist es, Bitcoin-Entitäten danach zu kategorisieren, ob und welchen Service sie im Zusammenhang mit dem Bitcoin-System anbieten.[342]

Hierzu haben etwa *Zola/ Eguimendia/ Bruse/ Urrutia* ein stufenweises *Classifier*-Verfahren (im Folgenden als *CML* bezeichnet) entwickelt.[343] Das *CML*-Verfahren soll Bitcoin-Entitäten in eine der folgenden sechs Kategorien einordnen:

336 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37580f.).
337 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37581).
338 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37581f.).
339 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37580).
340 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37583ff.).
341 *Chen/Zheng/Ngai/Zheng/Zhou*, IEEE Access 2019, 37575 (37585).
342 Vgl. hierzu *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1).
343 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1ff.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

- Exchange-Services = Anbieter eines Wechsels von Fiat-Geld in Bitcoin und andersherum
- Services = Unternehmen, die Bitcoin als Zahlungsmittel entgegennehmen
- Gambling-Services = Glücksspielanbieter
- Mining-Pools[344] = Zusammenschlüsse von Rechnern, um Erträge beim Bitcoin-Mining zu steigern
- Mixing Services[345] = Anbieter, die Rückverfolgbarkeit von Transaktionen erschweren
- Marketplace = Warenhandelsplatz

Hierzu werden zunächst die Bitcoin-Adressen zu *Entitäten geclustert*.[346] Im Anschluss werten mehrere *Classifier* die Transaktionsdaten von insgesamt 311 Bitcoin-*Entitäten* aus, bei denen davon ausgegangen wird, dass sie einen dieser sechs Services anbieten. Grundlage der Annahme sind die Angaben von *„WalletExplorer"*[347]. Die *Classifier* ermitteln auf der Grundlage dieser Daten wiederum typische Eigenschaften der *Entitäten*, die einen der sechs Services anbieten.

Basierend auf den so ermittelten typischen Eigenschaften des Transaktionsverhaltens können nun die Blockchain-Daten nach vergleichbaren Mustern durchsucht werden, um so Bitcoin-*Entitäten* in eine der sechs genannten Kategorien einzuordnen. Dabei verspricht das Verfahren eine Treffer-Genauigkeit von bis zu 100%.[348]

Ein ähnliches Verfahren haben *Harlev/ Sun Yin/ Langenheldt/ Mukkamala/ Vatrapu*[349] entwickelt, mit dem Unterschied, dass die *Entitäten* in die folgenden, zusätzlichen Kategorien eingeordnet wurden[350]:

- Hosted-Wallet: Anbieter, die es Nutzern ermöglichen, Bitcoin zu nutzen, ohne selbst *node* des *Peer-to-Peer-Netzwerks* zu werden
- Merchant-Service: Zahlungsabwicklungsdienstleister, die etwa die Abwicklung von Bitcoin-Zahlungen für Online-Shops ermöglichen

344 Siehe hierzu bereits oben unter Kap. 3, A.I.
345 Siehe hierzu etwa die ausführliche Darstellung zum Mixing-Service *CoinJoin* unter Kap. 3, A.I.4. m.w.N.
346 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (4f.). Siehe zum *Entitäten-Clustering* bereits ausführlich oben unter Kap. 3, A.I.
347 https://www.walletexplorer.com (letzter Abruf: 20. Dezember 2021).
348 *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (11).
349 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497ff.).
350 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3500f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

- Tor-Market: Handelsplattformen, die nur über einen *Tor-Browser*[351] erreicht werden können und auf denen überwiegend illegale Güter gehandelt werden
- Ransomware: Abwicklung von (Erpressungs-)Zahlungen im Fall von Schadsoftware
- Other: *Entitäten,* die zwar identifiziert wurden, die aber keiner der genannten Kategorien entsprechen, bspw. die Spendenadresse von Wikileaks

Das *Labelling* kann insoweit insgesamt dazu verwendet werden, um die Hintergründe von Transaktionen und den mit ihnen verfolgten Zweck besser nachzuvollziehen.[352]

IV. Zwischenergebnis

Die in der Blockchain enthaltenen Transaktionsdaten bieten verschiedenste Ansatzpunkte zur Auswertung.

So können eine Vielzahl von Bitcoin-Adressen einer einzelnen *Entität* zugeordnet werden. Außerdem können die Transaktionen insgesamt nach typischem und auffälligem Transaktionsverhalten analysiert werden, bei denen bestimmte Auffälligkeiten auf illegale Aktivitäten hindeuten können. Derartige Auffälligkeiten können noch präziser ermittelt werden, wenn die Hintergründe von einzelnem Transaktionsverhalten bekannt sind, um diese als Vergleichsmaßstab heranzuziehen.

Die beschriebenen Auswertungsmöglichkeiten unterliegen allerdings einem ständigen Wandel – sowohl des Nutzerverhaltens als auch der technischen Gegebenheiten – sodass die dargestellten Auswertungsmöglichkeiten nicht abschließend oder allgemeingültig sind.

B. Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens

Zusätzliche Erkenntnisse – insbesondere über die Identitäten von Bitcoin-Adressen und -*Entitäten* – können sich durch die Auswertung des Netz-

351 Zur Funktionsweise des *Tor-Browsers*, der es für den Nutzer ermöglicht, seine IP-Adresse zu verschleiern, im Einzelnen unter Kap. 3, B.II.1.

352 *Harlev/Sun Yin/Langenheldt/Mukkamala/Vatrapu*, HICSS 2018, 3497 (3497); *Zola/Eguimendia/Bruse/Urrutia*, arXiv:1910.06560 [cs.CR] 2019, 1 (1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

werkverhaltens und der Netzwerkverbindungen der Nutzer im Blockchain-Netzwerk ergeben. Denn, wie oben dargestellt[353], sind die *nodes* zu einem *Peer-to-Peer-Netzwerk* zusammengeschlossen, um eine unmittelbare Kommunikation untereinander zu ermöglichen.[354] Dieser unmittelbare Zusammenschluss bietet aber auch Auswertungsmöglichkeiten.

So können etwa die IP-Adressen einzelner Bitcoin-Adressen durch das Weiterleitungsverhalten von Transaktionsnachrichten im Netzwerk ermittelt werden (hierzu unter I.). Ebenso können die IP-Adressen sowohl durch Überwachung des Datenverkehrs (hierzu unter II.) als auch durch sog. *Bloom-Filter-Attacks* (hierzu unter III.) ermittelt werden.

I. Grundsatz – Auswertung der Verbreitung von Transaktionsnachrichten

Eine im Jahr 2011 entwickelte Möglichkeit, die IP-Adresse einer Bitcoin-Adresse zu ermitteln, bestand darin, sich mit allen *Full-nodes* des Bitcoin-Netzwerks gleichzeitig zu verbinden.[355] Da derjenige *node*, der eine Transaktionsnachricht erstellt und versendet, diese auch als erster ins Netzwerk versendet, konnte man davon ausgehen, dass die IP-Adresse des ersten Absenders auch die des Erstellers der Transaktionsnachricht ist.[356] Da der Absender einer Transaktionsnachricht diese auch entsprechend mit seinem *private key* signieren muss[357], konnte man annehmen, dass der Ersteller der Transaktionsnachricht auch der Inhaber der absendenden Bitcoin-Adresse war.[358] Diese Annahme muss mittlerweile nicht mehr unbedingt zutreffen. Denn auf Grund der vielzähligen kommerziellen *Online-Wallet-Anbieter* ist es für Bitcoin-Nutzer nicht mehr notwendig, selbst *node* des Bitcoin-Netzwerkes zu werden.[359]

353 Siehe hierzu oben unter Kap. 2, A.III.1.a) m.w.N.
354 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Hofert*, Regulierung der Blockchains, S. 17.
355 *Reid/Harrigan*, SPSN 2013, 197 (218); *Feld/Schönfeld/Werner*, PCS. 2014, 1121 (1122f.); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
356 *Reid/Harrigan*, SPSN 2013, 197 (218); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
357 Siehe hierzu ausführlich oben unter Kap. 2, A.II.2.
358 *Reid/Harrigan*, SPSN 2013, 197 (218); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
359 *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

II. Das Tor-Netzwerk – IP-Adressen-Verschleierung und Auswertungsmöglichkeit

Um die soeben beschriebene Ermittlung von IP-Adressen zu verhindern, verwenden viele Bitcoin-Nutzer den sog. *Tor-Browser*, durch den IP-Adressen über das *Tor-Netzwerk* verschleiert werden können.[360]

Allerdings ist es unter bestimmten Umständen trotzdem möglich, IP-Adressen von Nutzern zu ermitteln, ebenso wie möglicherweise sogar deren Datenverkehr auszuwerten (hierzu sogleich unter 2., 3.). Hierzu werden technische Besonderheiten des Bitcoin-Netzwerk-Protokolls und des *Tor-Netzwerks* ausgenutzt. Deshalb ist zunächst ein grundsätzliches Verständnis der technischen Funktionsweise des *Tor-Netzwerks* erforderlich.

1. Technische Funktionsweise des Tor-Netzwerks

Das *Tor-Netzwerk* ist allgemein eine Möglichkeit zur Anonymisierung des Datenverkehrs im Internet.[361] Um eine solche Anonymisierung zu erreichen, stellen Freiwillige ihre Rechner dem Netzwerk als Server zur Verfügung.[362] Dies sind die sog. *Relays*, die den Datenverkehr der Tor-Nutzer so weiterleiten, dass er nur noch schwer nachvollziehbar ist.[363]

Ein Nutzer, der seinen Datenverkehr anonymisieren möchte, muss den sog. *Tor-Browser* herunterladen.[364] Wird dieser für Internetkommunikation verwendet, lädt der *Tor-Browser* sich zunächst eine Liste aller verfügbaren *Relays* von einem zentralen Verzeichnisserver herunter.[365] Anschließend wählt er eine zufällige sog. *Route* von insgesamt drei *Relays* aus, über die die Kommunikation ablaufen soll.[366] Die *Relays* werden als *Guard (1. Relay), Middle (2. Relay), Exit (3. Relay)* bezeichnet.[367] Dabei kennen die

360 *Reid/Harrigan*, SPSN 2013, 197 (218); *Feld/Schönfeld/Werner*, PCS. 2014, 1121 (1122f.); *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2111).
361 *Krause*, NJW 2018, 678 (678).
362 *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
363 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (128).
364 *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
365 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (128); *Owen/Savage*, GCIG No. 20, 2015, 1 (1).
366 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
367 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Relays untereinander jeweils nur den vorangegangenen und den nachfolgenden *Relay* und die Kommunikation untereinander wird verschlüsselt.[368]

Der typische Zugriff – etwa auf die Google-Seite – läuft nun über die Umwege dieser drei *Relays* ab. So kann etwa der Google-Server, auf den zugegriffen wird, nur die IP-Adresse des *Exit-Relays* als diejenige erkennen, die auf die Google-Seite zugreift.[369]

Genauso läuft die Verbindung zum *Peer-to-Peer-Netzwerk* von Bitcoin über das *Tor-Netzwerk* ab, sodass für die *nodes*, mit dem der Nutzer sich verbindet, nur die IP-Adresse des *Exit-Relays* sichtbar ist.

So ist es für Nutzer möglich, ihre eigene IP-Adresse zu verbergen.

2. IP-Adressen-Ermittlung trotz des Tor-Netzwerks

Um trotzdem die oben beschriebene Verbreitung von Transaktionsnachrichten auswerten zu können und so die IP-Adressen von Bitcoin-Adressen ermitteln zu können, haben *Biryukov/ Khovratovich/ Pustogarov*[370] die oben beschriebene Auswertungsmöglichkeit erweitert. Diese Erweiterung basiert darauf, dass eine Verbindung mit Bitcoin-Netzwerk über das *Tor-Netzwerk* verhindert wird.[371]

Um dies zu erreichen, wird der sog. *Denial-of-Service*-Schutz (kurz: *DoS*) des Bitcoin-Netzwerks ausgenutzt.[372] *Denial-of-Service*-Attacken sind typische Cyberangriffe, bei denen ein Netzwerk absichtlich so überlastet wird, dass es nicht mehr verfügbar ist. Dies funktioniert regelmäßig dadurch, dass unzählig viele Anfragen an ein Netzwerk gestellt werden, unter denen dann das Netzwerk zusammenbricht.

Damit das Bitcoin-Netzwerk nicht durch eine *DoS*-Attacke überlastet wird, sieht das Bitcoin-Protokoll vor, dass jeder *node* eine Liste der IP-Adressen anlegt, mit denen er verbunden war und diese nach einem Strafpunktesystem bewertet, wenn sie „falsche“[373] Nachrichten versenden.[374] „Falsche“ Nachrichten sind etwa Transaktionsnachrichten ohne Inhalt oder

368 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
369 *Owen/Savage*, GCIG No. 20, 2015, 1 (1); *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (124).
370 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (1ff.).
371 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
372 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).
373 Übersetzung des englischen Begriffs „malformed“.
374 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

neue Blöcke ohne Inhalt. Erreicht nun eine bestimmte IP-Adresse eine bestimmte Höhe an Strafpunkten, wird sie für 24 Stunden für das Netzwerk gesperrt.[375]

Diesen Schutzmechanismus des Bitcoin-Netzwerks machen sich *Biryukov/ Khovratovich/ Pustogarov* zu Nutze, indem sie sich zunächst selbst über das *Tor-Netzwerk* mit anderen Bitcoin-*nodes* verbinden.[376] Dabei erkennen dann die Bitcoin-*nodes* nur die IP-Adresse des jeweiligen *Exit-relays* des *Tor-Netzwerks* als die IP-Adresse des verbundenen *nodes*.[377] Anschließend versenden *Biryukov/ Khovratovich/ Pustogarov* über diese Verbindung leere Transaktionsnachrichten an die verbundenen *nodes*, sodass die IP-Adressen der *Exit-relays* für eine weitere Verbindung mit dem Bitcoin-Netzwerk für 24 Stunden gesperrt werden.[378]

So kann verhindert werden, dass andere *nodes* sich über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbinden und so ihre IP-Adresse verschleiern. So können weiterhin die tatsächlichen IP-Adressen der Ersteller von Transaktionsnachrichten nach dem oben beschreibenen Verfahren[379] ermittelt werden.

Um die Ermittlung von IP-Adressen durch Auswertung der Verbreitung von Transaktions-nachrichten zu verhindern, wurde nach der Veröffentlichung der Methode von *Biryukov/ Khovratovich/ Pustogarov* die Verbreitung von Transaktionsnachrichten im Bitcoin-Protokoll entsprechend angepasst.[380] Allerdings soll auch das so angepasste Bitcoin-Protokoll Schwächen und Angriffsmöglichkeiten haben.[381]

3. Auswertung des Datenverkehrs

Die soeben dargestellte Methode, haben *Biryukov/ Pustogarov*[382] weiterentwickelt und hierbei nicht nur den *DoS*-Schutz des Bitcoin-Protokolls ausgenutzt, sondern auch Eigenheiten des *Tor-Netzwerkes* selbst, um den

375 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (3).
376 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
377 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
378 *Biryukov/Khovratovich/Pustogarov*, arXiv:1405.7418 [cs.CR] 2014, 1 (4f.).
379 Siehe hierzu unter Kap. 3, B.I.
380 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3).
381 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (3) m.w.N.
382 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (122ff.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Datenverkehr der *nodes,* die über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbunden sind, auszuwerten.[383]

Hierzu haben *Biryukov/ Pustogarov* zunächst eigene Bitcoin-*nodes* mit dem Bitcoin-Netzwerk verbunden und zusätzlich eigene *Tor-Exit-Relays* für das *Tor-Netzwerk* zur Verfügung gestellt.[384] Im Anschluss haben sich *Biryukov/ Pustogarov* selbst über *Tor-Exit-Relays,* die nicht von ihnen zur Verfügung gestellt wurden, mit Bitcoin-*nodes* verbunden, die nicht unter ihrer Kontrolle standen. Über diese Verbindung wurden dann, wie oben bereits dargestellt, wieder „falsche" Nachrichten an diese Bitcoin-*nodes* versendet.[385]

So konnten alle *Tor-Exit-Relays,* die nicht unter der Kontrolle von *Biryukov/ Pustogarov* standen, vom Bitcoin-Netzwerk gesperrt werden.[386] Wollte sich ein Nutzer nun über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbinden, musste er hierzu zwangsläufig einen der *Exit-Relays* wählen, die *Biryukov/ Pustogarov* bereitgestellt hatten.[387] So konnte der Datenverkehr eines Nutzers, der sich über das *Tor-Netzwerk* mit dem Bitcoin-Netzwerk verbunden hat, aufgezeichnet werden.[388] Zusätzlich haben *Biryukov/ Pustogarov* teilweise auch einzelne *Guard-Relays* für das *Tor-Netzwerk* bereitgestellt, sodass auch die IP-Adresse des verbundenen Nutzers ermittelt werden konnte und mit Bitcoin-Adressen in Verbindung gebracht werden konnte.[389]

III. Bloom-Filter-Attacks

Eine weitere Möglichkeit, um Bitcoin-Adressen und Wallets mit IP-Adressen zu verknüpfen, sind die sog. *Bloom-Filter-Attacks*.[390] Hierbei wird die technische Eigenheit der sog. *Bloom-Filter* ausgenutzt, die bei sog. *Simpli-*

383 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (125f.).
384 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (125).
385 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
386 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
387 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
388 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126).
389 *Biryukov/Pustogarov*, arXiv:1410.6079 [cs.CR] 2015, 122 (126f.).
390 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (326ff.); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9ff.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

fied Payment Verification Clients (im Folgenden als *SPV-Clients* bezeichnet) eingesetzt werden.[391]

Hintergrund der *SPV-Clients* ist die große Datenmenge, die bei der Teilnahme am Bitcoin-Netzwerk versandt, empfangen und gespeichert werden muss.[392] Da auch Bitcoin das Ziel verfolgt, ein einfach verwendbares Zahlungsmittel und -system anzubieten, ist diese große Datenmenge hinderlich – insbesondere, wenn Bitcoin auch als mobile Zahlungsmethode verwendet werden soll. Aus diesem Grund gibt es den sog. *SPV-Client*, der mit einer geringeren Datenmenge auskommt.[393] Dieser verbindet sich mit einem *Full-node* und hinterlegt bei ihm einen sog. *Bloom-Filter*, in dem die *public keys* und Bitcoin-Adressen hinterlegt sind, die für den Nutzer eines *SPV-Clients* relevant sind – dies sind regelmäßig die *public keys* und Bitcoin-Adressen des jeweiligen Nutzers.[394]

Ein *Bloom-Filter* ist dabei eine Datenstruktur, die über *Hashfunktionen* einen schnellen Abgleich ermöglicht, ob bestimmte Daten in einer Datenstruktur enthalten sind.[395] Dabei werden *Bloom-Filter* danach bewertet, wie hoch ihre Falsch-Positiv-Rate ist.[396] Im Fall von Bitcoin *SPV-Clients* werden *Bloom-Filter* mit einer Falsch-Positiv-Rate von 0,0146% verwendet.[397]

Wenn nun der *Full-node* neue Transaktionen von anderen *nodes* empfängt, fragt er beim *Bloom-Filter* ab, ob die *public keys* und Bitcoin-Adressen der neuen Transaktionen im *Bloom-Filter* enthalten sind.[398] Nur wenn das der Fall ist, leitet er die relevanten Transaktionsnachrichten an den *SPV-Client* weiter.[399] Dieser kann dann die Transaktionen verifizieren, wenn sie etwa in seiner *Wallet* enthalten sind.[400]

391 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (326); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
392 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327f.); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.
393 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 10.
394 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.
395 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9.
396 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9.
397 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 10.
398 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327).
399 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (327).
400 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 9f.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Die Ermittlungsmöglichkeit besteht nun für den *Full-node*, mit dem sich ein *SPV-Client* verbindet.[401] Da in der Bitcoin-Blockchain alle bisher verwendeten *public keys* und Bitcoin-Adressen enthalten sind, ist es für einen *Full-node* möglich, alle *public keys* und Bitcoin-Adressen des Bitcoin-Netzwerks beim *Bloom-Filter* abzufragen.[402] Da sowohl *public keys* als auch Bitcoin-Adressen bei dem *Bloom-Filter* hinterlegt sind, sinkt die Wahrscheinlichkeit, dass ein doppelt-falsch-positives Ergebnis ermittelt wird.[403] Wenn also sowohl *public key* als auch Bitcoin-Adresse als positives Ergebnis vom *Bloom-Filter* angegeben werden, ist es äußerst wahrscheinlich, dass die Bitcoin-Adressen sich tatsächlich in der *Wallet* des *SPV-Clients* befinden.[404]

Da außerdem eine Netzwerkverbindung zwischen *SPV-Client* und *Full-node* aufgebaut werden muss, in der zur Kommunikation auch die IP-Adresse des *SPV-Clients* übermittelt werden muss, können insoweit Bitcoin-Adressen einer IP-Adresse zugeordnet werden, sofern der *SPV-Client* nicht über das *Tor-Netzwerk* mit dem *Full-node* verbunden ist.[405]

IV. Zwischenergebnis

Die *Peer-to-Peer*-Verbindung des Bitcoin-Netzwerks bietet die Möglichkeit die IP-Adressen von Bitcoin-Nutzern zu ermitteln und diese unter Umständen einer Bitcoin-Adresse zuzuordnen.

Zwar gibt es etwa durch das *Tor-Netzwerk* die Möglichkeit IP-Adressen zu verschleiern, allerdings beinhalten auch diese Möglichkeiten ihre Schwachstellen, die eine erweiterte Auswertungsmöglichkeit zur Folge haben können.

Eine weitere Möglichkeit zur Ermittlung von IP-Adressen sind die bei *SPV-Clients* verwendeten *Bloom-Filter*.

Zu berücksichtigen ist aber auch hier, dass die vorgestellten Ermittlungsmöglichkeiten immer von den jeweiligen technischen Funktionsweisen und dem Nutzerverhalten abhängen und auf Grund der fortwährenden Anpassung der technischen Funktionsweise nicht abschließend oder allgemeingültig sind.

401 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (328); *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
402 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
403 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
404 *Nick*, Data-Driven De-Anonymization in Bitcoin, S. 11.
405 *Gervais/Karame/Gruber/Capkun*, ACSAC '14, 326 (328).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

C. Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten

Neben den bereits dargestellten Auswertungsmöglichkeiten ist es außerdem möglich, die Blockchain-Daten mit anderweitig verfügbaren Daten zu verknüpfen, um hieraus weitergehende Erkenntnisse über die Identitäten der Bitcoin Nutzer und deren Transaktionsverhalten zu erhalten.

So kann etwa das Internet – insbesondere Internetforen – nach Bitcoin-Adressen durchsucht werden, die von Nutzern oder Dritten veröffentlicht wurden (hierzu unter I.). Außerdem können etwa Daten von Drittanbieter-Cookies ausgewertet werden (hierzu unter II.) und bei blockchain-basierten *Internet-of-Things*-Anwendungen (im Folgenden als *IoT* bezeichnet) etwa Standortdaten ausgewertet werden (hierzu unter III.).

I. Durchsuchen des Internets nach Bitcoin-Adressen

Vor allem in der Anfangszeit von Bitcoin und anderen Kryptowährungen veröffentlichten Bitcoin-Nutzer ihre eigenen Bitcoin-Adressen – insbesondere in ihren Signaturen in Internetforen – um die Kryptowährung populär zu machen.[406]

Da die Bitcoin-Adressen und *public keys* eine bestimmte Zeichenstruktur haben[407], können Internet und Forenseiten systematisch nach derartigen Zeichenstrukturen mittels *Web-Crawler*[408] durchsucht werden.[409] So können zunächst verschiedenste Bitcoin-Adressen ermittelt und im Anschluss ausgewertet werden, ob diese etwa im Zusammenhang mit weiteren Informationen – wie etwa einer E-Mail-Adresse – veröffentlicht wurden.[410]

406 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1.

407 Für ein Beispiel vgl. *Kaulartz*, CR 2016, 474 (475).

408 Ein *Web-Crawler* ist ein Programm, das automatisch das Internet oder Webseiten nach bestimmten Inhalten durchsucht.

409 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3).

410 *Reid/Harrigan*, SPSN 2013, 197 (213); *Fleder/Kester/Pillai*, arXiv:1502.01657 [cs.CR] 2015, 1 (3f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

II. Auswertung von Dritt-Anbieter-Cookies

Eine weitere Auswertungsmöglichkeit besteht dann, wenn Bitcoin-Adressen auf Internetseiten angegeben und/oder verwendet werden, die Daten an Drittanbieter weitergeben und die so ermittelten Informationen dann mit den Transaktionsdaten der Blockchain verknüpft werden können.[411] Solche Drittanbieter werden insbesondere bei Online-Shopping-Seiten eingesetzt – etwa für Analyse-, Werbe- oder Zahlungsabwicklungszwecke.[412]

Bei einem normalen Online-Einkauf sind typischerweise folgende Parteien beteiligt:[413]

- Käufer
- Verkäufer
- Zahlungsabwicklungsdienstleister
- *Webtracker*

Bietet nun der Verkäufer die Zahlungsabwicklung über Bitcoin oder eine andere Kryptowährung an, kann es sein, dass auf der abschließenden Bestellseite *Webtracker*[414] von Drittanbietern (wie etwa Googleanalytics) eingesetzt werden.[415] So werden teilweise etwa Daten wie der Preis, der Bestellzeitpunkt, die E-Mail-Adresse des Bestellers oder der Name des Bestellers an Dritte übermittelt.[416]

Außerdem wird der Käufer regelmäßig nach Abschluss des Bestellvorgangs auf eine Zahlungsseite weitergeleitet, die regelmäßig vom Zahlungsabwicklungsdienstleister[417] betrieben wird.[418] Der Zahlungsabwicklungsdienstleistungsanbieter lässt sich dann die entsprechende Summe BTC an eine von ihm benannte – und teilweise extra für diese Zahlung gene-

411 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (1ff.).
412 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (1).
413 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
414 *Webtracker* sind Analyseprogramme, die das Nutzungsverhalten eines Besuchers einer Internetseite analysieren. Im Fall von Online-Shopping-Seiten wird etwa analysiert, welche Artikel angeklickt oder in den Warenkorb gelegt werden. Vgl. hierzu ausführlich *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (2f.).
415 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
416 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4ff.).
417 Bspw. der Anbieter https://bitpay.com (letzter Abruf: 20. Dezember 2021) bietet die Abwicklung derartiger Zahlungen an.
418 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

rierte Bitcoin-Adresse – überweisen.[419] Auch bei diesen Abläufen werden Drittanbieterdienste in Anspruch genommen. So vereinfachen etwa viele Zahlungsabwicklungsdienstleister die Zahlung für den Besteller dadurch, dass die Bitcoin-Empfangsadresse als QR-Code dargestellt wird.[420] Die Erstellung des QR-Codes wird aber regelmäßig von Dritten vorgenommen, sodass hierzu mindestens die Bitcoin-Empfangsadresse an diesen Dritten übermittelt wird.[421] Je nachdem, welche Informationen dabei noch an den Dritten übermittelt werden, kann dieser nun die Blockchain-Transaktionsdaten nach einer entsprechenden Transaktion durchsuchen und so zumindest die Bitcoin-Adresse des Käufers ermitteln.[422]

Je nachdem, welche Daten an Dritte übermittelt werden, ist es für diese im Anschluss möglich anhand der Transaktionsdaten der Blockchain zu ermitteln, welche Transaktionen im Zusammenhang mit den ihnen vorliegenden Daten steht.[423] So kann etwa die maßgebliche Transaktion in der Blockchain herausgefunden werden und so unter Umständen mit der E-Mail-Adresse oder dem Namen des Bestellers verknüpft werden.[424]

III. Standortdaten-Ermittlung bei IoT-Blockchain-Anwendungen

Die neueste Untersuchung des Privatsphäreschutzes bei Blockchain-Anwendungen von *Shahid et. Al.* setzt sich mit der Frage auseinander, ob ein ausreichender Schutz der Privatsphäre bei blockchain-basierten IoT-Systemen besteht, die u.a. auch Standortdaten enthalten und übermitteln.[425]

Betrachtet wird hierbei eine genehmigungsbedürftige Blockchain für ein sog. *Vehicular Ad Hoc Network* (im Folgenden als *VANET* bezeichnet).[426] Ein *VANET* ist ein Kommunikationssystem für Kraftfahrzeuge, die sich gegenseitig über Fahrverhältnisse wie etwa Stau, ein abruptes Bremsen oder

419 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (4).
420 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6).
421 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6).
422 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (6ff.).
423 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (9).
424 *Goldfeder/Kalodner/Reisman/Narayanan*, arXiv:1708.04748v1 [cs.CR] 2017, 1 (9f.).
425 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (116ff.).
426 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Ähnliches informieren, um mehr Sicherheit im Straßenverkehr zu ermöglichen.[427]

Hierbei läuft die Kommunikation der Fahrzeuge untereinander wiederum über ein *Peer-to-Peer-Netzwerk* ab, in dem die Fahrzeuge jeweils unter den Pseudonymen von *public keys* agieren.[428] Allerdings müssen die Fahrzeuge vorher bei einer zentralen Registrierungsstelle angemeldet werden, die dann die *public keys* vergeben.[429]

Inhalt der Kommunikation sind auch die jeweiligen Standortdaten der Fahrzeuge.[430] Dementsprechend ist es theoretisch möglich, wenn ein *public key* einem Fahrzeug zugeordnet werden kann, ein entsprechendes Bewegungsprofil des Fahrzeugs zu erstellen.[431]

IV. Zwischenergebnis

Die Transaktionsdaten der Blockchain können durch anderweitig verfügbare Daten aus dem Internet angereichert werden, um Ermittlungsergebnisse zu erhalten. Dabei können diese Daten etwa aus einer eigenen Veröffentlichung herrühren[432], aber auch unbewusst vom Betroffenen an Dritte übermittelt werden[433]. Soweit die Identitätsdaten der Betroffenen zentral verwaltet werden, kann dies zu erweiterten Auswertungsmöglichkeiten führen, die hier nur beispielhaft unter III. dargestellt wurden.

Auch hier ist anzumerken, dass die Auswertungsmöglichkeiten stark vom Nutzungsverhalten abhängen und insoweit nicht allgemeingültig sind.

427 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
428 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
429 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
430 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (117).
431 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (120).
432 Siehe hierzu unter Kap. 3, C.I.
433 Siehe hierzu unter Kap. 3, C.II.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

D. Zwischenergebnis

Bereits die bloßen Transaktionsdaten in der Blockchain bieten ein breites Spektrum an Auswertungsmöglichkeiten – insbesondere, wenn Hintergründe einzelner Transaktionsdaten bekannt sind und so ein Vergleich möglich ist.

So ist es zunächst möglich, mehrere Bitcoin-Adressen einer *Entität* zuzuordnen. Deren Transaktionsverhalten kann außerdem kategorisiert werden, wenn es vergleichbar ist mit dem Transaktionsverhalten von bekannten Services. Außerdem kann ausgewertet werden, was typisches und was atypisches Transaktionsverhalten ist und ob es bestimmte Transaktionen gibt, die auf illegale Aktivitäten wie Geldwäsche oder Betrug hindeuten.

Diese Auswertungsmöglichkeiten können präzisiert werden, wenn Daten des Netzwerkverhaltens und der Netzwerkverbindungen ausgewertet werden. So ist es unter Umständen möglich, eine Bitcoin-Adresse einer IP-Adresse zuzuordnen und möglicherweise auch den Datenverkehr eines *nodes* auszuwerten.

Weitere Erkenntnisse können sich außerdem durch die Verknüpfung mit anderweitig verfügbaren Daten ergeben.

Besonders hervorzuheben ist, dass die jeweils dargestellten Auswertungsmöglichkeiten kombiniert werden können.

So kann zum Beispiel eine IP-Adresse, die einer Bitcoin-Adresse durch eine *Bloom-Filter*-Attacke zugeordnet werden kann, durch ein *Multi-Input-Clustering*-Verfahren auf eine ganze *Entität* bezogen werden und deren Verhalten insgesamt als das eines *Exchange-Services* klassifiziert werden.

Zu beachten ist aber, dass alle Auswertungsmöglichkeiten entweder vom Nutzungsverhalten des Betroffenen oder von technischen Eigenheiten abhängen. Beides unterliegt einem stetigen, schnellen Wandel – insbesondere auch auf Grund der Auswertungsmöglichkeiten. Aus diesem Grund sind die hier lediglich auszugsweise vorgestellten Auswertungsmöglichkeiten nicht allgemeingültig und hängen davon ab, ob die technischen Eigenheiten und das jeweilige Nutzerverhalten weiterhin bestehen.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

> 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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

1. 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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

> *„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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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],

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

> *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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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 […] Eingriffe 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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

Kapitel 5 – Verfassungsrechtliche Rechtfertigung

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

A. Auswertungsmethoden in der Ermittlungspraxis

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

Dabei dürften sich insbesondere zwei Fragen stellen:

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

I. Einsatz zur Verdachtsbegründung

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

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

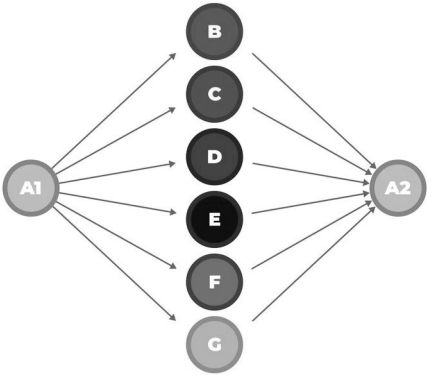
1031 Siehe hierzu unter Kap. 3 A.I.

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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



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

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

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

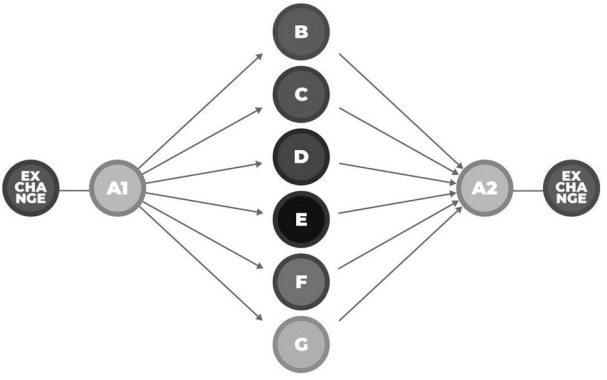
So könnte in dem oben angeführten Beispiel ermittelt werden, dass die von A1 empfangene Transaktion von einem *Exchange-Service* stammt und A2 die von ihm empfangenen Transkationen wieder an einen *Exchange-Service* weiterleiten. So würde sich das oben dargestellte Beispiel wie folgt graphisch darstellen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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb



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

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

Insoweit können die Ermittlungsmöglichkeiten zur Begründung eines Verdachts eingesetzt werden.

II. Einsatz zur Ermittlung nach bestehendem Verdacht

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

1037 Siehe hierzu unter Kap. 3 B.

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

1039 Siehe hierzu unter Kap. 3 A.III.

1040 Siehe hierzu unter Kap. 3 A.III.

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

IV. Zwischenergebnis

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

B. Einschlägige Ermächtigungsgrundlage in der StPO

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

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

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

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

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

1045 BVerfGE 6, 32ff.

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

1. § 94 StPO – Sicherstellung bzw. Beschlagnahme

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

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

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

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

a) Keine unmittelbare Einschlägigkeit von § 94 StPO

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

b) Keine Minus-Maßnahme der Beschlagnahme

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

c) Zwischenergebnis

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

II. § 98a StPO – Rasterfahndung

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

1. „Herkömmliche" Rasterfahndung – Historie und Praxis

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

1101 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 109f..

1102 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110; Löwe-Rosenberg/*Menges,* § 98a Rn. 9.

1103 Etwa mit den so ermittelten Rechnungsanschriften, sodass Sozialämter oder Pflegeheime aus den Datensätzen gestrichen wurden. Außerdem fand ein Abgleich mit den Daten der Einwohnermeldeämter statt. *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.

1104 Siehe hierzu im Einzelnen: *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.

1105 BeckOK-StPO/*Gerhold,* § 98a Rn. 12.

1106 BeckOK-StPO/*Gerhold,* § 98a Rn. 12.

1107 *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 110.

1108 BeckOK-StPO/*Gerhold,* § 98a Rn. 1.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

1128 Siehe hierzu im Einzelnen oben unter Kap. 3.

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

---

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

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

1138 BVerfG NJW 2009, 1405 (1406).

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

c) Herrschende Literaturauffassung

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

d) Begründung des Bundestages

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

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

e) Abweichende Literaturauffassungen

In Teilen der Literatur wurde diese Rechtsprechung aber auch kritisiert:

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

f) Kritische Würdigung

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(1) Erstellen von Persönlichkeitsbildern

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

(2) Streubreite

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

(3) Gesetzesbegründung des Bundestages

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

(4) Abweichende Literaturauffassungen

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

(5) Zwischenergebnis

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

1210 BVerfG NJW 2009, 1405ff.

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

h) Zwischenergebnis

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

i) Anwendung dieser Abgrenzung für die hier gegenständlichen Auswertungsmethoden

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

(2) Auswertung der Netzwerkverbindungen und des Netzwerkverhaltens

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

(3) Auswertung anderweitig verfügbarer Daten

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

(4) Zwischenergebnis

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

4. Datengrundlage der Rasterfahndung

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

(1) Herrschende Literaturauffassung

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

(2) Kritische Würdigung

i. Binnensystematik des § 98a StPO

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ii. Systematisches Verhältnis zu § 98c StPO

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

iii. EDV-gestützte Auswertung von Informationen

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

iv. Auswertung öffentlich verfügbarer Daten

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

v. Zwischenergebnis

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

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

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

(3) Zwischenergebnis

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

i. Öffentlich verfügbare Daten als freiwillig herausgegebene Daten?

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

1243 BVerfGE 130, 151 (202).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

c) Zwischenergebnis

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

5. Zwischenergebnis

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

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

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

1244 Vgl. BVerfGE 65, 1 (43).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

III. § 98c StPO – Maschineller Datenabgleich

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

IV. § 100a StPO – Telekommunikationsüberwachung

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

1261 SK-StPO/*Wolter/Greco,* § 100a Rn. 12.

1262 SK-StPO/*Wolter/Greco,* § 100a Rn. 13, die sich allerdings noch auf § 100a vor der gesetzlichen Kodifizierung der sog. Quellen-TKÜ beziehen.

1263 MüKo-StPO/*Günther,* § 100a Rn. 34.

1264 SK-StPO/*Wolter/Greco,* § 100a Rn. 13.

1265 Vgl. SK-StPO/*Wolter/Greco,* § 100a Rn. 13.

1266 Aus diesem Grund scheiden bis auf die sog. *Bloom-Filter-Attacks* alle hier gegenständlichen Auswertungsmethoden aus dem Schutzbereich des Art. 10 Abs. 1 GG aus, vgl. bereits unter Kap. 4, B.I.2.

1267 Aus diesem Grund scheiden die sog. *Bloom-Filter-Attacks* aus dem Schutzbereich des Art. 10 Abs. 1 GG aus, vgl. bereits unter Kap. 4, B.I.2.b)(2).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

V. § 100b StPO – Online-Durchsuchung

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

VI. § 100g StPO – Erhebung von Verkehrsdaten

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

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

1285 Siehe hierzu ausführlich oben unter Kap. 4, B.III.3.

1286 Gercke/Julius/Temming/Zöller/*Gercke,* § 100b Rn. 10; BeckOK-StPO/*Graf,* § 100b Rn. 8; vgl. BVerfG NJW 2016, 1781 (1793f.) zur präventiven Online-Durchsuchung des § 20k BKAG a.F.; vgl. BT-Drs. 18/12785 S. 54.

1287 Gercke/Julius/Temming/Zöller/*Gercke,* § 100g Rn. 1.

1288 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (83).

1289 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (83).

1290 BeckOK-StPO/*Bär,* § 100g; *Bär*, NStZ 2017, 81 (84); Hdb-StA/*Andrä/Tischer*, 1. Teil, 1.Kap., E. Rn. 69.

1291 BeckOK-StPO/*Bär,* § 100g, Rn. 47; *Bär*, NStZ 2017, 81 (84f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

VII. § 100j StPO – Bestandsdatenauskunft

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

VIII. §§ 161, 163 StPO – Ermittlungsgeneralklauseln

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

1318 BGHSt 41, 64 (Ls. 1).

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

IX. Zwischenergebnis

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

mittlungsgeneralklauseln gestützt werden können, muss nachfolgend untersucht werden.

C. Verfassungsmäßigkeit der Ermittlungsgeneralklauseln §§ 161, 163 StPO

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

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

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

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

1. Anforderungen des Zitiergebotes

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

1338 BVerfG NJW 1970, 1268 (1269).

1339 BVerfGE 120, 274 (303).

1340 BVerfGE 120, 274 (303).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

2. Das Zitiergebot bei der Ermittlungsgeneralklausel des § 161 StPO

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

III. Wesensgehaltsgarantie, Art. 19 Abs. 2 GG

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

IV. Parlamentsvorbehalt und Wesentlichkeitslehre

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

V. Bestimmtheitsgebot

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

VI. Verhältnismäßigkeitsgrundsatz

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

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

1408 BVerfG NJW 2009, 1405 (1407).

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

l. Legitimer Zweck, Geeignetheit und Erforderlichkeit

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

2. Verhältnismäßigkeit im engeren Sinne bzw. Angemessenheit

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

VII. Zwischenergebnis

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

I. Anfangsverdacht

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

I. Voraussetzungen eines Anfangsverdachts

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

a) Kein Anfangsverdacht beim proaktiven Aufklären von Dunkelfeldern

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

b) Objektive Anhaltspunkte

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

c) Hindeuten auf eine konkrete Straftat

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

d) Exkurs – Vorermittlungen

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

1469 *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130.

1470 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(2)i.

1471 Insoweit wäre allenfalls das Herunterladen der Blockchain-Daten im Rahmen derartiger Vorermittlungen möglich. Siehe zum Eingriff in das RiS beim Herunterladen von Blockchain-Daten bereits oben unter Kap. 4, B.II.2.c)(1).

1472 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b).

1473 Vgl. Löwe-Rosenberg/*Mavany,* § 152 Rn. 44.

1474 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130; Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.

1475 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130 Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.

1476 *Eisenmenger*, Grundrechtsrelevanz virtueller Streifenfahrten, S. 252; *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 130; Löwe-Rosenberg/*Erb* Vor. §§ 158 ff. Rn. 17; SK-StPO/*Weßlau/Deiters,* Vor. §§ 151 ff. Rn. 6f.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

e) Exkurs – Strafverfolgungsvorsorge

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

Zu unterscheiden sind in diesem Zusammenhang zwei verschiedene Fallkonstellationen:

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

f) Legales Verhalten zur Begründung eines Anfangsverdachts?

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

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

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

1490 BVerfGE 113, 348 (370).

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

h) Zwischenergebnis

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

2. Anfangsverdacht bei der Anwendung der Auswertungsmethoden

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

a) Einsatz zur Verdachtsbegründung

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

b) Einsatz zur Ermittlung nach bestehendem Verdacht

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

Hieraus ergeben sich entsprechende zwei Fragen:

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

(1) Verwertung von Daten aus einzelnen, vorangegangen Strafverfahren

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

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

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

1515 Siehe hierzu bereits oben unter Kap. 5, D.I.1.e); *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 87.

1516 BeckOK-StPO/*Wittig*, § 484.

1517 Vgl. BeckOK-StPO/*Wittig*, § 484 Rn. 1.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(2) Anfangsverdacht bei abstrakten Transaktionsmustern

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

d) Zwischenergebnis

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

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

1521 In der damals geltenden Fassung vom 01.04.2004.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

e) Exkurs – verdachtsbegründender Einsatz als zulässige Vorermittlungen?

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

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

II. Lediglich geringfügiger Grundrechtseingriff

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

a) Einfache Fahndungsmaßnahmen und kurzfristige Observationen

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

1541 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, B.II.2.
1542 Siehe hierzu im Einzelnen bereits oben unter Kap. 5, C.II.1.
1543 Dies war etwa der Fall bei der Suche nach potenziellen „Schläfern" im Anschluss an die Anschläge des 11. September 2001, vgl. *Middel*, Innere Sicherheit und präventive Terrorismusbekämpfung, S. 97.
1544 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 3 mit Verweis auf BVerfG NJW 2006, 1941 (1944f.).
1545 Vgl. Gercke/Julius/Temming/Zöller/*Gercke,* § 98a Rn. 3 mit Verweis auf BVerfG NJW 2006, 1941 (1944f.); BVerfGE 125, 260 (318).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

(5) Zwischenergebnis

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

1575 *Soiné*, NStZ 2014, 248 (251).

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

d) Insbesondere: Online-Ermittlungen

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

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

(1) Gegenstand der Online-Ermittlung

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

(2) Ähnliche, spezielle Ermittlungsbefugnisse

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

Denn, soweit etwa Zugangsbeschränkungen überwunden werden, soll etwa ein Eingriff in das Fernmeldegeheimnis vorliegen, für den eine entsprechende Rechtfertigung in Form einer gesetzlichen Befugnis erforderlich ist.[1597]

Dies ergibt sich insbesondere auch aus dem Vergleich mit den Ermittlungsbefugnissen der §§ 100a, 100b StPO. Denn diese ermöglichen – anders als bei den zuvor dargestellten Online-Ermittlungen nach §§ 161, 163 StPO – auch den Zugriff auf (Kommunikations-)Inhalte, die nicht im Internet allgemein zugänglich sind.[1598]

Nach § 100a StPO kann auch „ohne Wissen der Betroffenen […] die Telekommunikation überwacht und aufgezeichnet werden"[1599]. Klassischerweise betrifft § 100a StPO damit den Zugriff auf Telekommunikation, die vom Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG erfasst ist – der Schutzbereich des Art. 10 Abs. 1 GG und die Reichweite des nach § 100a StPO zulässigen Zugriffs sind aber nicht deckungsgleich.[1600] Nach § 100a Abs. 1 S. 2 StPO ist aber auch der Zugriff auf informationstechnisches Sys-

1595 Gercke/Julius/Temming/Zöller/*Zöller,* § 163 Rn. 12; *Klesczewski*, ZStW 123 (2013), 737 (739ff.).

1596 Vgl. *Soiné*, NStZ 2014, 248 (249); *Rosengarten/Römer*, NJW 2012, 1764 (1766f.) mit Verweis auf BVerfGE 120, 274 (345).

1597 *Klesczewski*, ZStW 123 (2013), 737 (739).

1598 Vgl. *Safferling/Rückert,* MMR 2015, 788 (793).

1599 Wortlaut des § 100a Abs. 1 S. 1 StPO.

1600 Siehe zur umstrittenen Frage, ob Schutzbereich des Art. 10 GG und Anwendungsbereich des § 100a StPO deckungsgleich sind, bereits ausführlich oben unter Kap. 5, B.IV.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

tem zur Überwachung der damit geführten Telekommunikation möglich (sog. Quellen-TKÜ).[1601] Jedenfalls betrifft § 100a StPO aber die nicht öffentlich geführte Telekommunikation – öffentlich geführte Telekommunikation ist dagegen vom Anwendungsbereich des § 100a StPO nicht erfasst.[1602]

Von der Ermittlungsbefugnis des § 100b StPO ist darüber hinaus die sog. Online-Durchsuchung erfasst.[1603] Denn nach § 100b StPO kann auf informationstechnische Systeme ohne Wissen des Betroffenen zugegriffen werden und die dort gespeicherten Daten erhoben werden. § 100b StPO ermöglicht damit einen Eingriff in das IT-Grundrecht und damit den Zugriff auf informationstechnische Systeme auf einem technischen Weg, der dafür nicht vorgesehen ist und damit den Zugriff unter Überwindung von berechtigten Vertraulichkeitserwartungen des Betroffenen.[1604]

Aus dem Vergleich der nach §§ 100a, 100b StPO zulässigen Ermittlungsbefugnisse mit den nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen ergibt sich daher insoweit, dass einerseits ein intensitätserhöhender Faktor vorliegt, wenn unter Überwindung von Zugangsbeschränkungen und berechtigten Vertraulichkeitserwartungen auf Kommunikation zugegriffen wird. Im Umkehrschluss ergibt sich daraus andererseits, dass dann ein intensitätsverringernder Faktor vorliegt, wenn es gerade keine Zugangsbeschränkungen oder berechtigte Vertraulichkeitserwartungen gibt. Insoweit ergibt sich hieraus auch, dass eine geringere Grundrechtsintensität vorliegt, wenn nur solche Informationen ausgewertet werden, die allgemein zugänglich sind.

(3) Exkurs – Grenze der nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen

Erste Grenzen der Zulässigkeit von Online-Ermittlungen nach §§ 161, 163 StPO hat *Rückert* entwickelt:

So arbeitet *Rückert* zunächst heraus, dass die bloße öffentliche Verfügbarkeit von Informationen noch nicht insgesamt dazu führe, dass auch die Ermittlungsgeneralklauseln als Rechtfertigung für den Grundrechtsein-

1601 Vgl. BeckOK-StPO/*Graf,* § 100a Rn. 113f.
1602 *Rückert*, ZStW 129 (2017), 302 (316); vgl. *Safferling/Rückert,* MMR 2015, 788 (793).
1603 BeckOK-StPO/*Graf,* § 100b.
1604 Siehe hierzu bereits oben unter Kap. 5, B.V.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

griff ausreichten.[1605] Hierzu zieht *Rückert* insbesondere einen Vergleich mit speziellen Ermittlungsbefugnissen in der analogen Welt heran, die sich ebenfalls auf Informationen aus dem öffentlichen Raum beziehen.[1606]

Ferner arbeitet *Rückert* heraus, dass insbesondere die automatisierte und die manuelle Auswertung von Informationen eine unterschiedliche Grundrechtsintensität aufweisen, sodass eine spezielle Ermächtigungsgrundlage erforderlich sein kann.[1607] Dabei stellt *Rückert* für die Frage der Grenzziehung darauf ab, ob von einer technikgestützten Auswertung die Gefahr für das allgemeine Persönlichkeitsrecht besteht, dass umfassende Persönlichkeits- und Bewegungsprofile erstellt werden könnten.[1608]

So kommt *Rückert* zu dem Ergebnis, dass die manuelle Erhebung und Auswertung von öffentlich verfügbaren Informationen im Internet wohl auf die Ermittlungsgeneralklauseln gestützt werden könne, da die Gefahr der Persönlichkeitsrechtsgefährdung gerade durch die beschränkten Möglichkeiten von manuellen Auswertungen begrenzt sei.[1609] Hinsichtlich einer „automatisierten Suche, Erhebung und Verarbeitung öffentlich zugänglicher Daten"[1610] kommt *Rückert* dagegen zu dem Ergebnis, dass zunächst danach zu differenzieren sei, ob derartige Ermittlungsinstrumente gegen konkret Tatverdächtige eingesetzt werden oder zum Zweck der Rasterdatenerhebung eingesetzt werden.[1611] Denn beim Einsatz zur Gewinnung von Beweisdaten würden Daten von unverdächtigen Personen nur erhoben, wenn dies unvermeidbar sei, wohingegen beim Einsatz zur Rasterdatenerhebung auch eine unüberschaubare Vielzahl nichtverdächtiger Personen betroffen sein könnte.[1612] Auf die Ermittlungsgeneralklauseln könnten automatisierte Ermittlungsmethoden nach *Rückert* allenfalls dann gestützt werden, wenn sie zur Gewinnung von Beweisdaten eingesetzt werden – *Rück-*

1605 *Rückert,* ZStW 129 (2017), 302 (325).
1606 *Rückert,* ZStW 129 (2017), 302 (325), der etwa auf die nur nach § 100h StPO zulässige Anfertigung von Bildaufnahmen im öffentlichen Bereich abstellt.
1607 *Rückert,* ZStW 129 (2017), 302 (326).
1608 *Rückert,* ZStW 129 (2017), 302 (326). Alternativ bestünde auch die Möglichkeit einer rein technischen Grenzziehung, die aber angesichts der vielfach bereits bei der einfachen Google-Suche eingesetzten Software nicht praktikabel ist, vgl. *Rückert,* ZStW 129 (2017), 302 (326). Vgl. zur Nutzung netzwerkinterner Suchfilter *Bauer*, Soziale Netzwerke, S. 145f. mit Verweis auf *Oermann/Staben*, Der Staat 2013, 630 (646).
1609 *Rückert,* ZStW 129 (2017), 302 (328).
1610 *Rückert,* ZStW 129 (2017), 302 (329).
1611 *Rückert,* ZStW 129 (2017), 302 (329).
1612 *Rückert,* ZStW 129 (2017), 302 (329).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ert empfiehlt jedoch auch für diesen Bereich eine gesetzliche Regelung, der sich an §§ 163e, 163f StPO orientieren solle.[1613] Dagegen sei nach *Rückert* die Grenze der Ermittlungsgeneralklauseln beim Einsatz zum Zweck der Rasterdatenerhebung überschritten, da hierdurch „zahlreiche[…] Daten von Nicht-Verdächtigen"[1614] einbezogen würden und insoweit eine große Vergleichbarkeit mit §§ 163d StPO und § 111 StPO bestünde.[1615]

(4) Zwischenergebnis

Aus dem Vorstehenden ergibt sich, dass nach § 161 Abs. 1 StPO jedenfalls der Aufruf und die Kenntnisnahme von öffentlich zugänglichen Inhalten im Internet zulässig ist, auch, wenn diese gezielt eingesetzt werden, um Informationen über Einzelpersonen zu ermitteln.[1616] Grenzen dieser nach § 161 Abs. 1 StPO zulässigen Online-Ermittlungen liegen dort, wo Zugangsbeschränkungen überwunden werden und berechtigte Vertraulichkeitserwartungen des Betroffenen bestehen.[1617] Hieraus ergibt sich, dass ein derartiger Zugriff wesentlich intensitätssteigernd ist.[1618] Eine weitere Grenze könnte auf Grund der Gefährdung des Persönlichkeitsrechts in der technikgestützten Auswertung öffentlich verfügbarer Inhalte liegen.[1619] Wann diese Grenze überschritten ist, dürfte maßgeblich davon abhängen, ob eine große Streubreite der Maßnahme vorliegt.[1620]

e) Abfragen von Kontoinformationen im Rahmen Europäischer Rechtshilfe

Schließlich können auch § 91c Abs. 2 Nr. 2 lit. b), lit. c) lit. aa) IRG und dessen Gesetzesbegründung als Vergleichsmaßstab herangezogen werden.

Die Vorschriften wurden zur Umsetzung der sog. Europäischen Ermittlungsanordnung (nachfolgend als „EEA" bezeichnet) eingeführt. Die EEA

1613 *Rückert,* ZStW 129 (2017), 302 (331).
1614 *Rückert,* ZStW 129 (2017), 302 (331).
1615 *Rückert,* ZStW 129 (2017), 302 (331f.).
1616 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(1).
1617 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(2)ii.
1618 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(2)ii.
1619 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(3)iii.
1620 Siehe hierzu soeben unter Kap. 5.D.II.1.d)(3)iii.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

beruht auf der RL (EU) 2014/41 (nachfolgend als „RL EEA" bezeichnet).[1621] Eines der Ziele der EEA ist es, die grenzüberschreitende Beweiserhebung innerhalb der EU zu vereinfachen und zu beschleunigen.[1622] Im Zusammenhang mit Ermittlungen bei Bankkonten enthält die RL EEA unter anderem die folgenden Vorgaben an die Mitgliedstaaten:

Art. 27 RL EEA enthält die Befugnis zur Ermittlung von „Informationen über Bank- und sonstige Finanzgeschäfte"[1623]. Nach Art. 27 Abs. 1 RL EEA soll eine EEA erlassen werden können, „um Angaben über bestimmte Bankkonten sowie über Bankgeschäfte zu erlangen, die während eines bestimmten Zeitraums über ein oder mehrere in der EEA angegebenes/angegebene Bankkonto/Bankkonten getätigt wurde, einschließlich der Angaben über sämtliche Überweisungs- und Empfängerkonten."[1624]

Darüber hinaus sieht Art. 28 Abs. 1 lit. a) RL EEA grundsätzlich die Möglichkeit einer fortlaufenden Überwachung von Bank- oder sonstigen Finanzgeschäften über einen bestimmten Zeitraum vor.[1625]

Zur Umsetzung der RL EEA hat der deutsche Gesetzgeber unter anderem einen zweiten Abschnitt des 10. Teils des IRG geschaffen und hierin Regelungen für die Umsetzung der EEA geschaffen.[1626] Hierin ist eine ergänzende Zulässigkeitsvoraussetzung[1627] für bestimmte Formen der Rechtshilfe in § 91c IRG enthalten.[1628] Ziel von § 91c IRG ist die Umsetzung der besonderen Zurückweisungsgründe der Art. 22ff. RL EEA.[1629] Dabei enthält § 91c Abs. 2 IRG eine „vollumfängliche Anwendung von § 59 Abs. 3 IRG"[1630]. § 59 Abs. 3 IRG regelt den Grundsatz, dass Rechtshilfe nur geleistet werden darf, „wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten."[1631] Hieraus ergibt sich, dass die Rechtshilfe nicht zulässig ist, „wenn die erbetene Ermittlungsmaßnahme in einem vergleich-

1621 BT-Drs. 18/9757, S. 17.
1622 BT-Drs. 18/9757, S. 19.
1623 So die amtliche Überschrift des Art. 27 RL (EU) 2014/41.
1624 So der Wortlaut des Art. 27 Abs. 1 RL (EU) 2014/41.
1625 *Leonhardt,* Die Europäische Ermittlungsanordnung in Strafsachen, S. 86.
1626 Vgl. BT-Drs. 18/9757, S. 17ff., S. 54f.
1627 Die grundsätzliche Zulässigkeit der sonstigen Rechtshilfe innerhalb der Europäischen Union richtet sich nach §§ 91a, 91b IRG, vgl. BT-Drs. 18/9757, S. 55, 57ff.
1628 BT-Drs. 18/9757, S. 62.
1629 BT-Drs. 18/9757, S. 62.
1630 BT-Drs. 18/9757, S, 62.
1631 So der Wortlaut des § 59 Abs. 3 IRG.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

baren innerstaatlichen Fall nicht zulässig wäre"[1632]. Dies ist etwa für die Kontoüberwachung in Echtzeit der Fall, die das deutsche Strafprozessrecht nicht kennt.[1633]

Für die hier gegenständliche Untersuchung sind dabei insbesondere die besonderen Zulässigkeitsvoraussetzungen für die Abfrage von Kontoinformationen in § 91c Abs. 2 Nr. 2 lit. b), lit. c) lit. aa) IRG und die jeweilige Gesetzesbegründung relevant.

§ 91c Abs. 2 Nr. 2 lit. b) IRG enthält dabei die besondere Zulässigkeitsvoraussetzung, dass Rechtshilfeersuchen zurückgewiesen werden können, wenn die „Abfrage von bestimmten Kontenbewegungen […] [als] Ermittlungsmaßname in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde[1634]. Hiermit soll der besondere Zurückweisungsgrund des Art. 27 Abs. 5 S. 3 RL EEA umgesetzt werden.[1635] In der Gesetzesbegründung verweist der Gesetzgeber zur Erhebung von Kontoinformationen auf die gängige Ermittlungspraxis, nach den „§§ 160, 161a StPO eine Auskunft von der betroffenen Bank"[1636] zu verlangen. Sollte die jeweilige Bank diesem Ersuchen nicht nachkommen, sei eine zeugenschaftliche Vorladung nach §§ 161a Abs. 2, 51, 70 StPO oder die Durchsuchung und Beschlagnahme nach §§ 98, 102, 103 StPO in Betracht zu ziehen.[1637]

§ 91c Abs. 2 Nr. 2 lit. c) lit. aa) IRG enthält darüber hinaus die besondere Zulässigkeitsvoraussetzung für sog. Echtzeitmaßnahmen und setzt damit den besonderen Zurückweisungsgrund aus Art. 28 Abs. 1 RL EEA um.[1638] Denn nach Art. 28 Abs. 1 RL EEA ist es grundsätzlich möglich, eine EEA zu erlassen, „um Beweismittel in Echtzeit, fortlaufend oder über einen bestimmten Zeitraum zu erheben."[1639] In Art. 28 Abs. 1 Hs. 2 RL EEA ist aber auch der besondere Zurückweisungsgrund enthalten, dass die „Vollstreckung [auch] versagt werden [kann], wenn die Durchführung der betreffenden Ermittlungsmaßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde."[1640] Dies ist insoweit relevant, als dass der Gesetzgeber in der Gesetzesbegründung darauf verweist, dass nach „der StPO

1632 BT-Drs. 18/9757, S, 62.
1633 BT-Drs. 18/9757, S, 62. Vgl. insoweit § 91c Abs. 2 Nr. 2 lit. c) lit. aa) IRG.
1634 BT-Drs. 18/9757, S. 63.
1635 BT-Drs. 18/9757, S. 63.
1636 BT-Drs. 18/9757, S. 40.
1637 BT-Drs. 18/9757, S. 40.
1638 BT-Drs. 18/9757, S. 64.
1639 BT-Drs. 18/9757, S. 40.
1640 So der Wortlaut des Art. 28 Abs. 1 Hs. 2 RL EEA.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

[…] in die Zukunft gerichtete Kontoüberwachungen in Echtzeit nicht zugelassen“[1641] sind.[1642] Nach der StPO seien allenfalls „periodische Auskunftsersuchen, durch die in gewissen Zeitabständen rückwirkende Kontoabfragen durch die Strafverfolgungsbehörden erfolgen“[1643], möglich.[1644]

Für die hier gegenständliche Untersuchung ergibt sich hieraus, dass nach Ermittlungsbefugnissen der §§ 161, 163 StPO weder Unterlagen herausverlangt werden können noch Konten fortlaufend überwacht werden können. Für ein Herausgabeverlangen von Unterlagen sind nur die Vorschriften zur Herausgabe und Beschlagnahme (§§ 94, 95, 98, 102, 103 StPO) einschlägig.[1645] Für eine fortlaufende Überwachung von Konten besteht in der StPO dagegen keine Ermächtigungsgrundlage.[1646]

Aus diesem Vergleich ergibt sich insoweit, dass kein geringfügiger Grundrechtseingriff mehr vorliegt, wenn Beweismittel (gegen den Willen des Berechtigten) sichergestellt werden oder eine fortlaufende Überwachung stattfindet. Insoweit besteht hier eine Parallele zur der bereits dargestellten Abgrenzung von kurz- und längerfristigen Observationen.[1647] Dementsprechend ergibt sich auch aus diesem Vergleich, dass bei umfangreicheren Informationserhebungen, sowie einer erhöhten Streubreite[1648] ein nicht mehr nur geringfügiger Grundrechtseingriff vorliegt.

f) Zwischenergebnis

Aus den vorstehenden Vergleichen der nach § 161 Abs. 1 StPO bisher als zulässig angesehenen Ermittlungsmaßnahmen mit den speziell geregelten Ermittlungsbefugnissen ergibt sich, dass für die Grundrechtsintensität von

1641 BT-Drs. 18/9757, S. 64.
1642 BT-Drs. 18/9757, S. 64.
1643 BT-Drs. 18/9757, S. 64.
1644 BT-Drs. 18/9757, S. 64.
1645 BT-Drs. 18/9757, S. 40; vgl. KK-StPO/*Griesbaum,* § 161 Rn. 8. Zu beachten ist insoweit, dass die freiwillige Herausgabe von potenziellen Beweismitteln nach § 94 Abs. 1 StPO ebenfalls nur ein Anfangsverdacht erforderlich ist. Lediglich die Beschlagnahme gegen den Willen des Berechtigten bedürfen den zusätzlichen Anforderungen der Beschlagnahme nach §§ 97, 98 StPO. Vgl. insoweit hierzu bereits ausführlich oben unter Kap. 5, B.I.1.
1646 BT-Drs. 18/9757, S. 64.
1647 Siehe hierzu bereits oben unter Kap. 5, D. II.1.a)(3).
1648 Denn auch bei der fortlaufenden Überwachung von Bankkonten dürfte eine größere Anzahl von Personen anlasslos von der Maßnahme betroffen werden.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Ermittlungsmaßnahmen unter anderem die folgenden Faktoren und Kriterien relevant sind:

Zunächst wirkt sich der Umfang der erhobenen Informationen auf die Grundrechtsintensität aus. So liegt jedenfalls eine gesteigerte Grundrechtsintensität bei umfangreicheren Datensätzen vor, eine geringe Grundrechtsrelevanz grundsätzlich, wenn nur einzelne Informationen erhoben werden.

Außerdem hängt die Grundrechtsintensität vom Inhalt und der Art der Erhebung der jeweiligen Information ab. So liegt insbesondere dann eine erhöhte Grundrechtsintensität vor, wenn bei der Erhebung berechtigte Vertraulichkeitserwartungen oder Zugangsbeschränkungen überwunden werden. So liegt etwa bereits bei der verdeckten Erhebung von Informationen grundsätzlich eine erhöhte Grundrechtsintensität vor. Besonders grundrechtsintensiv sind darüber hinaus Erhebungen, die unter Überwindung von grundrechtlich geschützten Vertraulichkeitserwartungen vorgenommen werden. Dagegen liegt eine deutlich geringere Grundrechtsintensität vor, wenn lediglich Informationen erhoben werden, die allgemein zugänglich sind und bei denen insoweit keine Vertraulichkeitserwartungen bestehen.

Darüber hinaus steht im engen Zusammenhang mit dem Inhalt und der Art der Erhebung auch die Art und Weise der Auswertung der Informationen, die sich ebenfalls intensitätssteigernd auswirken kann. So ist hier insbesondere die technikgestützte Auswertung von Informationen durch maschinelle Datenabgleiche in den Blick zu nehmen, bei der eine hohe Intensitätssteigerung vorliegt. Denn hierdurch können einerseits auch einzelne Informationen mit geringem Informationsgehalt derart miteinander verknüpft werden, dass sich hieraus sensible Informationen ergeben können. Andererseits können bei der technikgestützten Auswertung gerade auch viele Personen betroffen sein, die durch ihr Verhalten keinen Anlass gegeben haben, von einer staatlichen Ermittlungsmaßnahme betroffen zu sein (Streubreite).

Dabei ist die Streubreite insgesamt ein wesentlicher Faktor der Grundrechtsintensität von Ermittlungsmaßnahmen – sowohl bei der Auswertung von Informationen als auch bei der Erhebung der ausgewerteten Informationen. So besteht eine wesentlich erhöhte Grundrechtsintensität, wenn eine Vielzahl unbeteiligter Personen von staatlichen Ermittlungsmaßnahmen betroffen ist. Darüber hinaus ist hierbei die Grundrechtsintensität der Streubreite außerdem danach abzustufen, ob es überhaupt einen Anlass dafür gegeben hat, dass der Einzelne von der Maßnahme betroffen ist und in welcher Intensität und Form dieser Anlass bestanden hat.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

2. Rechtsprechung des BVerfG zu Kriterien und Bewertung der Grundrechtsintensität

Zu diesen Kriterien für die Bewertung der Grundrechtsintensität kommt auch die Rechtsprechung des BVerfG weitgehend.

So nimmt das BVerfG an, dass die Grundrechtsintensität „insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten beeinflusst wird“[1649]. So sind hier grundsätzlich vier verschiedene Kriterien zu unterscheiden, die sich allerdings in ihren Einzelheiten teilweise wieder überschneiden. Trotzdem soll nachfolgend versucht werden, diese Kriterien jeweils im Einzelnen darzustellen.[1650]

a) Art der erfassten Informationen

Grundsätzlich ist nach dem BVerfG zunächst für die Beurteilung der Grundrechtsintensität relevant, welche Persönlichkeitsrelevanz die jeweiligen Informationen haben.[1651] Insoweit wirkt sich etwa intensitätsverringernd aus, wenn die Daten anonym sind[1652] oder der Personenbezug erst durch Zusatzwissen hergestellt werden kann.[1653] Eine absolute Grenze der Intensität ist dagegen der Kernbereich privater Lebensgestaltung.[1654] Zu

1649 BVerfGE 120, 378 (Ls. 2).

1650 Nachfolgend wird insbesondere auch auf Rechtsprechung des BVerfG eingegangen, die sich zur Grundrechtsintensität bei Eingriffen in Art. 10, Art. 13 GG äußert. Nach BVerfGE 115, 320 (347) finden die in diesem Zusammenhang festgestellten Grundsätze aber auch für Eingriffe in das RiS Anwendung.

1651 BVerfGE 115, 320 (347); BVerfGE 118, 168 (196f.); vgl. außerdem BVerfGE 100, 313 (376); 109, 279 (353), 113, 348 (382) deren Maßstäbe zur Bewertung der Grundrechtsintensität bei Eingriffen in das Fernmeldegeheimnis, nach BVerfGE 115, 320 (347) grundsätzlich anwendbar sind.

1652 BVerfGE 65, 1 (45); BVerfGE 100, 313 (376); BVerfGE 115, 320 (347). Unklar ist allerdings, inwieweit bei anonymen Daten überhaupt ein Grundrechtseingriff vorliegen soll (vgl. hierzu ausführlich oben unter Kap. 4, B.I.b)). Grund hierfür könnte etwa sein, dass das BVerfG für die Bewertung der Grundrechtsintensität wechselseitig auf die jeweiligen Maßstäbe der Bewertung der Grundrechtsintensität bei Eingriffen in Art. 10, Art. 13 GG und das RiS nimmt, vgl. *Buermeyer,* Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug, S. 165f. Hieraus lässt sich aber der Rückschluss ziehen, dass die Grundrechtsintensität jedenfalls verringert ist, wenn kein unmittelbarer Personenbezug besteht.

1653 BVerfGE 128, 1 (53).

1654 BVerfGE 109, 279 (313).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

diesem Kernbereich privater Lebensgestaltung „gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen."[1655]

Bei der Bewertung der Persönlichkeitsrelevanz der erfassten Information ist außerdem nicht nur die jeweilige Einzelinformation maßgeblich, sondern auch welche Informationen durch eine weitergehende Verarbeitung und Verknüpfung gewonnen werden können und sollen.[1656] Denn je nach Verarbeitungs- und Verknüpfungsmöglichkeit durch Informationstechnologie können auch belanglose Daten einen neuen Stellenwert bekommen.[1657] So können insbesondere etwa auch lediglich technische Nebenprodukte, wie die Verbindungsdaten von Telekommunikation gerade in ihrer Verknüpfung eine besondere Persönlichkeitsrelevanz haben, da sie Rückschlüsse auf das soziale Umfeld des Betroffenen und die jeweiligen Kontakte zulassen.[1658]

In diesem Zusammenhang ist daher auch zu berücksichtigen, dass sich die Vielzahl der erhebbaren Daten intensitätssteigernd auswirkt,[1659] denn je umfangreicher die erhobenen bzw. erhebbaren Daten sind, desto mehr und genauere Informationen können auch durch ihre Verknüpfung erlangt werden.

b) Anlass und Umstände der Erhebung

Im Zusammenhang mit der Vielzahl der erhebbaren und erhobenen Daten ist außerdem relevant, ob und welcher Anlass für die Datenerhebung bestanden hat und unter welchen Umständen die Datenerhebung erfolgt ist.

So soll sich zunächst insbesondere die Streubreite der jeweiligen Maßnahme erheblich intensitätssteigernd auswirken. Insoweit soll für die Intensitätssteigerung maßgeblich sein, ob der Betroffene einen Anlass für die Erhebung der Daten gegeben hat „oder ob sie anlasslos erfolgt und damit

1655 BVerfGE 109, 279 (313).
1656 BVerfGE 65, 1 (45f.); BVerfGE 107, 299 (320); BVerfGE 115, 320 (348).
1657 BVerfGE 65, 1 (45).
1658 BVerfGE 107, 299 (319f.).
1659 BVerfGE 113, 348 (365).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

praktisch jeden treffen kann."[1660] Dies ist insbesondere dann intensitätserhöhend, wenn eine Vielzahl der Daten verfahrensunerheblich ist.[1661]

Dabei ist außerdem maßgeblich für die Intensität, ob und welche Nachteile dem Betroffenen durch die Maßnahme drohen und ob diese nicht ohne Grund befürchtet werden.[1662] Dementsprechend ist allerdings auch intensitätsverringernd, wenn die Betroffenen selbst einen Anlass dafür gegeben haben, von der jeweiligen Maßnahmen betroffen zu sein.[1663]

Hintergrund dieser hohen Intensität ist, dass Einschüchterungseffekte entstehen können, wenn eine große Anzahl Personen, die keinen Erhebungsanlass gegeben haben, von der Maßnahmen betroffen sind.[1664] Denn Sinn und Zweck des RiS ist es auch der Schutz der allgemeinen Verhaltensfreiheit des Einzelnen, die auch dann eingeschränkt sein kann, wenn der Einzelne nicht weiß, welche Informationen über ihn erhoben werden und er insoweit die Entscheidungen über sein Handeln möglicherweise anpasst und damit nicht mehr frei treffen kann.[1665]

Insoweit ist insgesamt relevant, welcher Personenkreis von der Maßnahme betroffen ist.[1666]

Darüber hinaus ist für die Grundrechtsintensität außerdem relevant unter welchen Umständen die Datenerhebung stattfindet.[1667]

Intensitätserhöhend wirkt sich dabei insbesondere die Heimlichkeit der Erhebung aus.[1668] Denn einerseits befindet sich der Betroffene in einer vermeintlich vertraulichen Situation, wenn die Datenerhebung heimlich stattfindet.[1669] Andererseits kann er die Maßnahme auf Grund der fehlenden Kenntnis nicht selbst beeinflussen und kann sich allenfalls nach dem Abschluss der Maßnahme und damit erst, wenn der Eingriff bereits vollzogen ist, rechtlich gegen die Maßnahme wehren.[1670]

1660 BVerfGE 120, 378 (402) mit Verweis auf BVerfGE 100, 313 (376, 392); BVerfGE 107, 299 (320f.); BVerfGE 109, 279 (353); BVerfGE 113, 29 (53); BVerfGE 113, 348 (383); BVerfGE 115, 320 (354).

1661 BVerfGE 113, 29 (53) zur Beschlagnahme von Datenträgern einer Anwaltskanzlei.

1662 BVerfGE 100, 313 (376).

1663 BVerfGE 128, 1 (53).

1664 BVerfGE 120, 378 (402) mit Verweis auf BVerfGE 65, 1 (42); BVerfGE 113, 29 (46).

1665 BVerfGE 65, 1 (43). Siehe hierzu bereits im Einzelnen oben unter Kap. 4, B.II.1.a).

1666 BVerfGE 120, 378 (Ls. 2). Siehe hierzu auch die eingängliche Formulierung unter Kap. 5, C.II.2.b)

1667 BVerfGE 120, 378 (Ls. 2).

1668 BVerfGE 107, 299 (321); BVerfGE 115, 166 (194); BVerfGE 115, 320 (353).

1669 BVerfGE 107, 299 (321) mit Verweis auf BVerfGE 34, 238 (247).

1670 BVerfGE 107, 299 (321).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Darüber hinaus wirkt sich besonders intensitätssteigernd aus, wenn bei der Datenerhebung Vertraulichkeitserwartungen verletzt werden, die einen besonderen grundrechtlichen Schutz genießen.[1671]

(1) Intensitätsverringerung bei öffentlich verfügbaren Daten?

Intensitätsverringernd könnte sich dagegen der Umstand auswirken, wenn Daten erhoben werden, die allgemein zugänglich bzw. öffentlich verfügbar[1672] sind. Zu einer Intensitätsverringerung wegen der allgemeinen Zugänglichkeit von personenbezogenen Informationen hat sich das BVerfG etwa in seinen Entscheidungen zu automatisierten Kfz-Kennzeichenerfassungen[1673] geäußert. Das BVerfG stellte im Rahmen der Bewertung der Grundrechtsintensität zwar fest, dass die automatisierten Kfz-Kennzeichenkontrollen insgesamt einen Eingriff „von erheblichem Gewicht"[1674] darstellten. Allerdings sei der Bewertung des „Eingriffsgewicht[s] mindernd einzustellen, dass die Kennzeichenkontrolle im öffentlichen Verkehrsraum stattfinde[…]. Sowohl die Kraftfahrzeugkennzeichen als auch das erfasste Bewegungsverhalten [sei] ohne weiteres für alle erkennbar."[1675]

Fraglich ist, ob dies auch für die Erhebung von öffentlich zugänglichen Daten im Internet gelten kann.

Gegen eine derartige Anwendbarkeit ließe sich nämlich anführen, dass das BVerfG in seiner Entscheidung zum VSG NRW[1676] eindeutig die Grenze eines Eingriffs für die Erhebung öffentlich verfügbarer Daten festgelegt

1671 BVerfGE 109, 279 (313f., 325, 327f.); BVerfGE 113, 348 (364f., 383, 392); BVerfGE 115, 320 (348); BVerfGE 130, 1 (36). Abweichend von BVerfGE 115, 320 (348) vertritt Richterin *Haas* in ihrem Sondervotum zum Beschluss des Ersten Senats vom 04. April 2006 – 1 BvR 518/02 –, dass bei heimlichen Maßnahmen die Intensitätssteigerung der Streubreite von Maßnahmen im Widerspruch zur intensitätssteigernden Heimlichkeit der Maßnahme stünden. Denn es sei widersprüchlich, dass einerseits ein Einschüchterungseffekt intensitätssteigernd sei und andererseits die Heimlichkeit und damit die Unkenntnis des Betroffenen von der konkreten Maßnahme intensitätssteigernd sei, vgl. BVerfGE 115, 320 (372).

1672 Siehe zur Begriffsbestimmung öffentlich verfügbarer Daten bereits oben unter Kap. 4, B.II.1.d)

1673 BVerfGE 120, 378 (404) BVerfGE 150, 244ff.; siehe hierzu im Einzelnen bereits oben unter Kap. 4, B.II.2.b)iii., iv.

1674 BVerfGE 150, 244 (283).

1675 BVerfGE 150, 244 (283); vgl. BVerfGE 120, 378 (404).

1676 BVerfGE 120, 274ff; siehe hierzu bereits im Einzelnen oben unter Kap. 4, B.II.2.b)(1)i.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

hat. Diese Grenze ist überschritten, wenn Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt."[1677] Wenn insoweit die Grenze des Eingriffs bei einer bestimmten Form der Erhebung (vereinfacht: dem gezielten Zusammentragen der Daten) überschritten ist, könnte man annehmen, dass hierin schon ein Umstand der Erhebung vorliegt. Wenn aber dieser bestimmte Umstand der Erhebung gerade die Grenze zum Vorliegen eines Eingriffs darstellt, wirkt es auf den ersten Blick widersprüchlich, gerade diesen Umstand dann wiederum als intensitätsverringernd zu berücksichtigen. Allerdings muss hierbei beachtet werden, dass hier bei der Festlegung der Grenze eines Eingriffs auf eine bestimmte Form des Zugriffs auf öffentlich verfügbare Daten und damit auf die Art und Weise der Erhebung – nämlich das gezielte Zusammentragen – abgestellt wird. Dagegen ist die öffentliche Verfügbarkeit ein Umstand der Daten selbst und deren Erhebbarkeit. Es ist daher nicht widersprüchlich, einerseits die Grenze eines Eingriffs von der Art und Weise der Erhebung abhängig zu machen und andererseits eine Intensitätsverringerung grundsätzlich auf Grund einer einfachen Erhebbarkeit und damit auf Grund der einfachen Verfügbarkeit von Daten anzunehmen. Hierzu passt etwa auch, dass das BVerfG in einer Entscheidung zum Gentechnikgesetz[1678] angibt, es wirke sich mildernd auf den Eingriff aus, wenn „der mit der Datenerhebung verbundene Aufwand verhältnismäßig gering"[1679] sei.

Allerdings ließe sich gegen eine Intensitätsverringerung von öffentlich verfügbaren Daten anführen, dass das BVerfG insbesondere in seiner grundlegenden Entscheidung zum RiS – dem Volkszählungsurteil[1680] – bestimmt hat, dass es im Rahmen des RiS gerade kein ‚belangloses' Datum mehr"[1681] gebe. Hieraus ließe sich wiederum auf den ersten Blick ein Widerspruch zur Intensitätsverringerung bei öffentlich verfügbaren Daten

1677 BVerfGE 120, 274 (345); siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)i.

1678 BVerfGE 128, 1 ff.; vgl. hierzu bereits oben unter Kap. 4, B.II.1.b)(1).

1679 BVerfGE 128, 1 (53). Allerdings stellt das BVerfG hier vorrangig darauf ab, dass es für denjenigen, der Angaben gegenüber der zuständigen Behörde abgeben muss, ein verhältnismäßig geringer Aufwand ist, diese Angaben zu machen. Dies ändert aber nichts daran, dass das BVerfG in diesem Zusammenhang insgesamt auf einen geringen Aufwand der Datenerhebung abstellt.

1680 BVerfGE 65, 1 ff.

1681 BVerfGE 65, 1 (45).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ableiten, da insoweit entgegen der grundlegenden Feststellung des BVerfG bei bestimmten Daten eine Abstufung vorgenommen werden würde. Dem steht allerdings entgegen, dass das BVerfG bei seiner Feststellung, dass es im Rahmen des RiS keine belanglosen Daten gebe, „auf die Art der Angaben [abstellt]“[1682]. Die öffentliche Verfügbarkeit von Daten ist dementgegen keine Art der Daten, sondern wiederum nur ein Umstand der Erhebbarkeit der Daten. Dass die Daten öffentlich verfügbar sind, hat keinerlei Auswirkung auf die Frage, welcher Art die Daten sind und welchen Inhalt sie haben.

Schließlich spricht für eine verringerte Intensität bei öffentlicher Verfügbarkeit ein umgekehrter Gleichlauf mit der besonderen Intensitätssteigerung, die dann vorliegt, wenn Daten erhoben werden, bei deren Erhebung grundrechtlich geschützte Vertraulichkeitserwartungen verletzt werden. Denn umgekehrt bestehen bei öffentlich verfügbaren Daten gerade keine Vertraulichkeitserwartungen, da der Betroffene hierbei nicht davon ausgehen kann, dass diese Daten nicht von Dritten zur Kenntnis genommen werden können.[1683] Problematisch hieran ist jedoch, dass das BVerfG bestimmt, „die Eingriffsintensität [sei] hoch, wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG“[1684]. Aus dem ersten Halbsatz dieser Bestimmung lässt sich daher grundsätzlich ableiten, dass die Eingriffsintensität insgesamt bei der Verletzung von Vertraulichkeitserwartungen hoch sei. Der zweite Halbsatz lässt dagegen den Rückschluss zu, dass sich die Verletzung von Vertraulichkeitserwartungen in besonderem Maße intensitätserhöhend auswirkt, wenn die Vertraulichkeitserwartungen auf einem grundrechtlichen Schutz beruhen. Problematisch ist daher die Frage, wie öffentlich verfügbare Daten in diesen Kontext einzuordnen sind. Denn bei öffentlich verfügbaren Daten können keine derartigen Vertraulichkeitserwartungen bestehen.[1685] Allerdings bestimmt das BVerfG in seiner Entscheidung zur polizeilichen Rasterfahndung[1686], dass sich bereits Vertraulichkeitserwartungen intensitätserhöhend auswir-

1682 BVerfGE 65, 1 (45).
1683 Vgl. BVerfGE 120, 351 (361).
1684 BVerfGE 115, 320 (348) mit Verweis auf BVerfGE 109, 279 (313f., 325, 327f.); BVerfGE 113, 348 (364f., 383, 391).
1685 Vgl. BVerfGE 120, 351 (361).
1686 BVerfGE 115, 320 ff.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ken – unabhängig davon, ob diese auf einem grundrechtlichen Schutz beruhen. Vertraulichkeitserwartungen, die nicht auf einem grundrechtlichen Schutz beruhen können etwa berufliche Schweigepflichten sein. Dies lässt insoweit den Rückschluss zu, dass der Ausgangspunkt des Schutzniveaus in diesem Zusammenhang bei Daten liegt, bei denen keinerlei Vertraulichkeitserwartungen bestehen. Das könnte insoweit bedeuten, dass das grundlegende Schutzniveau des RiS bereits bei öffentlich verfügbaren Daten besteht, sodass sich die öffentliche Verfügbarkeit nicht intensitätsverringernd auswirken kann.

In diesem Zusammenhang könnte jedoch zu berücksichtigen sein, dass das Nichtbestehen von Vertraulichkeitserwartungen nicht unbedingt mit der öffentlichen Verfügbarkeit von Daten gleichzusetzen ist. Denn, soweit der Betroffene Kenntnis von der öffentlichen Verfügbarkeit der Daten hat, muss er sich darüber bewusst sein, dass diese ungehindert von jedem Dritten zur Kenntnis genommen werden können. Dagegen ist die Stoßrichtung beim Nichtbestehen von Vertraulichkeitserwartungen eine andere. Denn der Betroffene muss nicht wie bei öffentlich verfügbaren Daten positiv davon ausgehen, dass jeder Dritte die Daten zur Kenntnis nehmen kann, sondern kann nur negativ nicht darauf vertrauen, dass diese nicht vertraulich sind, sondern möglicherweise auch von Dritten zur Kenntnis genommen werden können.

Insoweit lässt sich darauf abstellen, dass das grundlegende Schutzniveau bei Daten vorliegt, bei deren Erhebung keine Vertraulichkeitserwartungen bestehen. Erhöht ist die Intensität dagegen, wenn Vertraulichkeitserwartungen verletzt werden. Verringert ist die Intensität dagegen, wenn die erhobenen Daten öffentlich verfügbar sind.

(2) Zwischenergebnis

Insoweit lässt sich die Rechtsprechung des BVerfG insgesamt dahingehend verstehen, dass es sich intensitätsverringernd auswirkt, wenn die erhobenen Daten öffentlich verfügbar sind.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

c) Art der Verwertung der erhobenen Daten

Auf die Intensität des Grundrechtseingriffs wirkt sich außerdem die Art und Weise der Verwertung der Daten aus.[1687] Dabei ist zunächst zu berücksichtigen, dass das RiS zwar vor dem Hintergrund der Gefahren von informationstechnologischen Datenverarbeitungen entwickelt wurde[1688], sein Schutz aber nicht hierauf beschränkt ist.[1689] So schützt das RiS „generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten"[1690]. Dementsprechend können sich bestimmte Arten der Verwendungs- und Verarbeitungsmöglichkeiten intensitätssteigernd auswirken.[1691]

So ist die Intensität erhöht, wenn mit der Nutzung die Möglichkeit besteht, dass die Informationen für Folgeeingriffe genutzt werden, sowie, wenn die erhobenen Daten auch zu anderen Zwecken genutzt werden können.[1692]

Außerdem wirkt sich bei der elektronischen Datenverarbeitung auch die Menge der erheb- und verwertbaren Daten auf die Intensität aus, sodass etwa bei einer großen Menge an erheb- und verwertbaren Daten eine erhöhte Intensität vorliegt.[1693]

So kommt dem Grundrechtseingriff auch dann erhebliches Gewicht zu, wenn zwar die Einzelinformationen in ihrer Intensität hinter der Intensität der Schutzbereiche der Art. 10, Art. 13 GG zurückbleiben, sich aber durch ihre Zusammenführung und Verknüpfungsmöglichkeiten vielfältige neue Informationen ergeben können, die nach Art und Inhalt eine besonders starke Persönlichkeitsrelevanz haben können.[1694] Denn aus der „Zusammenführung und Kombination […] der […] Datenbestände und ihrem wechselseitigen Abgleich"[1695] lassen sich vielfältige neue Informationen ge-

1687 BVerfGE 120, 378 (Ls. 2).
1688 BVerfGE 65, 1 (41f.); vgl. Dürig/Herzog/Scholz/*Di Fabio,* Art. 2 Rn. 176.
1689 BVerfGE 78, 77 (84).
1690 BVerfGE 78, 77 (84).
1691 Vgl. BVerfGE 120, 378 (Ls. 2).
1692 BVerfGE 113, 348 (365).
1693 So insbesondere BVerfGE 113, 348 (365), wonach „[d]ie Vielzahl der im Rahmen der modernen Telekommunikation erfassbaren Daten […] zu einer besonderen Intensität" führt. Vgl. BVerfGE 65, 1 (42, 45); BVerfGE 113, 29 (45f.); BVerfGE 115, 320 (348), wonach etwa der Abgleich mehrerer Datensätze miteinander intensitätserhöhend wirkt.
1694 BVerfGE 115, 320 (347f.) mit Verweis auf BVerfGE 100, 313 (376); BVerfGE 107, 299 (319f.); BVerfGE 109, 279 (353).
1695 BVerfGE 115, 320 (349).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

winnen, die ebenfalls eine besondere Persönlichkeitsrelevanz haben können.[1696] Da das RiS aber gerade einen umfassenden Schutz der Privatheit und Verhaltensfreiheit ermöglichen soll, müssen insoweit im Rahmen der Intensität des Grundrechtseingriffs auch die Verarbeitungs- und Verknüpfungsmöglichkeiten von Datenberücksichtigt werden.[1697]

Zu berücksichtigen ist allerdings darüber hinaus, dass sich der besondere Schutzgehalt bei bestimmten Datenerhebungsmaßnahmen – etwa solche, die in den Schutzbereich der Art. 13, Art. 10 GG fallen – auch auf die sich daran anschließenden Datenverarbeitungsmaßnahmen erstrecken.[1698]

Dementsprechend müsste es sich umgekehrt allerdings auch intensitätsverringernd auswirken, wenn die Intensität der Datenerhebungsmaßnahme dadurch verringert ist, dass öffentlich verfügbare Daten erhoben werden.[1699]

Ferner müssen beim Einsatz von modernen Ermittlungsmethoden[1700] auch die Gefährdungen durch sog. additive Grundrechtseingriffe beachtet werden.[1701] Insoweit ergibt sich auch eine Intensitätssteigerung durch das Zusammenwirken verschiedener Überwachungsmaßnahmen.[1702]

d) Zwischenergebnis

Aus diesen Kriterien der Rechtsprechung lassen sich insoweit zwei maßgebliche, sozusagen übergeordnete Kriterien zur Bewertung der Grundrechtsintensität ableiten[1703]: einerseits die Persönlichkeitsrelevanz der jeweiligen Informationen und andererseits die Gefährdung der freien Entfaltung der Persönlichkeit insbesondere mit Blick auf die Verhaltensfreiheit[1704] – sowohl auf individueller als auch auf gesellschaftlicher Ebene.

1696 BVerfGE 115, 320 (349); BVerfG BeckRS 2020, 34607 (Rn. 110).
1697 Vgl. BVerfGE 65, 1 (44); BVerfGE 115, 320 (349).
1698 BVerfGE 109, 279 (325f.); BVerfGE 113, 348 (365). Vgl. zu den intensitätssteigernden Umständen von Datenerhebungen bereits soeben unter Kap. 5, C.II.2.b)(2).
1699 Siehe hierzu bereits soeben unter Kap. 5, C.II.2.b)(2)i.
1700 Insbesondere, wenn diese dem Betroffenen verborgen bleiben.
1701 BVerfGE 112, 304 (Ls. 2; 319f.); BVerfGE 141, 220 (280).
1702 BVerfGE 141, 220 (280) mit Verweis auf BVerfGE 112, 304 (319f.); vgl. hierzu bereits BVerfGE 112, 304 (319f.).
1703 Diese sind allerdings wiederum nicht trennscharf voneinander abzugrenzen, sondern bedingen sich wiederum gegenseitig.
1704 Vgl. insoweit die Begründung des Grundrechts auf informationelle Selbstbestimmung BVerfGE 65, 1 (43), wonach es sich insbesondere auch auf die Verhaltens-

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

So ist für die Grundrechtsintensität zunächst die Persönlichkeitsrelevanz der jeweiligen Einzelinformationen relevant. Dabei ist darüber hinaus aber auch die Persönlichkeitsrelevanz der Informationen, die sich aus der Verknüpfung der Einzelinformationen ergeben können, relevant. Insoweit ist etwa auch die Menge der erhobenen und erhebbaren Daten relevant, sowie die technischen Möglichkeiten der Verknüpfung.

Sowohl im Zusammenhang mit der Persönlichkeitsrelevanz der Informationen als auch mit der Gefährdung der Persönlichkeitsentfaltung und Verhaltensfreiheit sind Anlass und Umstände der Erhebung zu berücksichtigen. Dabei wirken sich insbesondere anlasslose, heimliche und solche Datenerhebungen, bei denen (grundrechtlich) geschützte Vertraulichkeitserwartungen verletzt werden, intensitätssteigernd aus. Intensitätsverringernd wirkt es sich dagegen aus, wenn öffentlich verfügbare Daten erhoben werden. Dabei schlägt sich diese Intensitätssteigerung und -verringerung auch auf die anschließende Datenverarbeitung durch. Zu berücksichtigen sind dabei außerdem, die Gefahren, die für die Persönlichkeitsentfaltung durch mehrere miteinander verbundene Grundrechtseingriffe entstehen, die zu einem Gefühl dauerhafter Überwachung führen können.

3. Bewertung der Grundrechtsintensität der hier gegenständlichen Maßnahmen

Nach den vorstehend herausgearbeiteten Kriterien zur Bewertung der Grundrechtsintensität stellt sich nun die Frage, wie die Grundrechtsintensität der hier gegenständlichen Auswertungsmethoden anhand dieser Kriterien zu bewerten ist.

a) Entitätsclustering

Beim sog. *Entitäts-Clustering* ist das Ziel, mehrere *Bitcoin-Adressen* einer einzelnen *Entität* zuzuordnen – sie insoweit zu gruppieren.[1705] Hierzu werden die in der jeweiligen Blockchain enthaltenen Daten systematisch dahingehend analysiert, ob und welche *Bitcoin-Adressen* bei mehreren

weisen des Einzelnen auswirkt, wenn er nicht weiß, welche Daten und Informationen über ihn verfügbar sind.

1705 Siehe hierzu bereits oben unter Kap. 3, A.I.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Transaktionen in unterschiedlichen Kombinationen genutzt werden.[1706] Datengrundlage dieser Auswertungsmethode sind damit die unmittelbaren Blockchain-Daten.[1707]

Technisch und in der Ermittlungspraxis dürften hierbei zwei unterschiedliche Einsatzmöglichkeiten bestehen, die wohl auch eine unterschiedliche Grundrechtsintensität nach sich ziehen: einerseits lässt sich das *Entitäts-Clustering* auf die gesamten Blockchain-Daten anwenden, um so alle dort genutzten und vorhandenen *Bitcoin-Adressen* insgesamt zu *Entitäten* zuzuordnen.[1708] Andererseits wäre es technisch wohl auch möglich, die gesamten Blockchain-Daten nur nach den *Bitcoin-Adressen* einer einzelnen[1709] *Entität* zu durchsuchen.

Nachfolgend wird zunächst auf die Grundrechtsintensität eingegangen, die beiden Einsatzmöglichkeiten gemeinsam ist (hierzu unter (1)), um im Anschluss auf die Unterschiede der Grundrechtsintensität bei diesen Einsatzmöglichkeiten einzugehen (hierzu unter (2)) und abschließend die Grundrechtsintensität des *Entitäts-Clusterings* bewerten zu können (hierzu unter (3)).

(1) Grundrechtsintensität, die bei beiden Einsatzmöglichkeiten vorliegt

Intensitätssteigernd wirkt sich jedenfalls der Umfang der erhobenen Daten in Form der Blockchain-Daten aus. Denn die Blockchain-Daten enthalten umfassend die Transaktionsdaten einer jeweiligen Kryptowährung. Die Erhebung geht insoweit weit über die Erhebung von lediglich einzelnen Informationen hinaus. Es ist außerdem nicht möglich, die Erhebung und Auswertung auf einzelne Daten der Blockchain zu beschränken. Denn einerseits dürfte dies rein technisch schon Schwierigkeiten aufwerfen, da beim Verwenden eines jeweiligen *full-clients* in der Regel die gesamten Blockchain-Daten heruntergeladen werden. Andererseits könnte ohne die gesamten Blockchain-Daten auch nicht die Funktionsfähigkeit der Auswer-

1706 Siehe hierzu im Einzelnen und zu den verschiedenen Möglichkeiten des *Entitäts-Clusterings* ausführlich oben unter Kap. 3, A.I.

1707 Siehe hierzu bereits oben unter Kap. 3, A.I.

1708 Siehe zur Frage, ob in diesem Anwendungsfall überhaupt ein ausreichender Anfangsverdacht vorliegt, bereits oben unter Kap. 5, D.I.2. Hier muss insoweit für die Bewertung der Grundrechtsintensität unterstellt werden, dass ein ausreichender Anfangsverdacht besteht.

1709 Oder auch mehreren, bestimmten.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

tungsmethode gewährleistet werden. Denn eine gesamte *Entität* kann ja gerade nur dadurch zuverlässig, wirksam und vor allem umfassend ermittelt werden, dass die gesamten Blockchain-Daten nach entsprechenden Transaktionsdaten durchsucht werden, die im Zusammenhang mit einer oder mehreren, bestimmten *Bitcoin-Adressen* stehen.[1710] Wenn nur Teile der Transaktionsdaten erhoben und ausgewertet würden, könnten eben nicht alle *Bitcoin-Adressen* einer entsprechenden *Entität* zugeordnet werden.

Zu berücksichtigen ist jedoch zunächst, dass nach der hier vertretenen Auffassung die bloße Erhebung der Blockchain-Daten noch keinen Eingriff in das RiS darstellt, sondern ein Grundrechtseingriff erst bei dem systematischen Datenabgleich der Blockchain-Daten vorliegt.[1711] Da aber auch der Datenabgleich, durch den ein Eingriff in das RiS vorliegt[1712], die gesamten Blockchain-Daten zum Gegenstand hat, wirkt sich jedenfalls in dieser Hinsicht der Umfang der Daten hier intensitätssteigernd aus.

In Bezug auf die Datengrundlage des Abgleichs könnte jedoch intensitätsverringernd zu berücksichtigen sein, dass beim *Entitäts-Clusterings* nur ein einzelner Datenbestand – die Transaktionsdaten der jeweiligen Blockchain – ausgewertet wird und nicht mehrerer Datenbestände miteinander abgeglichen werden.[1713] Nach hier vertretener Auffassung kommt es für die Persönlichkeitsrelevanz und der Gefahr, dass umfassende Persönlichkeitsbilder erstellt werden, jedoch nicht darauf an, ob mehrere verschiedene Datenbestände miteinander zum Abgleich gebracht werden, sondern auf die möglichen Inhalte, die sich aus der Auswertung des jeweiligen Datenbestandes ergeben können.[1714] Da auch nach der Rechtsprechung des BVerfG aus Kontoinformationen erhebliche Rückschlüsse auf das jeweilige Sozialverhalten der Betroffenen abgeleitet werden können[1715], kann daher hier nicht von einer verringerten Grundrechtsintensität ausgegangen werden, nur weil lediglich die Blockchain-Daten ausgewertet werden. Insoweit wirkt es sich nicht intensitätsverringernd aus, dass beim *Entitäts-Clustering* lediglich die jeweiligen Blockchain-Daten ausgewertet werden.

1710 Siehe zur Funktionsweise der *Entitäts-Clustering*-Verfahren im Einzelnen oben unter Kap. 3, A.I.
1711 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c).
1712 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c).
1713 Vgl. insoweit zur geringeren Grundrechtsintensität bei der Abfrage von nur einer einzelnen Datenquelle BVerfG NJW 2009, 1405 (1407).
1714 Siehe hierzu ausführlich oben unter Kap. 5, B.II.3.
1715 BVerfGE 118, 168 (185f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Intensitätsverringernd ist mit Blick auf die Art und den Inhalt der Informationen allerdings zu berücksichtigen, dass die Blockchain-Daten selbst keinen unmittelbaren Rückschluss auf die hinter den *Bitcoin-Adressen* stehenden Personen zulassen.[1716] Zwar dürfte die Ermittlung der jeweiligen Identitäten gerade auch eines der Ziele der Ermittlungsbehörden sein, die Daten selbst sind aber zunächst jedenfalls pseudonymisiert[1717], sodass die Grundrechtsintensität daher verringert ist.

Mit Blick auf die Art und Weise der Anwendung des *Entitäts-Clusterings* ist dagegen intensitätssteigernd zu berücksichtigen, dass das *Entitäts-Clustering* heimlich – also ohne Kenntnis der Betroffenen – stattfindet. Dabei ist insbesondere zu berücksichtigen, dass es auf Grund der vorwiegenden Pseudonymität der Blockchain-Daten nach Abschluss der Auswertung in der Regel überhaupt nicht möglich ist, die von der Auswertung betroffenen Personen hierüber zu informieren, sodass die betroffenen Personen die Rechtmäßigkeit der Maßnahme gerichtlich überprüfen lassen könnten. Dies ist insoweit intensitätssteigernd zu berücksichtigen, als dass der Schutz des RiS gerade auch vor dem Hintergrund der Gefährdung der Persönlichkeitsentfaltung und der Verhaltensfreiheit besteht, die dadurch entstehen können, dass der Einzelne nicht weiß, wer wann was über ihn weiß.[1718] Insoweit kann auf Grund der Heimlichkeit der hier gegenständlichen Auswertungsmethode ein diffuses Überwachungsgefühl bei den einzelnen Nutzern von Blockchain-Technologien entstehen, das insbesondere auch zu einer Verhaltensanpassung führen kann.[1719]

In diesem Zusammenhang ist jedoch wesentlich intensitätsverringernd zu berücksichtigen, dass die ausgewerteten Daten öffentlich verfügbar sind und insoweit die Betroffenen davon ausgehen konnten und wohl auch mussten, dass die Daten von Dritten zur Kenntnis genommen werden. Technisch ist die dezentrale Verwaltung durch die Blockchain-Technologien ja gerade darauf angelegt, dass andere Nutzer die jeweiligen Transaktionen zur Kenntnis nehmen und sie auf Richtigkeit überprüfen und anschlie-

1716 Siehe hierzu bereits ausführlich oben unter Kap. 2, A.II.2. und Kap. 4, B.II.1.c).

1717 So *Finck*, Blockchain and the GDPR, S. 26f. Die in der Blockchain enthaltenen Daten sind pseudonym, da es grundsätzlich durch Zusatzwissen möglich ist, einen Personenbezug herzustellen, *Spindler/Bille,* WM 2014, 1357 (1359); vgl. *Boehm/Pesch*, MMR 2014, 75 (75f.); *Kaulartz,* CR 2016, 474 (480);

1718 BVerfGE 65, 1 (43).

1719 Siehe hierzu insbesondere die bereits entwickelten Möglichkeiten sog. *Mixing-Services,* hierzu bereits ausführlich oben unter Kap. 3, A.I.4.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ßend bestätigen.[1720] Insoweit kann auch kein Vertrauen darauf bestehen, dass staatliche Stellen die jeweiligen Daten nicht zur Kenntnis nehmen.[1721]

Intensitätssteigernd zu berücksichtigen ist dagegen, dass die Auswertung technikgestützt stattfindet und daher weit mehr Verarbeitungs- und Verknüpfungsmöglichkeiten bestehen als bei einer händischen Auswertung. Zwar ließe sich anführen, dass die technische Unterstützung, die bei den *Clustering*-Verfahren eingesetzt wird, grundsätzlich keine umfangreichen Verknüpfungen ermöglichen, sondern weitgehend nur eine erweiterte Suchfunktion darstellt. Denn das *Entitäts-Clustering* beschränkt sich in seiner technischen Umsetzung grundsätzlich darauf, dass die gesamten Blockchain-Transaktionsdaten nach Transaktionen durchsucht werden, bei denen die *Bitcoin-Adresse,* deren *Entität* gesucht wird, ebenfalls genutzt wurde, um zu ermitteln, ob und in welchem Zusammenhang diese *Bitcoin-Adresse* mit anderen *Bitcoin-Adressen* verwendet wurde. Dementsprechend stellt das *Entitäts-Clustering* in seiner Grundfunktion nur eine Suchfunktion nach bestimmten Inhalten dar. Allerdings muss berücksichtigt werden, dass ein derartig umfangreicher Datensatz wie etwa die Bitcoin-Blockchain wohl händisch gar nicht hiernach durchsucht werden könnte. So waren etwa in der Bitcoin-Blockchain am 20. Dezember 2021 mehr als 696 Millionen Transaktionen enthalten.[1722] Diese Transaktionen händisch nach der Verwendung von einer bestimmten *Bitcoin-Adresse* zu durchsuchen dürfte praktisch fast unmöglich sein. Außerdem kann durch ein *Clustering* Verfahren automatisch nicht nur nach Transaktionen einer bestimmten, einzelnen *Bitcoin-Adresse* gesucht werden, sondern darüber hinaus können, wenn bereits eine weitere *Bitcoin-Adresse* einer *Entität* zugeordnet wurde, die Transaktionsdaten der Blockchain nach dieser weiteren *Bitcoin-Adresse* automatisch auch durchsucht werden. Insoweit ist das *Entitäts-Clustering* zwar eines der einfachsten technischen Auswertungsmöglichkeiten, die hier betrachtet werden, im Vergleich zu einer händischen Auswertung, sind die Verknüpfungs- und Verarbeitungsmöglichkeiten durch das *Entitäts-Clustering* jedoch weit erhöht, sodass hiermit auch eine entsprechende Intensitätssteigerung einhergeht.

1720 Siehe zur technischen Funktionsweise des Überprüfungsmechanismus in Blockchain-Systemen bereits ausführlich oben unter Kap. 2, A.II.7.c), III.1.c).

1721 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).

1722 https://www.blockchain.com/charts/n-transactions-total (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(2) Unterschiedliche Grundrechtsintensität

Unterschiedlich ist die Grundrechtsintensität beider Einsatzmöglichkeiten dagegen hinsichtlich der Streubreite und der damit verbundenen Anlasslosigkeit von Grundrechtseingriffen zu bewerten.

So liegt eine erhebliche Streubreite vor, wenn alle *Bitcoin-Adressen,* die in der Blockchain insgesamt vorkommen, zu *Entitäten geclustert* werden. Denn hiervon sind insoweit alle Nutzer der jeweiligen Blockchain betroffen, unabhängig davon, ob sie einen Anlass dafür gegeben haben, der über das bloße Nutzen einer Blockchain hinausgeht. Mit einer derartigen Anwendung des *Entitäts-Clusterings* ginge daher auch eine erhebliche Gefahr mit einher, dass die Nutzer von Blockchains ihr Verhalten entsprechend anpassen.

Dass die Nutzer ihr Transaktionsverhalten bereits entsprechend angepasst haben, zeigt sich bereits daran, dass es mittlerweile die bereits erwähnten *Mixing-Services* gibt, die eingesetzt werden, um ein *Entitäts-Clustering* jedenfalls zu erschweren.[1723]

Insoweit liegt eine erhebliche Intensitätssteigerung vor, wenn die *Entitäts-Clustering*-Verfahren eingesetzt werden, um alle *Bitcoin-Adressen* einer Blockchain zu *Entitäten* zu *clustern.*

Nicht so eindeutig kann dagegen die Frage beantwortet werden, wie die Grundrechtsintensität zu bewerten ist, wenn nur die *Entitäten* bestimmter *Bitcoin-Adressen,* bei denen etwa der Verdacht einer Straftat besteht, ermittelt werden. Problematisch ist nämlich, dass einerseits keine *Entitäts-Cluster* von unbeteiligten Dritten erstellt werden, andererseits stellt sich die Frage, ob nicht die anderen Nutzer, deren *Entitäten* zwar nicht ermittelt werden, deren Transaktionsdaten aber trotzdem abgeglichen werden müssen, um als sog. Nicht-Treffer auszuscheiden, trotzdem in ihren Grundrechten betroffen sind. Insoweit stellt sich hier die Frage, ob auch hier die als Nichttreffer ausgeschiedenen Personen bzw. Daten in ihren Grundrechten betroffen sind. Denn dann läge auch in diesem Anwendungsfall eine erhöhte Streubreite vor, da auch hier anlasslos in die Grundrechte Unbeteiligter eingegriffen werden würde.

1723 Siehe hierzu bereits ausführlich oben unter Kap. 3, A.I.4. Ob dies allerdings am staatlichen Einsatz derartiger *Entitäts-Clustering*-Verfahren oder etwa an einem entsprechenden privaten Einsatz liegt, ist unklar.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Zur Beantwortung dieser Frage muss nochmals die Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung[1724] herangezogen werden. Denn grundsätzlich liegt auch nach dieser neuen Rechtsprechung des BVerfG dann kein Grundrechtseingriff vor, wenn Daten lediglich technikbedingt miterhoben werden und im Anschluss unmittelbar und spurenlos wieder ausgeschieden werden.[1725] Allerdings hat das BVerfG seine Rechtsprechung mit seiner zweiten Entscheidung zur automatisierten Kfz-Kennzeichenkontrolle im Jahr 2018 dahingehend konkretisiert, dass dann kein lediglich technikbedingtes Miterheben vorliegt, wenn sich an den ausscheidenden Daten bereits ein spezifisches Interesse verdichtet hat.[1726] Das BVerfG hat für die automatisierte Kfz-Kennzeichenkontrolle mittlerweile festgestellt, dass hierbei auch ein derartiges spezifisches Interesse an den Nichttreffern bestünde, da die Maßnahme nur dann wirkungsvoll sei, wenn auch die Nichttreffer zunächst miterhoben würden, um so die Treffer zu ermitteln. Insoweit bestünde bei der automatisierten Kfz-Kennzeichenkontrolle ein spezifisches Interesse an den gesamten Daten, da nur so die Maßnahme wirksam sei, sodass auch bei den sog. Nichttreffern ein Grundrechtseingriff vorläge.[1727]

Insoweit stellt sich die Frage, ob und inwieweit die Grundsätze dieser Rechtsprechung bei dem hier gegenständlichen *Entitäts-Clustering,* das zwar nur in Bezug auf bestimmte, einzelne *Bitcoin-Adressen* eingesetzt wird, aber trotzdem die gesamte Blockchain-Daten nach Treffern und eben auch Nichttreffern durchsucht, Anwendung finden können. Sollte nach der Anwendung dieser Grundsätze auch hier ein Grundrechtseingriff für die Nichttreffer vorliegen, läge auch dann eine hohe Streubreite des *Entitäts-Clusterings* vor, wenn dieses nur eingesetzt würde, um die *Entitäten* einzelner *Bitcoin-Adressen* zu ermitteln. Daher stellt sich die Frage, ob hier in vergleichbarer Weise ein großer Datensatz lediglich mit dem Ziel, diesen zu verkleinern, erhoben wurde und insoweit auch ein spezifisches Interesse an den als Nichttreffer ausgeschiedenen Daten besteht.

Dies könnte auf den ersten Blick insoweit der Fall sein, da ja gerade die gesamten Blockchain-Daten nach Treffern einer oder mehrerer bestimmter *Bitcoin-Adressen* abgeglichen werden. Zwar dürfte es auch möglich sein,

1724 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.
1725 BVerfGE 100, 313 (366).
1726 BVerfGE 150, 244 (266). vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.
1727 BVerfGE 150, 244 (266); vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nur einzelne Teilbereiche der Blockchain-Daten nach entsprechenden Treffern zu durchsuchen – etwa die Transaktionsdaten des vergangenen Jahres – das Ziel des *Entitäts-Clusterings* dürfte es aber in der Regel sein, alle *Bitcoin-Adressen* zu ermitteln, die zu einer bestimmten *Entität* gehören. Dieses Ziel kann aber nur dann erreicht werden, wenn auch die gesamten Transaktionsdaten der jeweiligen Blockchain hiernach durchsucht und analysiert werden. Insoweit besteht grundsätzlich zunächst auch ein spezifisches Interesse an den gesamten Blockchain-Daten.

Allerdings muss berücksichtigt werden, dass – anders als bei der automatisierten Erhebung von Kfz-Kennzeichen – in der Erhebung der Blockchain-Daten noch kein Grundrechtseingriff vorliegt, da diese ohnehin öffentlich verfügbar sind.[1728] Insoweit liegt beim *Entitäts-Clustering* noch kein Eingriff dadurch vor, dass die Daten erhoben werden. Sondern der Eingriff liegt erst darin, dass die Daten systematisch ausgewertet werden.[1729] Insoweit liegt auch bei der Erhebung der Blockchain-Daten noch kein Grundrechtseingriff vor, selbst, wenn zum Zwecke des *Entitäts-Clusterings* ein spezifisches Interesse an dem gesamten Datensatz besteht. Dass die Erhebung der Blockchain-Daten selbst keinen Grundrechtseingriff darstellen, während die Erhebung der ebenfalls im öffentlichen Verkehrsraum verfügbaren Kfz-Kennzeichen bereits einen Eingriff darstellen, hat den technischen Hintergrund, dass für die Erhebung der Blockchain-Daten lediglich die Teilnahme an dem jeweiligen Blockchain-Netzwerk erforderlich ist und die gesamten Blockchain-Daten bereits als einheitlicher Datensatz vorhanden sind, wohingegen für die automatisierte Erfassung der Kfz-Kennzeichen zunächst entsprechende technische Anlagen eingerichtet werden müssen und die Kfz-Kennzeichen hiermit erst erfasst werden müssen.[1730] Die Erhebung der für das *Entitäts-Clustering* erforderlichen Daten stellt daher – anders als bei der automatisierten Kfz-Kennzeichenkontrolle – keinen Grundrechtseingriff dar.

Insoweit kann für die Frage der Streubreite nur darauf abgestellt werden, ob im Rahmen des unmittelbaren Datenabgleichs des *Entitäts-Clusterings* ein Grundrechtseingriff hinsichtlich der ausscheidenden Personen vorliegt. Da hierbei aber nur nach Treffern der gesuchten *Bitcoin-Adressen* gesucht

1728 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).
1729 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).
1730 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

wird, lässt sich annehmen, dass die Nichttreffer insoweit spurenlos und unmittelbar technisch ausgeschieden werden.[1731]

Daher liegt hier beim *Entitäts-Clustering* kein Grundrechtseingriff für die ausgeschiedenen Nichttreffer vor. Ein Grundrechtseingriff liegt nur für die ermittelten Treffer vor.

Soweit das *Entitäts-Clustering* etwa eingesetzt wird, um lediglich die *Entität* einer *Bitcoin-Adresse,* die mutmaßlich im Zusammenhang mit einer Straftat steht, zu ermitteln, erfolgt dieser Grundrechtseingriff daher nicht anlasslos.

Insoweit besteht beim Einsatz des *Entitäts-Clusterings* lediglich zur Ermittlung des *Clusters* einer oder mehrerer bestimmter *Bitcoin-Adressen,* bei denen ein Anlass für die Ermittlung besteht, keine erhöhte Streubreite, da jeweils nur ein anlassbezogener Grundrechtseingriff vorliegt und keine Vielzahl von Grundrechtsträgern ohne Anlass betroffen sind.

Festzuhalten bleibt daher, dass die Ermittlung aller *Entitäten* einer jeweiligen Blockchain eine erhebliche Streubreite aufweist und insoweit auch eine erheblich erhöhte Grundrechtsintensität vorliegt.

An dieser erhöhten Grundrechtsintensität fehlt es dagegen, wenn lediglich die *Entität* von einzelnen, bestimmten *Bitcoin-Adressen* ermittelt wird und ein Anlass dieser Ermittlung besteht.

(3) Abschließende Bewertung der Grundrechtsintensität

Vor diesem Hintergrund ergibt sich, dass nur dann ein lediglich geringfügiger Grundrechtseingriff vorliegt, wenn *Entitäts-Clustering*-Verfahren nur in Bezug auf bestimmte, einzelne *Bitcoin-Adressen* eingesetzt werden, bei denen ein Anlass für die Ermittlung besteht. Die Grenze der nach § 161 Abs. 1 StPO zulässigen Grundrechtsintensität ist dagegen überschritten, wenn die *Entitäts-Clustering*-Verfahren eingesetzt werden, um Blockchain-Daten insgesamt nach *Entitäts-Clustern* auszuwerten.

Grund für diese Bewertung ist, dass sich wesentlich intensitätsverringernd die grundsätzliche Pseudonymität der ausgewerteten Daten und die öffentliche Verfügbarkeit auswirken. Dem steht lediglich die geringfügige

1731 Vgl. zum Nichtvorliegen eines Grundrechtseingriffs, wenn Daten technisch spurenlos unmittelbar ausgeschieden werden BVerfGE 100, 313 (366); BVerfGE 150, 244 (266). Vorteilhaft wäre es, wenn technisch tatsächlich abgesichert würde, dass die Nichttreffer ohne irgendwelche weitere Erkenntnismöglichkeiten ausgeschieden werden.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Intensitätssteigerung durch den Umfang der ausgewerteten Daten und deren möglicher Persönlichkeitsrelevanz sowie die Heimlichkeit der Ermittlung und die technikgestützte Auswertung entgegen, die aber insgesamt nicht zu einer Einordnung als grundrechtsintensive Ermittlungsmaßnahme führen. Anders ist dies zu beurteilen, wenn eine erhöhte Streubreite dadurch vorliegt, dass anlasslos eine große Vielzahl von Personen ebenfalls von der Maßnahme betroffen sind.

b) Aufdecken von auffälligem Transaktionsverhalten

Bei dem in Kap. 3, A.II. dargestellten Aufdecken von auffälligem Transaktionsverhalten wird durch die systematische Analyse der Transaktionsdaten, die in der Blockchain enthalten sind, ermittelt, ob und welche Transaktionen von dem durchschnittlichen bzw. typischem Transaktionsverhalten abweichen.[1732] Technisch müssen hierzu zunächst die gesamten Transaktionsdaten der Blockchain analysiert werden, um so zu ermitteln, welches Transaktionsverhalten typisch ist und welches Transaktionsverhalten hiervon abweicht.[1733]

In der Ermittlungspraxis kann diese Auswertungsmethode nur in Bezug auf konkrete einzelne Transaktionen oder *Bitcoin-Adressen* eingesetzt werden. Nur, wenn bei einzelnen Transaktionen oder *Bitcoin-Adressen* bereits aus anderen Gründen der Anfangsverdacht einer Straftat besteht, kann die Auswertungsmethode eingesetzt werden und so der Anfangsverdacht etwa dadurch erhärtet werden, dass die Transaktion oder *Bitcoin-Adresse* tatsächlich auffällig ist. Grund hierfür ist das Erfordernis eines konkreten Anfangsverdachts nach § 161 Abs. 1 StPO.[1734] Insoweit stellt sich die Frage, wie sich dies auf die Grundrechtsintensität des Einsatzes dieser Auswertungsmethode auswirkt.

Hinsichtlich der Datengrundlage – der ausgewerteten Blockchain-Daten – gelten die Ausführungen zur Grundrechtsintensität des *Entitäts-Clusterings*[1735] hier entsprechend. Zusammenfassend soll daher nur kurz festge-

1732 Siehe hierzu im Einzelnen oben unter Kap. 3, A.II.
1733 Siehe hierzu im Einzelnen oben unter Kap. 3, A.II m.w.N.
1734 Siehe zu den Anforderungen des Anfangsverdachts und den daraus resultierenden Folgen für den Einsatz der Auswertungsmethoden ausführlich oben unter Kap. 5, D.I.
1735 Siehe hierzu im Einzelnen oben unter Kap. 5, D.II.3.a)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

halten werden, dass sich der Umfang der erhobenen Daten, sowie deren mögliche Persönlichkeitsrelevanz auf Grund der Nähe zu Kontoinformationen, sowie die heimliche Erhebung und die technikgestützte Auswertung[1736] intensitätssteigernd auswirken. Wesentlich intensitätsverringernd wirken sich dagegen die Pseudonymität der Daten, sowie deren öffentliche Verfügbarkeit aus. Aus diesen Faktoren ergibt sich, dass grundsätzlich ein geringfügiger Grundrechtseingriff bei Erhebung und Auswertung[1737] von Blockchain-Daten vorliegt.

Fraglich ist allerdings, wie in diesem Zusammenhang die Streubreite der Maßnahme zu bewerten ist. Hierbei muss beachtet werden, dass die Auswertungsmethoden einerseits nur in Bezug auf eine konkrete Transaktion oder *Bitcoin-Adresse* vorgenommen wird, sodass insoweit jedenfalls keine große Anzahl Unbeteiligter anlasslos betroffen ist. Andererseits muss beachtet werden, dass um zu diesem Ergebnis, ob eine konkrete Transaktion auffällig ist oder nicht, zunächst ermittelt werden muss, wodurch sich auffälliges bzw. typisches Verhalten auszeichnet. Auch diese vorgelagerte Ermittlung von typischem und auffälligem Transaktionsverhalten ist Teil der hier gegenständlichen Auswertungsmethode.

Insoweit stellt sich die Frage, ob dadurch, dass zunächst der Vergleichsmaßstab, welche Transkationen typisch und welche auffällig sind, eine hohe Streubreite dieser Auswertungsmethode vorliegt.

Da grundsätzlich auch der Datenabgleich einen eigenständigen Grundrechtseingriff darstellt[1738], ließe sich insoweit annehmen, dass auch in der systematischen Analyse nach typischem und untypischem Transaktionsverhalten ein Grundrechtseingriff vorliegt. Insoweit läge hierin auch eine erhöhte Streubreite, die zu einer erhöhten Grundrechtsintensität führen könnte.

Dem ließe sich allerdings entgegenhalten, dass hier zwar grundsätzlich ein Datenabgleich vorliegt, dieser aber gerade nicht mit dem Ziel erfolgt, durch Verknüpfung von Einzelinformationen weitere Informationen über

1736 Zwar liegt hier eine andere Variante der technischen Auswertung vor – nämlich das Ermitteln eines typischen bzw. durchschnittlichen Transaktionsverhaltens in einem ersten Schritt und dann der Vergleich von Transaktionen mit diesem Durchschnitt, dies ändert aber nicht an der Bewertung der Intensität, da auch hier durch den Einsatz von Technik eine Auswertung ermöglicht wird, die so nicht händisch möglich wäre.

1737 Zur Grundrechtsintensität der hier gegenständlichen Auswertungsmethode sogleich im Einzelnen.

1738 Vgl. BVerfGE 150, 244 (266).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

eine oder mehrere einzelne Transaktionen zu erhalten, sondern das Ziel darin liegt, abstrakt einen Vergleichsmaßstab zu erhalten.

Das trifft jedoch nur im ersten Schritt – der Ermittlung des abstrakten Vergleichsmaßstabes – zu. Denn der Vergleichsmaßstab dient ja gerade dazu, einzelne Transkationen mit ihm zu vergleichen und so eine weitere Einzelinformation über die jeweils verfahrensgegenständliche Transaktion zu erhalten – entspricht sie dem typischen Transaktionsverhalten oder nicht.

Daher muss hier grundsätzlich auf Grund der hohen Streubreite auch eine entsprechende Intensitätssteigerung angenommen werden. Auf Grund dieser Intensitätssteigerung liegt hierin grundsätzlich auch kein lediglich geringfügiger Grundrechtseingriff mehr vor.

Um diese erhöhte Grundrechtsintensität zu vermeiden, könnte es in der Ermittlungspraxis aber möglich sein, die Auswertung in einer anderen Art vorzunehmen: So ließe sich die Auswertung technisch etwa auch in Form eines „Treffer-/Nichttreffer-Modells" anwenden, wobei die Auswertung nur im Hintergrund stattfinden würde und lediglich die Transaktion, bei der aus einem anderen Grund ein Verdacht besteht, mit typischem Transaktionsverhalten verglichen wird.[1739] Die Ermittlungsbehörden könnten insoweit selbst nicht auf das Ergebnis der Auswertung, was eine typische Transaktion ist, zugreifen, sondern würden nur das Ergebnis erhalten, ob eine oder mehrere bestimmte Transaktionen typisch oder auffällig sind. Dabei müsste aber technisch und praktisch gewährleistet werden, dass die Ermittlungsbehörden keinen Zugriff auf Inhalt und Ergebnisse dieser Auswertungen im Hintergrund haben. Hierdurch könnte nämlich die Intensität des Grundrechtseingriffs der Auswertungsmethode verringert werden. Denn für die Bewertung der Intensität ist auch maßgeblich, ob die betroffenen Personen anonym bleiben und ob und welche Nachteile die Betroffenen befürchten müssen oder sie nicht ohne Grund befürchten.[1740] Durch die Einsatzmöglichkeit eines „Treffer-/Nichttreffer-Modells" sind zwar auch al-

1739 Ein vergleichbares „Treffer-/Nichttreffer-Modell" wird insbesondere auch beim grenzüberschreitenden Austausch von DNA-Profilen vorgenommen, vgl. insoweit den Beschluss 2008/616/JI des Rates vom 23. Juni 2008.
zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität. Siehe zu diesem Verfahren und dem hieraus resultierenden Grundrechtsschutz außerdem ausführlich *Böse*, Grundsatz der Verfügbarkeit von Informationen, S. 142ff., S. 147.

1740 Vgl. BVerfGE 100, 313 (376); BVerfGE 107, 299 (320).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

le anderen Nutzer der jeweiligen Blockchain von der Auswertungsmethode zunächst betroffen, sie müssen aber keinerlei Nachteile befürchten, wenn die Ergebnisse der systematischen Analyse von typischen Transaktionsverhalten nur in der Weise verwendet werden können, dass einzelne Transaktionen mit dem typischen Transaktionsverhalten verglichen werden können. Außerdem könnte so sichergestellt werden, dass die Personen anonym bleiben. Insoweit ließe sich durch diese Art des Einsatzes der Auswertungsmethode die Intensität der Beeinträchtigung für die Betroffenen verringern, die anlasslos von der Maßnahme betroffen sind.

In dieser Form ließe sich das Aufdecken bzw. in diesem Fall das Ermitteln von auffälligem Transaktionsverhalten noch zulässigerweise als geringfügigen Grundrechtseingriff auf § 161 Abs. 1 StPO stützen.

c) Vergleich mit bekanntem Transaktionsverhalten

Die in Kap. 3, A.III. dargestellten Auswertungsmethoden weisen bestimmte Ähnlichkeiten zu den soeben bereits bewerteten Auswertungsmethoden auf, gehen teilweise aber auch über sie hinaus.[1741] Denn bei den Auswertungsmethoden mit dem Oberbegriff des „Vergleichs mit bekanntem Transaktionsverhalten" werden im Grundsatz wiederum die in der Blockchain enthaltenen Daten systematisch analysiert, in diesem Fall aber noch – vereinfacht gesprochen – mit Zusatzwissen kombiniert, um so genauere Informationen etwa über die Hintergründe der Transaktionen zu erhalten.[1742]

So können etwa durch das in Kap. 3, A.III.1. dargestellte Verfahren Transaktionen bzw. *Entitäten* ermittelt werden, die mutmaßlich im Zusammenhang mit Betrug stehen. Hierzu wird in einem ersten Schritt durch einen *Classifier* das typische Transaktionsmuster ermittelt, das bei Transaktionen besteht, die im Zusammenhang mit Betrug stehen. Durch die so abstrahierten Merkmale von Betrugstransaktionen kann dann die Blockchain nach ähnlichen Transaktionsmustern durchsucht werden.

Vergleichbar ist die in Kap. 3, A.III.2. dargestellte Auswertungsmethode, bei der ebenfalls in einem ersten Schritt Transaktionen analysiert wurden, die im Zusammenhang mit Schneeballsystemen auf der Ethereum-Blockchain standen. Durch das ebenfalls so abstrahierte Transaktionsmuster

1741 Siehe zu diesen Auswertungsmethoden im Einzelnen oben unter Kap. 3, A.III.
1742 Vgl. hierzu bereits oben unter Kap. 3, A.III.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

konnte anschließend die Ethereum-Blockchain nach vergleichbaren Transaktionsmustern durchsucht werden.

Ähnlich, aber noch etwas weitgehender bzw. breiter angelegt, ist die in Kap. 3, A.III.3. darstellte Auswertungsmethode der sog. *Labelling*-Verfahren. Hierbei wurde wiederum eine bestimmte Datengrundlage mittels *Classifier* analysiert, um so die abstrakten Transaktionsmuster bestimmter Anwendungsmöglichkeiten von *Bitcoin-Adressen* zu erhalten und anschließend die Blockchain-Daten nach dem Vorliegen vergleichbarer Transaktionsmuster zu durchsuchen. Die *Labelling*-Verfahren gehen insoweit über den Vergleich mit Betrugs- und Schneeballtransaktionen hinaus, als dass hierbei einerseits in einem vorgelagerten Schritt zunächst die in der Blockchain enthaltenen *Bitcoin-Adressen* zu *Entitäten* gruppiert werden. Andererseits wird zwar ebenfalls ein *Classifier* eingesetzt, um abstrakt Transaktionsmuster zu ermitteln, hierbei werden aber nicht nur ein einzelnes Transaktionsmuster – wie das von Betrugs- oder Schneeballtransaktionen – ermittelt, sondern Ziel war etwa die Ermittlung von insgesamt sechs verschiedenen *Labels,* u.a. *Exchange-* und *Mixing-Services*.[1743]

Gemeinsam ist diesen Auswertungsmethoden insoweit, dass sie auf Grund von bestimmtem Hintergrundwissen zunächst auf einer abstrakten Ebene in einem sog. Trainingsschritt die typischen Transaktionsmuster von bestimmten Anwendungsbereichen ermitteln, um im Anschluss nach weiteren Transaktionen zu suchen, die diesem Muster ähnlich sind.

Auf Grund des erforderlichen Anfangsverdachts[1744] können diese Auswertungsmethoden in der Ermittlungspraxis nur eingesetzt werden, um weitere Hintergründe zu einer bestimmten, bereits aus einem anderen Grund als verdächtig eingestuften Transaktion zu ermitteln. So könnte etwa die Identität einer bestimmten Person, die über eine oder mehrere bestimmte *Bitcoin-Adressen* verfügt, dadurch ermittelt werden, dass die Transaktionen dieser *Bitcoin-Adresse* nachverfolgt werden und sobald sie bei einem *Exchange-Service* angelangt sind, die Identität des Kunden abgefragt wird, die die entsprechende *Bitcoin-Adresse* verwendet hat.[1745] Dabei ist zu

1743 Siehe hierzu im Einzelnen bereits oben unter Kap. 3, A.III.3.

1744 Siehe insoweit zu der weiteren Variante des Einsatzes, bei der die Blockchain-Daten unmittelbar nach Transaktionsmustern durchsucht werden, die auf bestimmte Straftaten hindeuten und dem hierbei fehlenden Anfangsverdacht oben unter Kap. 5, D.I.2.c)

1745 Vgl. zur Pflicht der Kundenidentifizierung im Rahmen der Geldwäscheprävention bereits oben unter Kap. 4, B.II.1.c)(1). Die Strafverfolgungsbehörden sind nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG berechtigt, im Fall des

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

berücksichtigen, dass eine unmittelbare Abfrage der Identitätsdaten der bestimmten *Bitcoin-Adresse* beim Anbieter eines *Exchange-Services* nur dann möglich ist, wenn eine unmittelbare Transaktion zwischen der „verdächtigen" *Bitcoin-Adresse* und der *Bitcoin-Adresse* des *Exchange-Services* stattgefunden hat. Da wohl insbesondere diejenigen, die ihre *Bitcoin-Adressen* zum Zwecke illegaler Aktivitäten verwenden, keinen unmittelbaren Kontakt zu *Exchange-Services* haben, die im Rahmen Geldwäscherechtlicher Präventionspflichten zur Kundenidentifizierung verpflichtet sind, dürften die Auszahlungen in Fiat-Geld wohl in der Regel über mindestens eine weitere *Bitcoin-Adresse* stattfinden. Für die Strafverfolgungsbehörden dürfte es aber möglich sein, dass auch die Identitäten dieser noch unverdächtigen *Bitcoin-Adresse* abgefragt werden, um anschließend, bei der so ermittelten Person eventuell weitere Anhaltspunkte für die Identitätsermittlung der unmittelbar verdächtigen *Bitcoin-Adresse* zu erhalten.

Hinsichtlich der Grundrechtsintensität dieser Auswertungsmethoden ist wiederum auf die gegenständliche Datengrundlage der Blockchain-Daten und deren Erhebung zu verweisen[1746]: intensitätssteigernd wirken sich der Umfang und die Heimlichkeit der erhobenen und ausgewerteten Daten der Blockchain aus, sowie deren Persönlichkeitsrelevanz auf Grund der Nähe zu Kontoinformationen. Intensitätsverringernd wirken sich dagegen Pseudonymität und öffentliche Verfügbarkeit der ausgewerteten Daten aus.

Darüber hinaus muss bei der hier gegenständlichen Auswertungsmethode die umfangreiche technische Unterstützung intensitätssteigernd berücksichtigt werden. Denn, wenn bei den *Entitäts-Clustering*-Verfahren noch darauf abgestellt wurde, dass diese vergleichsweise technisch simpel seien, ist dies insbesondere bei den hier gegenständlichen *Labelling*-Verfahren anders zu beurteilen. Bei den *Labelling*-Verfahren wird nämlich ein *Clustering*-Verfahren für die gesamten Blockchain-Daten vorgeschaltet. Darüber hinaus werden die Transaktionsdaten etwa dahingehend ausgewertet, welche Höhe eingehende und ausgehende Transaktionen haben, wie viele *Bit-*

Verdachts einer Straftat diese Daten bei den entsprechenden Anbietern abzufragen. Praktisch dürfte allerdings das Problem bestehen, dass selbst wenn bekannt ist, dass diese *Bitcoin-Adresse* von einem *Exchange-Service* verwendet wird, noch nicht klar ist, welcher *Exchange-Service* dies ist. Allerdings dürfte es wohl möglich sein, bei allen von der BaFin genehmigten Unternehmen, die derartige Services anbieten, eine entsprechende Abfrage zu machen, soweit die Informationen, welche *Bitcoin-Adresse* zu welchem *Exchange-Service* gehören nicht gespeichert werden, sondern nur zur Identifizierung der unmittelbar „verdächtigen" *Bitcoin-Adresse* verwendet werden.

1746 Siehe hierzu bereits oben unter Kap. 5, D.II.3.a)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

coin-Adressen für ein- und ausgehende Transaktionen verwendet werden und wie viele *Bitcoin-Adressen* nur für einzelne Transaktionen verwendet werden. Diese Auswertungen beziehen sich jeweils auf alle *Entitäten.* Dementsprechend gehen die technischen Möglichkeiten dieser Auswertungen weit über das händisch Mögliche hinaus und ermöglichen systematische Verknüpfungen von Einzelinformationen.

Außerdem muss ebenfalls intensitätssteigernd berücksichtigt werden, dass durch das Erstellen von Transaktionsmustern weitergehende Informationen über einzelne Transaktionen und *Entitäten* erhalten werden können. Dementsprechend ist die Persönlichkeitsrelevanz insoweit erhöht. Soweit es auf die Verknüpfung mehrerer Datenbestände ankommen sollte[1747], ergibt sich insoweit ebenfalls eine Intensitätssteigerung dadurch, dass die in der Blockchain enthaltenen Daten mit Zusatzinformationen zu einzelnen Hintergründen verknüpft werden.

Fraglich ist wiederum, wie in diesem Zusammenhang die Streubreite des Einsatzes dieser Auswertungsmethode zu bewerten ist.

Denn problematisch ist hier wiederum, dass die Auswertungsmethode wiederum mehrere Schritte der Datenverarbeitung voraussetzt. So muss in einem ersten Trainingsschritt anhand von Transaktionsdaten mit bekanntem Hintergrund das Transaktionsmuster von bestimmten Akteuren ermittelt werden. Dabei muss außerdem berücksichtigt werden, dass zur Ermittlung dieses einzelnen Transaktionsmusters auch alle weiteren, in der Blockchain enthaltenen Transaktionsdaten herangezogen werden müssen. Denn ein bestimmtes Transaktionsmuster kann nur durch den Vergleich mit anderen Transaktionsmustern ermittelt werden. Die besonderen Eigenschaften von Mustern ergeben sich insoweit nur aus dem Vergleich mit den Eigenschaften aller anderen Transaktionen. Erst nach diesem umfangreichen Trainingsschritt kann ermittelt werden, ob eine oder mehrere bestimmte Transaktionen Ähnlichkeiten mit diesem Transaktionsmuster aufweisen. Für den hier beschriebenen Einsatz der Auswertungsmethode in der Form, dass bei Transaktionen oder *Bitcoin-Adressen,* die bereits aus einem anderen Grund verdächtig sind, geprüft werden soll, ob sie etwa mit einem *Exchange-Anbieter* interagiert hat, muss also zunächst das Transaktionsmuster eines *Exchange-Anbieters* dadurch ermittelt werden, dass die Transaktionen von *Exchange-Anbietern* mit allen anderen in der Blockchain enthaltenen Transaktionen verglichen werden. Dementsprechend besteht hier zunächst

1747 Vgl. BVerfG NJW 2009, 1405 (1406f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

eine hohe Streubreite, die zu einer erhöhten Grundrechtsintensität führt, die über das nach §§ 161, 163 StPO zulässige Maß hinausgeht.

In Betracht kommt aber auch hier, die Intensität wiederum durch eine Art „Treffer-/Nichttreffer-Modell" zu verringern. So könnte etwa bei einer verdächtigen *Bitcoin-Adresse* zunächst deren „naheliegenden" Transaktionen und *Bitcoin-Adressen* betrachtet werden. Naheliegend wären dann etwa die Transaktionen oder *Bitcoin-Adressen,* mit denen die verdächtige *Bitcoin-Adresse* unmittelbar oder maximal über 2-3 weitere Transaktionen interagiert hat. Bildlich gesprochen ergäbe sich so ein Kreis um die verdächtige *Bitcoin-Adresse* herum. In diesem umliegenden Kreis könnte dann geprüft werden, ob eine der *Bitcoin-Adressen* etwa einer *Entität* zuzuordnen ist, die Kundenidentifizierungspflichten unterliegt, um so Anhaltspunkte für die Identitätsermittlung der verdächtigen *Bitcoin-Adresse* zu erhalten.

Dabei müsste wiederum sichergestellt werden, dass die Ergebnisse der Auswertungsmethode – also das Transaktionsmuster bestimmter *Labells* – nicht zur Kenntnis genommen werden kann. Es dürfte von den Strafverfolgungsbehörden nur eingesehen werden, ob es in einem zu definierenden naheliegenden Umkreis um die verdächtige *Bitcoin-Adresse* eine *Entität* mit einem Transaktionsmuster, das auf eine Identifizierungspflicht hindeutet, gibt.

So würde wiederum die Anonymität aller anderen Nutzer der Blockchain gewahrt werden. Außerdem würde sichergestellt, dass Nutzer nur anlassbezogen betroffen wären. Für die identifizierungspflichtigen Dienstleister bestünde dieser Anlass zwar unabhängig von einem Verdacht einer Straftat. Allerdings wurde die Identifizierungspflicht bei Dienstleistern im Umfeld von Kryptowährungen gerade mit dem Ziel eingeführt, die Anonymität bei Kryptowährungen aufheben zu können.[1748]

(1) Exkurs – Grundrechtsintensität beim Einsatz zum Aufdecken von Transaktionsmustern, die auf bestimmte Straftaten hindeuten

Alternativ ließe sich diese Auswertungsmethode grundsätzlich auch einsetzen, um anhand von Transaktionsmustern, die auf bestimmte illegale Aktivitäten hindeuten, unmittelbar Transaktionen zu ermitteln, die mutmaßlich im Zusammenhang mit Straftaten stehen. Zwar ist dieser Einsatz nach

1748 So Erwägungsgrund Nr. 9, RL (EU) 2018/843, die mit der am 01.01.2020 in Kraft getretenen Änderung von KWG und GwG umgesetzt wurde, vgl. BT.-Drs. 19/13827.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

§ 161 Abs. 1 StPO auf Grund des hierfür erforderlichen Anfangsverdachts nicht zulässig, seine Grundrechtsintensität soll hier jedoch trotzdem kurz dargestellt werden. Denn fraglich ist, ob eine durch ein „Treffer-/Nichttreffer-Modell" verringerte Grundrechtsintensität auch dann vorliegen kann, wenn die gesamten Blockchain-Daten nach Transaktionsmustern durchsucht werden, die unmittelbar auf bestimmte illegale Aktivitäten hindeuten.

Denn einerseits dürfte insoweit eine erhöhte Anzahl an Personen betroffen sein – nämlich alle, die dieses Transaktionsmuster tatsächlich aufweisen. Andererseits muss in diesem konkreten Anwendungsfall berücksichtigt werden, dass diese Personen ja nicht anlasslos betroffen werden. Sondern der Grund hierfür liegt darin, dass sie ein Transaktionsmuster aufweisen, das unmittelbar auf illegale Aktivitäten hindeutet.

So nimmt das BVerfG in seinem MIKADO-Beschluss vom 17.2.2009[1749] an, dass bei dem Abgleich „allgemeine[r] Merkmale […] regelmäßig auch zahlreiche unbeteiligte Personen"[1750] betroffen sind. Dies soll dagegen nicht der Fall sein, wenn im Rahmen der Abfrage von Kreditkartendaten, gezielt nach Personen gesucht werde, die mit hinreichender Wahrscheinlichkeit strafbare Handlungen vorgenommen haben.[1751] Da nur die Daten von Personen, bei denen auf Grund der bestimmten Kreditkartenbuchung eine hinreichende Wahrscheinlichkeit für das Vorliegen einer Straftat bestand, übermittelt wurden, wurden auch diejenigen Personen, bei denen die entsprechende Buchung nicht vorlag, nicht in ihren Grundrechten betroffen.

Hiernach wären von der Ermittlung bestimmter illegaler Transaktionsmuster auch nur diejenigen Personen in ihren Grundrechten betroffen, bei denen ein entsprechendes Transaktionsmuster vorliegt. Bei diesen bestünde aber auf Grund des Transaktionsmusters ein entsprechender Anlass, dass sie Gegenstand der Ermittlungsmaßnahme geworden sind, sodass keine Vielzahl Unbeteiligter Personen betroffen wäre.

Fraglich ist aber auch hier, ob diese vom BVerfG im MIKADO-Beschluss aufgestellten Grundsätze nach der zweiten Entscheidung zur automatisierten Kfz-Kennzeichen-Erfassung[1752] noch gelten können. Denn hierin hat das BVerfG festgelegt, das auch diejenigen, die auf Grund des Datenabgleichs mit dem Fahndungsbestand unmittelbar als „Nichttreffer" ausge-

1749 BVerfG NJW 2009, 1405 ff.
1750 BVerfG NJW 2009, 1405 (1406).
1751 BVerfG NJW 2009, 1405 (1407).
1752 BVerfGE 150, 244 ff. Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b)(1)iv.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

schieden wurden, durch die Erfassung und den Abgleich in ihrem RiS betroffen seien. Zu berücksichtigen ist jedoch, dass das BVerfG auch in seiner zweiten Entscheidung zur automatisierten Kfz-Kennzeichenerfassung bei dem Grundsatz verbleibt, dass weiterhin dann kein Grundrechtseingriff vorliegt, wenn die Daten lediglich technikbedingt miterhoben werden, und anschließend unmittelbar anonym und ohne weiteres Erkenntnisinteresse wieder ausgesondert werden. Das BVerfG formuliert insoweit von diesem Grundsatz nur eine Rückausnahme dahingehend, dass ein Eingriff jedoch dann vorliegen soll, wenn „die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung" sei.[1753] Ob in diesem Zusammenhang bei der Erhebung eines großen Datenbestandes ein Eingriff in das RiS vorliege, hänge maßgeblich davon ab, ob sich „bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet habe, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen"[1754] sei. Abweichend von diesen Grundsätzen ist bei dem hier gegenständlichen Einsatz der Auswertungsmethode zunächst zu berücksichtigen, dass die Erhebung der Blockchain-Daten zunächst noch keinen Eingriff in das RiS begründet.[1755] Darüber hinaus muss beachtet werden, dass zwar grundsätzlich das Ziel verfolgt wird, die „Treffer" von bestimmten, auf illegale Aktivitäten hindeutenden Transaktionsmuster zu ermitteln und insoweit auch das Ziel verfolgt wird, die erfassten Datenbestände zu verkleinern. Anders als bei der automatisierten Kfz-Kennzeichenerfassung ist dies aber nicht das einzig verfolgte Ziel der Erhebung der Blockchain-Daten. Denn diese müssen allein technikbedingt vollständig erhoben werden. Es besteht kein unmittelbares Interesse daran „alle Treffer" zu erhalten, sondern für die Strafverfolgung kann es bereits ausreichen, einige „Treffer" zu ermitteln. Insoweit lässt sich bei einer Gesamtbetrachtung nicht annehmen, dass sich ein spezifisches Interesse an den erhobenen Daten verdichtet hat, das einen Grundrechtseingriff begründen kann.

Dementsprechend können weiterhin die Grundsätze des MIKADO-Beschlusses hier Anwendung finden, sodass auch hier keine Vielzahl Unbeteiligter betroffen ist, wenn die Betroffenheit auf einer konkreten Grundlage

1753 BVerfGE 150, 244 (266).

1754 BVerfGE 150, 244 (266) mit Verweis auf BVerfGE 115, 320 (343) und BVerfGE 120, 378 (398).

1755 Siehe hierzu bereits oben ausführlich unter Kap. 4, B.II.2.c)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

beruht, die mit hinreichender Wahrscheinlichkeit auf ein strafbares Verhalten hindeutet. Insoweit hängt die Grundrechtsintensität dieses Einsatzes der Auswertungsmethode maßgeblich von der Zuverlässigkeit der Auswertungsmethode ab. Denn nur, wenn auf Grund eines bestimmten Transaktionsmusters tatsächlich eine hinreichende Wahrscheinlichkeit eines strafbaren Verhaltens vorliegt, wird hinreichend ausgeschlossen, dass Unbeteiligte in ihren Grundrechten betroffen sind.

(2) Zwischenergebnis

Bei der Auswertungsmethode des Vergleichs mit bekanntem Transaktionsverhalten liegt allenfalls ein noch geringfügiger Grundrechtseingriff, der nach § 161 Abs. 1 StPO zulässig wäre, vor, wenn in der beschriebenen Form eines „Treffer-/Nichttreffer-Modells" nur naheliegende Transaktionen und *Bitcoin-Adressen* auf einen bestimmten Hintergrund untersucht werden.

Hinsichtlich der Suche nach Transaktionsmustern, die unmittelbar auf strafbares Verhalten hindeuten, liegt zwar der für § 161 Abs. 1 StPO erforderliche Anfangsverdacht nicht vor[1756], die Maßnahme könnte jedoch auf Grund der Rechtsprechung des BVerfG im MIKADO-Beschluss[1757] noch als geringfügiger Grundrechtseingriff zu bewerten sein.

d) Auswertung des Netzwerkverhaltens und der Netzwerkverbindungen

Darüber hinaus muss die Grundrechtsintensität der in Kap. 3, B. dargestellten Auswertungsmethoden bewertet werden, bei denen maßgeblich das Netzwerkverhalten im Blockchain-Netzwerk ausgewertet wird, um so insbesondere die jeweiligen IP-Adressen den *Bitcoin-Adressen* zuordnen zu können.[1758]

Hierzu wird nachfolgend zunächst auf die grundlegende Möglichkeit der Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten eingegangen (hierzu unter (1)), um anschließend auf die zusätzlich möglichen Auswertungen im Zusammenhang mit dem *Tor-Netzwerk* einzugehen (hierzu unter (2), (3)). Abschließend wird die Grundrechtsintensität der sog. *Bloom-Filter-Attacks* bewertet (hierzu unter (4)).

1756 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.2.c).
1757 BVerfG NJW 2009, 1405ff.
1758 Siehe hierzu ausführlich oben unter Kap. 3, B.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(1) Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten

Zur Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten wurde eine Verbindung mit allen *Full-nodes* hergestellt, um so die Verbreitung von Transaktionsnachrichten im Bitcoin-Netzwerk nachverfolgen zu können und so die IP-Adresse des ersten Absenders der *Bitcoin-Adresse,* die Absender der Transaktionsnachricht war, zuordnen zu können.[1759]

Hinsichtlich der Grundrechtsintensität auf Grund des Umfangs der erhobenen Daten muss hier abweichend von den bereits bewerteten Auswertungsmethoden berücksichtigt werden, dass die Auswertung der Weiterleitung der Transaktionsnachrichten nicht auf der Grundlage aller Blockchain-Daten stattfindet. Dahingehend ist der Umfang der ausgewerteten Daten insoweit geringer als der Umfang der Blockchain-Daten. Allerdings geht der Umfang der ausgewerteten Daten in anderer Hinsicht weit über die Auswertung der Blockchain-Daten hinaus. Denn zur Auswertung des Netzwerkverhaltens muss neben den jeweiligen Transaktionsnachrichten auch erhoben werden, wie sich diese Transaktionsnachrichten jeweils im Netzwerk von allen *Full-nodes* verbreitet hat. Hierzu wurde zunächst eine unmittelbare Verbindung zu allen *Full-nodes* hergestellt, um so von jedem *Full-node* die von ihm weitergeleiteten Transaktionsnachrichten zu erheben und zu speichern. Auf Grund dieser umfangreichen Daten der Netzwerkverbindungen ist auch für die Auswertung des Netzwerkverhaltens eine Intensitätserhöhung auf Grund des Umfangs der erhobenen und ausgewerteten Daten anzunehmen.

Ein weiterer Unterschied zu den bereits bewerteten Auswertungsmethoden liegt darin, dass bei der Auswertung des Netzwerkverhaltens bereits in der Erhebung und Speicherung ein Eingriff in das RiS vorliegt – anders als bei der Erhebung der Blockchain-Daten.[1760] Denn insbesondere hier liegt bereits eine gezielte Speicherung der Verbindungsdaten vor.[1761]

Ebenfalls abweichend könnte zu berücksichtigen sein, dass bei der Auswertung des Netzwerkverhaltens zunächst einmal keine umfassenden Persönlichkeitsbilder erstellt werden können bzw. sollen, da das Ziel der Maßnahme ja darin liegt, *Bitcoin-Adressen* einer IP-Adresse zuzuordnen und nicht die Transaktionen selbst ausgewertet werden wie bei den vorstehend bewerteten Auswertungsmethoden. Insoweit sind zunächst nicht die

1759 Siehe hierzu im Einzelnen ausführlich unter Kap. 3, B.I.
1760 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c)(1).
1761 Siehe hierzu bereits oben unter Kap. 4, B.II.2.c)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

mit Kontoinformationen vergleichbaren Transaktionsdaten der Blockchain Gegenstand der Auswertung, sondern nur das Weiterleitungsverhalten der *Full-nodes*. Allerdings muss auch beachtet werden, dass hiervon ja gerade auch die Transaktionsnachrichten beinhaltet sind – diese werden ja gerade weitergeleitet. Insoweit liegt das Ziel zwar nicht in dem Erstellen von Persönlichkeitsprofilen anhand von Daten, die mit Kontoinformationen vergleichbar sind, es ist aber anhand der Datengrundlage ebenso möglich – auch wenn der Umfang der Transaktionsdaten im Vergleich zu den umfangreichen Blockchain-Daten beschränkt ist. Daher ist auch hier die Gefahr, dass umfassende Persönlichkeitsbilder erstellt werden, intensitätssteigernd zu berücksichtigen. Soweit dagegen für die Intensitätssteigerung darauf abgestellt wird, dass Daten aus mehreren verschiedenen Quellen miteinander abgeglichen werden, ließe sich auf den ersten Blick zwar annehmen, dass hier eine einheitliche Datenquelle bestünde. Allerdings muss beachtet werden, dass bei der Auswertung des Netzwerkverhaltens gerade die Weiterleitungsdaten aller *Full-nodes* erhoben werden müssen. Insoweit liegen hier auch unzählig viele einzelne Datenquellen vor, die jeweils miteinander zum Abgleich gebracht werden.

Im Vergleich zu den zuvor bewerteten Auswertungsmethoden ist außerdem intensitätssteigernd zu berücksichtigen, dass hier die erhobenen und ausgewerteten Daten teilweise einen Rückschluss auf die dahinterstehenden Personen zulassen. Denn Ziel der Auswertung ist es ja gerade, eine *Bitcoin-Adresse* einer IP-Adresse zuordnen zu können, die jedenfalls einer natürlichen oder juristischen Person zugeordnet werden kann.[1762] Insoweit geht die Auswertung des Netzwerkverhaltens über die Auswertung der unmittelbaren Blockchain-Daten hinaus, da diese vorwiegend pseudonym waren. Die hier betrachteten Netzwerkverbindungsdaten sind aber gerade personenbeziehbar. Dies muss insbesondere gelten, wenn die Verschleierung von IP-Adressen über das *Tor-Netzwerk* aktiv im Rahmen der Auswertungsmethode verhindert werden.

Ebenfalls intensitätssteigernd wirkt sich hier aus, dass die Maßnahme wiederum heimlich erfolgt und es praktisch nicht möglich sein wird, alle Betroffenen hierüber zu informieren.

Dagegen ergibt sich keine weitergehende Intensitätssteigerung daraus, dass sich die Strafverfolgungsbehörden zur Erhebung der Daten mit den Betroffenen in eine Kommunikationsbeziehung begeben. Zwar kann sich

1762 Vgl. EuGH NJW 2016, 3579 Ls. 1.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

eine dauerhafte Täuschung gegenüber einer Vielzahl Betroffener intensitätssteigernd auswirken[1763], zu berücksichtigen ist hier jedoch, dass ein Grundrechtseingriff nach dem BVerfG nur dann vorliegt, wenn „dabei ein schutzwürdiges Vertrauen in die Identität und die Motivation seines Kommunikationspartners" besteht[1764]. Bei den hier gegenständlichen Auswertungen des Netzwerkverhaltens liegt dagegen nur eine Kommunikationsbeziehung zu allen *Full-nodes* über das öffentlich zugängliche Blockchain-Netzwerk vor. Auf Grund der öffentlichen Zugänglichkeit des Netzwerkes kann daher kein schutzwürdiges Vertrauen in die jeweiligen Kommunikationspartner bestehen.[1765]

In diesem Zusammenhang ist jedoch die maßgebliche Intensitätsverringerung zu berücksichtigen, die sich gerade aus der öffentlichen Zugänglichkeit des Netzwerkes ergibt. Denn die hier gegenständlichen Daten werden eben aus dem öffentlich zugänglichen Blockchain-Netzwerk erhoben, so dass grundsätzlich kein Vertrauen der Betroffenen an deren Vertraulichkeit besteht.

Besonders intensitätssteigernd ist jedoch wiederum die technische Auswertung zu berücksichtigen. Denn wiederum wäre es sowohl bei der Masse der Transaktionsdaten als auch hier insbesondere bei den darüberhinausgehenden Daten über die Weiterleitung der Transaktionsnachrichten keinesfalls möglich, diese händisch auszuwerten. Eine solche Auswertung ist nur technikgestützt möglich. Dementsprechend kann die IP-Adresse einer *Bitcoin-Adresse* nur dadurch zugeordnet werden, dass hier eine technikgestützte Auswertung stattfindet.

Fraglich ist, wie wiederum die Streubreite dieser Auswertungsmethode zu bewerten ist und ob es die Möglichkeit gibt, die Auswertungsmethode mit einer geringen Streubreite einzusetzen.

Ursprünglich wurde die Auswertungsmethode in der Form eingesetzt, dass über einen längeren Zeitraum zunächst die Daten über die Weiterleitung von Transaktionsnachrichten von allen *Full-nodes* erhoben wurden und anschließend danach ausgewertet wurden, von welchem *Full-node* welche Transaktionsnachricht zuerst in das Blockchain-Netzwerk versandt wurde. Ziel war es insoweit, möglichst viele *Bitcoin-Adressen* einer IP-Adresse zuordnen zu können, unabhängig von einem konkreten Anlass. Insoweit besteht bei dieser Form des Einsatzes eine stark erhöhte Streubrei-

1763 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.II.1.c)
1764 BVerfGE 120, 274 (345).
1765 Vgl. BVerfGE 120, 274 (345f.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

te, die zu einer derart erhöhten Grundrechtsintensität führt, dass sie nicht mehr als geringfügig einzustufen ist.

In Betracht kommt jedoch, die Auswertung des Netzwerkverhaltens anlassbezogen vorzunehmen. So könnte etwa die Auswertungsmethode wiederum eingesetzt werden, wenn eine konkret verdächtige *Bitcoin-Adresse* vorliegt, um diese möglichst einer IP-Adresse zuzuordnen. In diesem Fall müssten dann wiederum die Daten über die Weiterleitung der Transaktionsnachricht von allen *Full-nodes* erhoben werden, um so zu ermitteln, ob die verdächtige *Bitcoin-Adresse* eine Transaktion getätigt hat und über die Auswertung der Verbreitung dieser Transaktionsnachricht die IP-Adresse ermittelt werden kann.

Insoweit würden grundsätzlich nur anlassbezogen die jeweiligen Daten über das Weiterleitungsverhalten erhoben und ausgewertet werden.

Problematisch ist in diesem Zusammenhang jedoch, dass anders, als bei der Auswertung der unmittelbaren Blockchain-Daten hier bereits in der Erhebung der Daten ein Eingriff in das RiS vorliegt.[1766] Zwar ließe sich zunächst anführen, dass auch diese Daten lediglich technikbedingt miterhoben würden und anschließend anonym und spurenlos wieder gelöscht würden, sodass in diesem Fall kein Grundrechtseingriff vorliegt.[1767] Allerdings muss auch hier wiederum die Rechtsprechung des BVerfG zur automatisierten Kfz-Kennzeichenerfassung beachtet werden, nach der jedoch ein Grundrechtseingriff vorliegt, wenn die Daten lediglich mit dem Ziel der Verkleinerung erhoben werden und sich insoweit ein spezifisches Interesse an den erhobenen Daten bereits verdichtet hat. Anders als bei den vorstehend bereits bewerteten Auswertungen der unmittelbaren Blockchain-Daten, muss hier berücksichtigt werden, dass die Auswertung des Netzwerkverhaltens in Bezug auf eine konkrete *Bitcoin-Adresse* nur dann wirksam ist, wenn die Daten der Weiterleitung aller Transaktionsnachrichten erhoben werden. Denn nur so kann gewährleistet werden, dass im Falle einer neuen Transaktion der verdächtigen *Bitcoin-Adresse* diese auch einer IP-Adresse zugeordnet werden kann. Dementsprechend liegt auch hier eine umfassende Datenerhebung mit dem Ziel der Verkleinerung vor, sodass hier auch die „Nichttreffer" in ihrem RiS betroffen sind und insofern eine große Anzahl an Personen in ihren Grundrechten betroffen ist, die keinen Anlass hierfür gegeben hat. Daher liegt auch dann, wenn die Daten des Netzwerkverhaltens nur im Falle einer verdächtigen *Bitcoin-Adresse*

1766 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.c)(2).
1767 Vgl. BVerfGE 100, 313 (366).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ausgewertet werden, eine hohe Streubreite vor, die zu einer entsprechend hohen Grundrechtsintensität führt.

Aus diesem Grund liegt – unabhängig von der konkreten Einsatzmöglichkeit – eine erhöhte Streubreite und damit ein erhöhter Grundrechtseingriff vor, der nicht mehr nur geringfügig ist.

(2) Auswertung der Verbreitung von Transaktionsnachrichten, wenn zusätzlich eine Verbindung über das Tor-Netzwerk verhindert wird

Fraglich ist, ob sich hinsichtlich dieser Grundrechtsintensität etwas verändert, wenn zur Datenerhebung die Verbindung über das *Tor-Netzwerk* verhindert wird.

Insoweit könnte sich die Frage stellen, ob hier eine weitere Steigerung der Grundrechtsintensität dadurch vorliegt, dass berechtigte Vertraulichkeitserwartungen überwunden werden.[1768] Dies ist jedoch hier nicht der Fall, denn auch in dem Fall, dass die Verbindung über das *Tor-Netzwerk* verhindert wird, werden die maßgeblichen Daten über eine öffentlich zugängliche Verbindung mit dem Blockchain-Netzwerk erhoben. Insoweit wird nur verhindert, dass im Rahmen der Datenerhebung die IP-Adressen der Betroffenen verschleiert werden, an der Erhebung selbst ändert sich allerdings nichts. Deshalb ändert sich auch nichts an den nichtbestehenden Vertraulichkeitserwartungen bei der Datenerhebung, sodass auch hier insgesamt von einer gesteigerten Grundrechtsintensität ausgegangen werden muss, die nicht mehr als geringfügig einzustufen ist.

(3) Auswertung des Datenverkehrs des Tor-Netzwerks

Das Gleiche muss selbst dann gelten, wenn darüber hinaus die Daten ausgewertet werden, die dadurch erhoben werden, dass die Strafverfolgungsbehörden selbst *Tor-Exit-Relays* bereitstellen, um so die Kommunikation, die über das *Tor-Netzwerk* mit dem Blockchain-Netzwerk stattfindet, erheben und auswerten zu können. Denn insoweit muss wiederum gelten, dass in dieser Kommunikationsbeziehung kein berechtigtes und schutzwürdiges Vertrauen besteht.[1769] Soweit die so erhobenen Daten in vergleichba-

1768 Vgl. zu dieser Intensitätssteigerung bereits unter Kap. 5, C.II.2.b)(2).
1769 Siehe hierzu bereits Kap. 4, B.II.2.c)(2).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

rer Weise ausgewertet werden, muss insoweit eine entsprechend erhöhte Grundrechtsintensität vorliegen, die ebenfalls als nicht mehr geringfügig anzusehen ist.

(4) Bloom-Filter-Attacks

Auch mit den in Kap. 3, B.III. dargestellten sog. *Bloom-Filter-Attacks* lassen sich IP-Adressen einzelnen *Bitcoin-Adressen* zuordnen.

Hierzu wird die Verwendung von sog. *Bloom-Filtern* bei den sog. *SPV-Clients* ausgenutzt.[1770] *SPV-Clients* werden zur Datenminimierung eingesetzt, damit Bitcoin auch über mobile Endgeräte genutzt werden kann. Hierzu hinterlegt der *SPV-Client* in einem *Bloom-Filter* bei einem *Full-node* die *Bitcoin-Adressen,* die für den Nutzer des *SPV-Clients* relevant sind – in der Regel *Bitcoin-Adressen,* über die der *SPV-Client* verfügt. Bei neuen Transaktionsnachrichten fragt dann der *Full-node* bei diesem *Bloom-Filter* ab, ob eine der *Bitcoin-Adressen* der neuen Transaktionsnachrichten im *Bloom-Filter* enthalten ist, um so nur die neuen Transaktionsnachrichten an den *SPV-Client* weiterzuleiten, die auch für den Nutzers des *SPV-Clients* relevant sind.

Bei der *Bloom-Filter-Attack* fragt nun der *Full-node,* bei dem der *Bloom-Filter* des *SPV-Clients* hinterlegt ist, alle bisher in der Blockchain verwendeten *Bitcoin-Adressen* und die dazugehörigen *public keys* ab, um so zu ermitteln, welche *Bitcoin-Adressen* zur *Wallet* des *SPV-Clients* gehören. Da zwischen *Full-node* und *SPV-Client* eine Netzwerkverbindung bestehen muss, kennt der *Full-node* die IP-Adresse des *SPV-Clients* und kann so die ermittelten *Bitcoin-Adressen* dessen IP-Adresse zuordnen.

Der Umfang der so ermittelten Daten und die damit einhergehenden Grundrechtsintensität hängen von der Art und Weise des Einsatzes der *Bloom-Filter-Attack* ab. So könnte sie grundsätzlich etwa nur in Bezug auf einen speziellen *SPV-Client* eingesetzt werden, um dessen *Bitcoin-Adressen* jeweils einer IP-Adresse zuzuordnen. Insoweit bestünde lediglich ein relativ geringer Umfang an erhobenen Daten.

Dies dürfte in der Ermittlungspraxis allerdings wenig zielführend sein. Denn ein vorrangiges Ziel der Ermittlungen liegt ja darin, die Identität hinter einer bestimmten *Bitcoin-Adresse* zu ermitteln.[1771] Bei der *Bloom-Filter-*

1770 Siehe hierzu im Einzelnen unter Kap. 3, B.III.
1771 Siehe hierzu bereits oben unter Kap. 5, B.II.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Attack ist aber vorher nicht bekannt, welche *Bitcoin-Adressen* der jeweilige *SPV-Client* verwaltet – dies soll ja gerade ermittelt werden. Insoweit wäre es ein Glückstreffer, wenn nur mit einer einzelnen *Bloom-Filter-Attack* bei einem *SPV-Client* die IP-Adresse einer bestimmten, verdächtigen *Bitcoin-Adresse* ermittelt werden könnte.

Daher ist es wahrscheinlicher, dass die *Bloom-Filter-Attack* in der Ermittlungspraxis eher in der Form eingesetzt wird, dass bei einer verdächtigen *Bitcoin-Adresse* die *Bloom-Filter-Attack* bei allen möglichen *SPV-Clients* eingesetzt wird, um so eventuell die IP-Adresse der verdächtigen *Bitcoin-Adresse* ermitteln zu können.

In diesem Fall ist die Grundrechtsintensität der Auswertungsmethode bereits auf Grund des Umfangs der erhobenen Daten jedenfalls erhöht. Denn hierbei müssen jedenfalls die gesamten Blockchain-Daten erhoben werden, um so alle bisher verwendeten *Bitcoin-Adressen* abgleichen zu können.

Ebenfalls stark erhöht ist die Grundrechtsintensität außerdem auf Grund der hohen Streubreite, die dieser Form des Einsatzes der *Bloom-Filter-Attack* einhergeht. Denn bei dieser Form des Einsatzes ist eine große Anzahl Unbeteiligter in ihren Grundrechten betroffen, da wohl auch alle abgefragten *SPV-Clients,* die nicht über die verdächtige *Bitcoin-Adresse* verfügen als „Nichttreffer" in ihrem RiS betroffen sind. Nach dem BVerfG liegt nämlich auch ein Eingriff in das RiS der Personen vor, die als „Nichttreffer" ausgeschieden werden, wenn „die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung"[1772] sei und sich bei einer Gesamtbetrachtung das behördliche Interesse an den erhobenen Daten bereits in einer einen Grundrechtseingriff auslösenden Weise verdichtet habe.[1773] Wenn also die *Bloom-Filter-Attack* bei allen verfügbaren *SPV-Clients* eingesetzt wird, um so die IP-Adresse einer bestimmten, verdächtigen *Bitcoin-Adresse* zu ermitteln, ist diese Maßnahme nur erfolgversprechend, wenn sie auch tatsächlich bei allen verfügbaren *SPV-Clients* eingesetzt wird. Daher hat sich beim Einsatz der *Bloom-Filter-Attack* bereits ein spezifisches Interesse an den anschließend ausscheidenden Daten verdichtet, sodass auch die „Nichttreffer" in ihrem RiS betroffen sind und demensprechend eine hohe Streubreite vorliegt.

Darüber hinaus muss intensitätssteigernd berücksichtigt werden, dass durch die *Bloom-Filter-Attacks* ein unmittelbarer Personenbezug möglich

1772 BVerfGE 150, 244 (266).
1773 BVerfGE 150, 244 (266).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

gemacht wird und insoweit die Gefahr besteht, dass ein Persönlichkeitsprofil, das auf Grund der Blockchain-Daten erstellt wird, einer Person zugeordnet werden kann. Soweit nach anderer Auffassung auf die Verknüpfung unterschiedlicher Datenquellen abgestellt wird, liegt auch diese durch den Abgleich der *Bitcoin-Adressen,* die in der Blockchain gespeichert sind, mit den in den *Bloom-Filtern* hinterlegten *Bitcoin-Adressen* vor. Auch insoweit wäre die Grundrechtsintensität entsprechend erhöht.

Ferner ist wiederum die technische Unterstützung intensitätssteigernd zu berücksichtigen, da hieraus wiederum Rückschlüsse und Informationen gewonnen werden können, die durch einen händischen Abgleich nicht möglich wären.

Diesen intensitätssteigernden Aspekten steht wiederum maßgeblich die öffentliche Verfügbarkeit der erhobenen und ausgewerteten Daten gegenüber. Denn einerseits sind zunächst die in die Blockchain enthaltenen *Bitcoin-Adressen* öffentlich verfügbar. Andererseits beruht die Auswertung der *Bloom-Filter* darauf, dass sich die Strafverfolgungsbehörden in eine Telekommunikationsbeziehung mit den betroffenen *SPV-Clients* begeben, um so deren *Bloom-Filter* abgleichen zu können. Allerdings besteht kein schutzwürdiges Vertrauen der Nutzer, die die *SPV-Clients* verwenden, in die mit den *Full-nodes* geführte Telekommunikation.

Diese Faktoren – insbesondere die hohe Streubreite – führen insgesamt zu einer erhöhten Grundrechtsintensität des Einsatzes von *Bloom-Filter-Attacks,* die nicht mehr als geringfügig anzusehen sind.

Darüber hinaus könnte die *Bloom-Filter-Attack* auch unabhängig von einem bestehenden Verdacht eingesetzt werden, um so möglichst viele *Bitcoin-Adressen* einer IP-Adresse zuzuordnen, damit in einem Verdachtsfall auf diese Daten zurückgreifen zu können. Dieser Einsatz entspricht daher einer Datensammlung auf Vorrat. Insoweit würde sich jedoch die Streubreite nochmals erhöhen, sodass die Grundrechtsintensität auch hier jedenfalls nicht mehr als geringfügig einzuordnen ist.

(5) Zwischenergebnis

Bei allen Auswertungen des Netzwerkverhaltens und der Netzwerkverbindungen liegt auf Grund der erhöhten Streubreite ein nicht mehr nur geringfügiger Grundrechtseingriff vor.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

e) Auswertung durch Verknüpfung mit anderweitig verfügbaren Daten

Die Grundrechtsintensität der in Kap. 3, C. dargestellten Auswertungsmethoden durch eine Verknüpfung von anderweitig verfügbaren Daten hängt u.a. auch von deren konkretem Einsatz ab.

(1) Durchsuchen des Internets nach Bitcoin-Adressen

Wenn etwa das Internet nach *Bitcoin-Adressen* durchsucht wird, um so Anhaltspunkte für die dahinterstehende Identität zu erhalten[1774], dürfte insbesondere der bisher maßgebliche Faktor der Streubreite vom konkreten Einsatz abhängen.

Denn einerseits ist es möglich, in einem konkreten Verdachtsfall das Internet nach einer verdächtigen *Bitcoin-Adresse* zu durchsuchen – etwa einfach mit Google. In diesem Fall dürfte die Streubreite verhältnismäßig gering sein, denn soweit etwa über Foren-Beiträge oder Ähnlichem Anhaltspunkte für die Identität der verdächtigen *Bitcoin-Adresse* erhalten werden, erfolgt dies jedenfalls anlassbezogen. Außerdem wäre auch der Umfang der erhobenen Daten verhältnismäßig gering. Intensitätssteigernd wären allerdings sowohl die heimliche Erhebung, sowie die Gefahr, dass anschließend personenbezogene Persönlichkeitsprofile erstellt werden könnten[1775] zu berücksichtigen. Andererseits muss wiederum intensitätsverringernd berücksichtigt werden, dass sowohl die Blockchain-Daten als auch die durchsuchten Daten des Internets öffentlich verfügbar sind. Insoweit ließe sich im Fall dieses Einsatzes noch ein geringfügiger Grundrechtseingriff annehmen.

Andererseits ist es eben auch möglich, durch einen *Web-Crawler* das Internet systematisch nach der bestimmten Zeichenstruktur von *Bitcoin-Adressen* und *public keys* zu durchsuchen, um so möglichst viele Daten über möglichst viele *Bitcoin-Adressen* zu erhalten[1776], die dann im Fall eines konkreten Verdachts genutzt werden können. Der Einsatz würde insoweit anlasslos erfolgen und damit eine besonders hohe Streubreite aufweisen, sodass jedenfalls kein geringfügiger Grundrechtseingriff mehr vorliegt.

1774 Siehe hierzu im Einzelnen oben unter Kap. 3, C.I.
1775 Bzw., dass hier ein Abgleich mehrerer unterschiedlicher Datenquellen stattfindet.
1776 Siehe hierzu im Einzelnen oben unter Kap. 3, C.I.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(2) Auswertung von Dritt-Anbieter-Cookies

Bisher ist noch nicht eindeutig klar, wie konkret die Auswertung von Dritt-Anbieter-Cookies zum Zweck der Strafverfolgung eingesetzt werden kann. So stellt sich für die Bewertung der Grundrechtsintensität insbesondere die Frage danach, wie die von den Dritt-Anbieter-Cookies erhobenen Daten von den Strafverfolgungsbehörden erhoben werden können und ob diese nur in einem konkreten Verdachtsfall erhoben werden können, ohne dass die Daten von Dritten hiervon betroffen sind. Darüber hinaus dürfte die Grundrechtsintensität auch davon abhängen, welchen Umfang die erhobenen Daten haben. Dabei muss auch berücksichtigt werden, dass jedenfalls die Blockchain-Daten einen großen Umfang haben und durch die zusätzliche Auswertung von Dritt-Anbieter-Cookies weitergehende Rückschlüsse mit möglicher Persönlichkeitsrelevanz haben können[1777].

(3) Standortdaten-Ermittlung bei IoT-Blockchain-Anwendung

Ebenfalls bisher noch nicht klar ist, wie die von *Shahid et.al.*[1778] lediglich theoretisch dargestellte Auswertung von IoT-Blockchain-Anwendungen tatsächlich eingesetzt werden kann. Daher kann auch hier wiederum nur auf die Faktoren, die für die Bewertung der Grundrechtsintensität maßgeblich werden können, eingegangen werden.

So dürfte hier in einem besonderen Maße der Umfang der erhobenen Daten sowie deren mögliche Persönlichkeitsrelevanz zu beachten sein. Denn, wenn mittels der in der Blockchain enthaltenen Daten durch die Verknüpfung von Einzelinformationen konkrete Bewegungsprofile von einzelnen Personen erstellt werden können, erhöht dies die Grundrechtsintensität in besonderem Maße.

Darüber hinaus dürfte wiederum maßgeblich zu beachten sein, wie zielgerichtet wie Maßnahme eingesetzt werden kann und, ob eine hohe Anzahl Unbeteiligter hiervon betroffen sein kann.

1777 Bzw. es werden mehrere unterschiedliche Daten miteinander abgeglichen.

1778 *Shahid/Pissinou/Njilla/Alemany/Imteaj/Makki/Aguilar*, MobiQuitous '19 2019, 116 (116ff.).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

f) Kombination von Auswertungsmethoden

Wenn schließlich in der Ermittlungspraxis die einzelnen Auswertungsmethoden miteinander kombiniert werden, erhöht sich die Grundrechtsintensität jeweils um die Intensität der jeweiligen Auswertungsmethode.

Insoweit muss etwa berücksichtigt werden, dass etwa bei der Kombination von *Labelling*-Verfahren und Auswertung des Weiterleitungsverhaltens der Transaktionsnachrichten zunächst jedenfalls die Streubreite nochmals erhöht ist. Darüber hinaus muss in diesem Zusammenhang in besonderem Maße auch die erhöhte Gefahr der Persönlichkeitsrelevanz berücksichtigt werden. Denn einerseits wird es insbesondere über die Zuordnung einer IP-Adresse zu einer *Bitcoin-Adresse* möglich, einen konkreten Personenbezug herzustellen. Andererseits ist es außerdem möglich, mittels der systematischen Auswertung der Transaktionsmuster weitergehende Rückschlüsse zu erhalten, die abhängig von den Daten der jeweiligen Trainingsgrundlage und auch besondere Persönlichkeitsrelevanz haben könnten.

Insoweit führt die Kombination mehrere Auswertungsmethoden zu einer erhöhten Grundrechtsintensität, die jedenfalls nicht mehr geringfügig ist.

g) Zwischenergebnis

Als noch geringfügiger Grundrechtseingriff zulässig ist das *Entitäts-Clustering,* soweit es nur in einem Verdachtsfall bezogen auf eine verdächtige *Bitcoin-Adresse* eingesetzt wird. Die Grenze der Geringfügigkeit wird allerdings auf Grund einer erhöhten Streubreite überschritten, wenn anlasslos alle in einer Blockchain enthaltenen *Bitcoin-Adressen* zu *Entitäten* gruppiert werden.

Bei dem Aufdecken von auffälligem Transaktionsverhalten besteht ebenfalls das Problem der erhöhten Streubreite, die zu einer erhöhten Grundrechtsintensität führt, da jedenfalls eine systematische Auswertung aller in der Blockchain enthaltenen Transaktionsdaten erforderlich ist. Insoweit ist allenfalls der Einsatz der Auswertungsmethode in Form eines „Treffer-/Nichttreffer-Modells“ als noch geringfügiger Grundrechtseingriff zulässig, da so vermieden werden kann, dass die Betroffenen, die keinen Anlass für die Ermittlung gegeben haben, Gegenstand strafrechtlicher Ermittlungen werden.

Ein ähnliches Problem stellt sich auch bei den als *Labelling*-Verfahren bezeichneten Auswertungsmethoden. Denn auch hier müssen jedenfalls

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

alle in der Blockchain enthaltenen Transaktionsdaten zunächst systematisch ausgewertet werden, damit ein Vergleichsmaßstab besteht. Auf Grund dieser hohen Streubreite ist daher wiederum allenfalls der Einsatz dieser Auswertungsmethode in vergleichbarer Form wie ein „Treffer-/Nichttreffer-Modell" als noch geringfügiger Grundrechtseingriff vorstellbar, um so zu vermeiden, dass Unbeteiligte Gegenstand strafrechtlicher Ermittlungen werden. Hinsichtlich des Einsatzes eines *Labelling*-Verfahrens zur Ermittlung von noch unbekannten Transaktionen, die auf Grund ihres Transaktionsmusters auf bestimmte illegale Aktivitäten hindeuten, hängt die Zulässigkeit als geringfügiger Grundrechtseingriff davon ab, wie zuverlässig die Ergebnisse dieser Auswertungsmethode sind.

Bei der Auswertung des Netzwerkverhaltens stellt sich die Bewertung der Grundrechtsintensität noch etwas anders dar, denn hier besteht bereits bei der Erhebung der jeweiligen Datengrundlage ein Eingriff in das RiS. Insoweit besteht etwa bereits bei der grundlegenden Auswertung der Daten über die Weiterleitung von Transaktionsnachrichten auch dann eine erhöhte Streubreite, wenn sie nur in Bezug auf eine konkret verdächtige *Bitcoin-Adresse* vorgenommen wird. Denn hierzu müssen grundsätzlich alle Weiterleitungsdaten mit dem Ziel, diese wiederum zu verkleinern, erhoben werden, sodass bereits in der Erhebung und Aussonderung der „Nichttreffer" ein Grundrechtseingriff vorliegt, der zu einer entsprechenden Streubreite und damit einhergehenden erhöhten Grundrechtsintensität führt. Gleiches gilt, soweit darüber hinaus die Verbindung über das *Tor-Netzwerk* verhindert wird und die über das *Tor-Netzwerk* übermittelten Daten in vergleichbarer Weise ausgewertet werden. Insoweit besteht hier jedenfalls keine geringfügige Grundrechtsintensität mehr.

Ähnlich gilt dies für die sog. *Bloom-Filter-Attacks.* Denn in der Ermittlungspraxis wird diese Auswertungsmethode so eingesetzt werden müssen, dass nicht nur ein einzelner *SPV-Client* abgefragt wird, sondern möglichst alle verfügbaren. Insoweit ergibt sich auch hier wiederum eine erhöhte Streubreite, da auch hier bereits auch für die „Nichttreffer" ein Grundrechtseingriff vorliegt, der sich daraus ergibt, dass die gesamten Daten mit dem Ziel der Verkleinerung erhoben werden. Dementsprechend ist auch der Einsatz der *Bloom-Filter-Attacks* wohl in der Regel auch als nicht mehr geringfügig einzustufen.

Anders stellt sich die Grundrechtsintensität dar, wenn lediglich das Internet anlassbezogen nach Anhaltspunkten zur Identitätsermittlung durchsucht wird – dann dürfte der Grundrechtseingriff noch geringfügig sein. Die Grenze der Geringfügigkeit ist jedoch überschritten, wenn anlassunab-

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

hängig mittels *Web-Crawler* die öffentlich verfügbaren Inhalte im Internet nach möglichst vielen Hintergrundinformationen durchsucht werden, um so hierauf im Verdachtsfall zurückgreifen zu können.

Hinsichtlich der Auswertung von Dritt-Anbieter-Cookies und IoT-Blockchain-Anwendungen hängt die jeweilige Grundrechtsintensität grundsätzlich von deren konkreter Umsetzung ab. Dabei dürfte insbesondere relevant werden, ob und welche Rückschlüsse auf die Persönlichkeit gezogen werden können und ob und wie viele Unbeteiligte von den Auswertungsmethoden betroffen werden.

Schließlich liegt auf Grund der erhöhten Streubreite und Gefahr der Persönlichkeitsrelevanz kein geringfügiger Grundrechtseingriff mehr vor, wenn die einzelnen Auswertungsmethoden miteinander kombiniert werden.

4. Zwischenergebnis

Ein lediglich geringfügiger Grundrechtseingriff liegt dann vor, wenn die in Kap. 3, A. dargestellten Auswertungsmethoden, die als Datengrundlage die unmittelbaren Blockchain-Daten nutzen, anlassbezogen eingesetzt werden und dabei sichergestellt wird, dass unbeteiligt Betroffene nicht Gegenstand eines Strafverfahrens werden können und deren personenbezogene Daten nur zu Vergleichszwecken betroffen werden. Ebenfalls nur geringfügig ist auch der Grundrechtseingriff, bei der anlassbezogenen Suche nach weiteren Anhaltspunkten im öffentlich zugänglichen Internet.

Der Einsatz aller weiteren Auswertungsmethoden ist als nicht mehr geringfügig anzusehen. Hintergrund dieser unterschiedlichen Einordnung ist maßgeblich, dass bei allen Auswertungsmethoden, die nicht nur die jeweiligen Blockchain-Daten als Grundlage nutzen, bereits in der gezielten Erhebung und Speicherung der jeweiligen Daten ein Grundrechtseingriff vorliegt, der eine entsprechend höhere Streubreite auslöst.

III. Zwischenergebnis

Dementsprechend können nur die Kap. 3, A., C.I. dargestellten Auswertungsmethoden zulässigerweise auf §§ 161, 163 StPO gestützt werden, wenn sie lediglich in Bezug zu einem konkreten Straftatverdacht eingesetzt werden. Eine darüber hinausgehende Anwendung der Auswertungsmethoden

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ist dagegen nicht mehr durch die Ermittlungsgeneralklauseln der §§ 161, 163 StPO verfassungsrechtlich gerechtfertigt.

E. Zusammenfassung

Aus den vorstehenden Ausführungen ergibt sich zunächst, dass als Ermächtigungsgrundlage für den Einsatz der hier gegenständlichen Auswertungsmethoden des Kapitels 3 nur die Ermittlungsgeneralklauseln der §§ 161, 163 StPO einschlägig sein können.

Zwar ermächtigt insbesondere § 98a StPO zu einem maschinellen Datenabgleich und damit zu einem Eingriff in das RiS. Der Anwendungsbereich des § 98a StPO ist allerdings in mehrfacher Hinsicht eingeschränkt und besonders geprägt von der ursprünglichen Rasterfahndung. Dementsprechend ist § 98a StPO für die hier gegenständlichen Auswertungsmethoden selbst dann nicht einschlägig, wenn man der hier vertretenen Auffassung folgt, dass auch der Datenabgleich von nur einer Speicherstelle in den Anwendungsbereich des § 98a StPO fällt, wenn eine Datenabfrage und ein Datenabgleich mit dem Ziel, einen unbestimmten Personenkreis zu ermitteln, stattfindet. Denn die Datengrundlage des maschinellen Datenabgleichs des § 98a StPO ist auf Grund des begrenzten Wortlauts auf Daten, die entweder freiwillig herausgegeben wurden oder zuvor nach § 98a Abs. 2 StPO erhoben bzw. übermittelt wurden, beschränkt. Insoweit kann § 98a StPO nicht einschlägig sein, wenn – wie bei den hier gegenständlichen Auswertungsmethoden – zuvor Daten aus öffentlich zugänglichen Quellen von den Strafverfolgungsbehörden erhoben wurden.

Insoweit bestätigt sich das bereits eingangs erwähnte Problem, dass der Fokus der Ermittlungsbefugnisse der StPO auf der Erhebung von bestimmten Daten liegt und nicht auf bestimmten Datenverarbeitungsmaßnahmen.

Die hier einschlägigen Ermittlungsgeneralklauseln der §§ 161, 163 StPO genügen grundsätzlich den verfassungsrechtlichen Anforderungen an die Einschränkung des RiS.

Sie können allerdings nur eine verfassungsrechtliche Rechtfertigung für geringfügige Grundrechtseingriffe darstellen, da sie einerseits als Generalklauseln relativ unbestimmt sind und andererseits zur Ermittlung sämtlicher Straftaten einschlägig sind und insoweit nur bei geringfügigen Grundrechtseingriffen verhältnismäßig sind.

Ob ein geringfügiger Grundrechtseingriff bei den hier gegenständlichen Auswertungsmethoden vorliegt, hängt maßgeblich auch davon ab, ob hier

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

eine noch geringe Streubreite vorliegt. Dies hängt teilweise wiederum von dem konkreten Einsatz der Auswertungsmethoden ab.

Dementsprechend genügen die §§ 161, 163 StPO als verfassungsrechtliche Rechtfertigung für die hier gegenständlichen Auswertungsmethoden nur dann, wenn die unmittelbaren Blockchain-Daten nur im konkreten Verdachtsfall und auch nur in Bezug auf diesen konkreten Verdachtsfall ausgewertet werden und, wenn technisch sichergestellt wird, dass Daten, die nicht Gegenstand des konkreten Verdachts sind, ohne weitere Erkenntnisse ausgesondert werden. Darüber hinaus kann das öffentlich zugängliche Internet auch anlassbezogen nach weiteren Informationen durchsucht werden.

Dem entgegen besteht durch die §§ 161, 163 StPO keine ausreichende verfassungsrechtliche Rechtfertigung für die Auswertungsmethoden, die in Kap. 3, B. dargestellt wurden. Denn anders als bei der Auswertung der unmittelbaren Blockchain-Daten liegt bei den in Kap. 3, B. dargestellten Auswertungsmethoden in der Regel bereits durch die Datenerhebung ein Eingriff in das RiS vor, sodass sich die Streubreite entsprechend maßgeblich erhöht.

Außerdem bieten die Ermittlungsgeneralklauseln keine verfassungsrechtliche Rechtfertigung für den Einsatz der in Kap. 3, A. dargestellten Auswertungsmethoden, wenn diese in der Form eingesetzt werden, dass auch Erkenntnisse über Personen, die nicht Gegenstand des konkreten Verdachts sind, hieraus hervorgehen können.

Soweit darüber hinaus die Erkenntnisse der jeweiligen Auswertungsmethoden miteinander kombiniert werden, steigert sich die Grundrechtsintensität, sodass die §§ 161, 163 StPO keine ausreichende verfassungsrechtliche Rechtfertigung mehr bieten.

Dementsprechend kann eine Verletzung des RiS durch die Anwendung der hier gegenständlichen Auswertungsmethoden vorliegen.

F. Lösungsvorschlag – § 98a Abs. 2 S. 2 StPO-E

Da der Einsatz der hier gegenständlichen Auswertungsmethoden nur teilweise durch die §§ 161, 163 StPO verfassungsrechtlich gerechtfertigt ist, empfiehlt sich die Schaffung einer neuen, ausreichenden Rechtsgrundlage für den Einsatz der Auswertungsmethoden.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dabei muss berücksichtigt werden, dass in § 98a StPO bereits eine verfassungsgemäße[1779] Ermächtigungsgrundlage besteht, die grundsätzlich zu einem Eingriff in das RiS in Form der Auswertung von personenbezogenen Daten ermächtigt, der eben auch eine Vielzahl an unbeteiligten Personen betrifft.[1780] Insoweit bietet § 98a StPO bereits eine ausreichend bestimmte[1781] und verhältnismäßige Ermächtigungsgrundlage für maschinelle Datenabgleiche, bei der technikgestützt eine große Menge personenbezogener Daten ausgewertet werden.

Es bietet sich daher an, § 98a Abs. 2 StPO um folgenden Satz 2 zu erweitern:

> *„Zu diesem Zweck sind die Strafverfolgungsbehörden außerdem ermächtigt, allgemein zugängliche Daten zu erheben und für den Abgleich zu verarbeiten."*

Hierdurch könnte gewährleistet werden, dass auch die hier gegenständlichen Auswertungsmethoden in den Anwendungsbereich der Rasterfahndung nach § 98a StPO fallen würden. Denn, dass die hier gegenständlichen Auswertungsmethoden nicht vom Anwendungsbereich des § 98a StPO erfasst sind, beruht nach der hier vertretenen Auffassung nur darauf, dass die Datengrundlage des maschinellen Datenabgleichs in § 98a Abs. 1 StPO auf Grund des begrenzten Wortlauts auf freiwillig herausgegebene Daten oder zuvor nach § 98a Abs. 2 StPO erhobene Daten beschränkt ist. Wenn aber die Strafverfolgungsbehörden mit dem vorgeschlagenen S. 2 des § 98a Abs. 2 StPO selbst zur Erhebung öffentlich zugänglicher Daten ermächtigt wären, könnte auch die maschinelle Auswertung von derartigen Daten auf § 98a StPO gestützt werden.

Durch eine Erfassung der maschinellen Datenabgleiche der hier gegenständlichen Auswertungsmethoden in § 98a StPO könnte außerdem gewährleistet werden, dass die mit den Auswertungsmethoden verbundenen Grundrechtseingriffe in einem angemessenen Verhältnis zu den mit ihnen verfolgten Zwecken stehen würden. Denn anders als bei den Ermittlungsgeneralklauseln setzt § 98a Abs. 1 StPO das Vorliegen zureichender tatsächli-

1779 Löwe-Rosenberg/*Menges,* § 98a Rn. 14; vgl. BVerfGE 115, 320ff.

1780 Löwe-Rosenberg/*Menges,* § 98a Rn. 12ff.

1781 § 98a StPO genügt grundsätzlich den verfassungsrechtlichen Bestimmtheitsanforderungen, Löwe-Rosenberg/*Menges,* § 98a Rn. 12ff.; Siehe zur Problematik der Bestimmtheit des § 98a SK-StPO/*Wohlers/Greco,* § 98a Rn. 6 m.w.N., die allerdings auch zu dem Ergebnis kommen, dass § 98a StPO hinreichend bestimmt ist.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

cher Anhaltspunkte für das Vorliegen einer Straftat von erheblicher Bedeutung aus dem Katalog der Nr. 1 – 6 voraus.[1782] Insoweit wäre die Zulässigkeit der Grundrechtseingriffe, die mit den hier gegenständlichen Auswertungsmethoden einhergehen, entsprechend begrenzt.

Weiterhin wäre durch die explizite Erfassung der Erhebung öffentlicher verfügbarer Daten zum Zweck von maschinellen Datenabgleichen das besonders im Rahmen des RiS zu beachtende Bestimmtheitsgebot gewahrt.[1783] So wäre für den Bürger einerseits klar ersichtlich, dass zu bestimmten Zwecken öffentlich verfügbare Daten maschinell abgeglichen werden dürfen und andererseits wäre hieraus im Umkehrschluss erkennbar, dass der Handabgleich von öffentlich verfügbaren Daten auf Grund der hierbei nicht gesteigerten Grundrechtsintensität nur den Anforderungen der §§ 161, 163 StPO unterliegen würde.

Außerdem würde der gesteigerten Grundrechtsintensität durch den in § 98b StPO enthaltenen Richtervorbehalt Rechnung getragen.

Bei einer Umsetzung der vorgeschlagenen Änderung müsste allerdings das Zitiergebot beachtet werden, da hierdurch neue Grundrechtsbeschränkungen möglich wären.[1784]

In der Kommentarliteratur wird angenommen, die Rasterfahndung sei bei der auch maschinellen Auswertung von öffentlich verfügbaren Daten nicht anwendbar, da hierin auf Grund der öffentlichen Verfügbarkeit entweder kein oder nur ein geringfügiger Grundrechtseingriff vorliege, der auch auf die §§ 161, 163 StPO gestützt werden könne.[1785] Dem sind die bereits dargestellten Ausführungen zur Grundrechtsintensität entgegenzuhalten.[1786] Insbesondere ist anzumerken, dass bereits in der zielgerichteten Erhebung von öffentlich verfügbaren Daten ein Eingriff in das RiS vor-

1782 Siehe hierzu bereits ausführlich unter Kap. 5, D.II.1.a)(1).

1783 Siehe zu den Bestimmtheitsanforderungen bereits ausführlich unter Kap. 5, C.IV.

1784 Vgl. BVerfGE 113, 348 (366), wonach das Zitiergebot auch bei Änderungen von bereits bestehenden Ermächtigungsgrundlagen zu beachten ist, die zu neuen Grundrechtsbeschränkungen führen.

1785 KK-StPO/*Greven,* § 98a Rn. 33; SK-StPO/*Wohlers/Greco,* § 98a Rn. 4; KMR-StPO/*Jäger,* § 98a Rn. 7, der allerdings unter Verweis auf *Rückert,* ZStW 129 (2017), 302 (332f.) angibt, dass möglicherweise ab einer automatisierten Erhebung und Auswertung von öffentlich zugänglichen Informationen eine mit §§ 111, 163d StPO vergleichbare Eingriffsintensität bestehen würde.

1786 Siehe hierzu ausführlich bereits unter Kap. 5, D.II.3.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

liegt[1787], der bei den hier gegenständlichen Auswertungsmethoden teilweise auch einen gesteigerten Grundrechtseingriff darstellt.[1788]

Insoweit bietet die hier vorgeschlagenen Lösung einen hinreichenden Ausgleich zwischen dem Strafverfolgungsinteresse, dass weiterhin bei allen Straftaten grundsätzlich allgemein zugängliche Informationen im Internet – auch unter Verwendung von Suchmaschinen – genutzt werden können, der maschinelle Datenabgleich von allgemein zugänglichen Informationen aus dem Internet aber nur unter den zusätzlichen Voraussetzungen der §§ 98a, 98b StPO zulässig ist.

1787 Vgl. BVerfGE 120, 274 (345).
1788 Siehe hierzu ausführlich bereits unter Kap. 5, D.II.3.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Kapitel 6 – Exkurs – Datenschutzrechtliche Einordnung (privater) Auswertungen von Blockchain-Systemen

Blockchains sind mittlerweile auch Gegenstand der juristischen Diskussionen im Rahmen des europäischen Datenschutzrechts der DSGVO. Hierbei stellen sich etwa Fragen, die teilweise Ähnlichkeit zu den bereits diskutierten Fragen der strafprozessualen Zulässigkeit haben.

Diese Fragen sollen nachfolgend kurz dargestellt werden, um zu prüfen, ob und inwieweit sie etwa zur Unterstützung der vorstehenden Ergebnisse der strafprozessualen Zulässigkeit von Blockchain-Auswertungen herangezogen werden können.

So ist etwa auch für die Eröffnung des sachlichen Anwendungsbereichs der DSGVO zunächst erforderlich, dass personenbezogene Daten vorliegen[1789] (hierzu unter A.). Darüber hinaus muss – soweit der Anwendungsbereich der DSGVO eröffnet ist – ein Erlaubnistatbestand für jegliche Datenverarbeitungen im Zusammenhang mit Blockchains einschlägig und erfüllt sein[1790] (siehe hierzu unter B.).

A. Anwendungsbereich der DSGVO

Für die Eröffnung des Anwendungsbereichs der DSGVO ist in sachlicher Hinsicht nach Art. 2 Abs. 1 DSGVO erforderlich, dass eine „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten“[1791] oder

1789 Vgl. Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 DSGVO; *Bechtolf Vogt,* ZD 2018, 66 (68); *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 72.

1790 Vgl. *Hofert,* ZD 2017, 161 (165), der allerdings noch auf die zu diesem Zeitpunkt geltenden Erlaubnistatbestände des BDSG abstellt. Siehe zum Erfordernis von Erlaubnistatbeständen allgemein Simitis-Hornung-Spiecker/*Albrecht,* Einführung zu Art. 6, Rn. 1. Über diese Fragen hinaus werden etwa auch die Fragen nach der datenschutzrechtlichen Verantwortlichkeit bei Blockchains und nach der hinreichenden Umsetzbarkeit von Betroffenenrechte in der Blockchain diskutiert. Siehe hierzu etwa *Janicki/Saive,* ZD 2019, 251 (252f.); ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 171ff; *Bechtolf/Vogt,* ZD 2018, 66 (69f.). Da diese Fragen allerdings keine unmittelbare Relevanz für die hier gegenständliche Untersuchung haben, werden sie hier nicht dargestellt.

1791 So der Wortlaut des Art. 2 Abs. 1 Hs. 1 DSGVO.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

eine „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“[1792] vorliegt.[1793] Darüber hinaus darf keiner der in Art. 2 Abs. 2 DSGVO aufgeführten Ausnahmetatbestände vorliegen.

I. Verarbeitung personenbezogener Daten

Sowohl der Begriff der „Verarbeitung“ als auch der Begriff der „personenbezogenen Daten“ werden in Art. 4 Nr. 1, Nr. 2 DSGVO legal definiert.

1. Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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 natürlichen Person sind, identifiziert werden kann“[1794].

Grundsätzlich ist insoweit erforderlich, dass Daten verarbeitet werden, die sich mindestens auf eine identifizierbare Person beziehen. Daten, die

1792 So der Wortlaut des Art. 2 Abs. 1 Hs. 2 DSGVO.

1793 Die Eröffnung des räumlichen Anwendungsbereichs nach Art. 3 DSGVO ist für die hier gegenständliche Untersuchung nicht relevant, da sie lediglich voraussetzt, dass die für die Datenverarbeitung verantwortliche Stelle oder der Auftragsverarbeiter eine Niederlassung innerhalb der EU hat, vgl. BeckOK-DSR/*Hanloser,* DSGVO Art. 3 Rn. 2. Dies kann zwar für die Frage nach dem anwendbaren Datenschutzrecht beim Fortschreiben der jeweiligen Blockchain relevant werden (siehe zur technischen Funktionsweise des Fortschreibens von Blockchains oben unter Kap. 2, A.III.), bei dem hier gegenständlichen Einsatz der Auswertungsmethoden wird dagegen davon ausgegangen, dass die Datenverarbeitung von einer verantwortlichen Stelle innerhalb der EU vorgenommen wird, sodass jedenfalls der territoriale Anwendungsbereich der DSGVO eröffnet ist.

1794 Art. 4 Nr. 1 DSGVO.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

keinerlei Personenbezug aufweisen, sind dementsprechend vom Anwendungsbereich der DSGVO ausgenommen.[1795]

Bisher ist nicht eindeutig geklärt, aus welcher Perspektive die Identifizierbarkeit von natürlichen Personen zu beurteilen ist.[1796] Dies ist auch für die Verarbeitung von Daten in Blockchains besonders relevant. Denn auf Grund der dezentralen Verwaltungsstruktur von Blockchains[1797] verfügt keine zentrale Instanz über die Möglichkeit alle verwendeten *public keys* bzw. *Bitcoin-Adressen* einer natürlichen Person zuzuordnen. Im Umkehrschluss bedeutet dies jedoch nicht, dass die natürlichen Personen nicht identifizierbar sind. Denn etwa der zur Identifizierung verpflichtete[1798] *Exchange-Anbieter* kann die verwendete *Bitcoin-Adresse* eines Kunden mit dessen Kundendaten in Verbindung bringen. Andererseits ist es darüber hinaus insbesondere möglich, bestimmte *Bitcoin-Adressen* einfach zu googlen und hieraus entweder die Identität der natürlichen Person oder weitere Anhaltspunkte hierfür zu erhalten.[1799]

Insoweit ist für die Beurteilung, ob personenbezogene Daten vorliegen oder nicht, insbesondere die Perspektive und die Erkenntnisquellen desjenigen, der die Daten verarbeitet, relevant.[1800]

Umstritten war bereits im Rahmen des BDSG und der RL 95/46/EG (nachfolgend „DS-RL") die Grenze der Bestimmbarkeit bei personenbezo-

1795 Sydow-DSGVO/*Ziebarth,* Art. 4 Rn. 24 m.w.N; BeckOK-DSR/*Schild,* DS-GVO Art. 4 Rn. 15.

1796 Siehe hierzu ausführlich etwa *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 85ff.

1797 Siehe hierzu bereits ausführlich oben unter Kap. 2, B.III. m.w.N.

1798 Die Identifizierungspflicht ergibt sich aus § 1 Abs. 11 Nr. 10 KWG i.V.m. § 2 Abs. 1 Nr. 2, §§ 10ff. GwG.

1799 Gibt man etwa die *Bitcoin-Adresse* „165dtfwNvyMUbLGdqf87w8DfZX7i542Fyr" bei Google ein, führt das erste Suchergebnis zu einer Analyseseite, auf der man sämtliche Ein- und Ausgänge dieser *Bitcoin-Adresse* nachvollziehen kann (https://www.blockchain.com/btc/address/165dtfwNvyMUbLGdqf87w8DfZX7i542Fyr letzter Abruf: 20. Dezember 2021). Als zweites Suchergebnis gelangt man auf die Spendenseite der Tageszeitung „taz" (https://taz.de/1-Zahlen-mit-Bitcoins/!142454/ letzter Abruf: 20. Dezember 2021), auf der erkennbar ist, dass diese *Bitcoin-Adresse* als Spendenkonto der taz verwendet wird.

1800 Vgl. *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 73. Darüber hinaus ist auch maßgeblich relevant, um welche Daten es sich handelt, da der Nutzer einer Blockchain ja gerade durch die Art und Weise seiner Nutzung Einfluss auf seine Identifizierung nehmen kann.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

genen Daten.[1801] Dieser Streit hat sich auch mit Inkrafttreten der DSGVO nicht geklärt.[1802]

Bei Daten in Blockchain-Systemen geht mittlerweile die überwiegende Auffassung davon aus, dass personenbezogenen Daten wohl häufig vorliegen.[1803] Dies kann allerdings von einer Einzelfallbetrachtung hinsichtlich der verarbeitenden Stelle und der verarbeiteten Informationen abhängig sein.[1804]

Insoweit besteht eine Parallelität zwischen der Reichweite des Personenbezugs im Rahmen der DSGVO und des RiS.[1805]

Zu beachten ist jedoch ein wesentlicher Unterschied zwischen der Einordnung im Rahmen des RiS und im Rahmen der DSGVO: im Rahmen des RiS wurde die Einordnung maßgeblich damit begründet, dass die Strafverfolgungsbehörden gegenüber den zur Identifizierung verpflichteten Stellen nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG Auskunft über die Identitätsdaten von bestimmten *Bitcoin-Adressen* verlangen konnten.[1806] Diese Befugnisse stehen privaten Stellen grundsätzlich nicht zu. Allerdings bestehen auch für private Stellen grundsätzlich Möglichkeiten, einen Personenbezug herzustellen.[1807]

Insoweit liegen bei Blockchain-Daten auch im Rahmen der DSGVO in der Regel personenbezogene Daten vor.

1801 Siehe hierzu ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 75ff. Dieser Meinungsstreit wurde bereits im Rahmen des RiS dargestellt, siehe hierzu ausführlich unter Kap. 4, B.II.1.b)(2) m.w.N.

1802 Vgl. *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 85.

1803 *Bechtolf/Vogt*, ZD 2018, 66 (69); *Böhme/Pesch,* DuD 2017, 473 (481); *Finck*, Blockchain and the GDPR, S. 14ff; *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 121ff; BeckOK-DSR/*Schild,* DSGVO Art. 4 Rn. 20a.

1804 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 122f., der nachfolgend Fallgruppen bildet und diese hinsichtlich eines möglichen Personenbezugs einordnet.

1805 Ein Grund hierfür dürfte allerdings maßgeblich auch darin liegen, dass zur Frage, ob im Rahmen des RiS personenbezogene Daten vorliegen hinsichtlich der Identifizierbarkeit insbesondere auch auf die Maßstäbe des Datenschutzrechts der DSGVO und des früheren BDSG abgestellt wird, vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.1.b).

1806 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.1.c).

1807 Zu diesen Möglichkeiten insbesondere *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 138 m.w.N.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dieses Ergebnis unterstreicht dementsprechend das bereits im Rahmen des RiS erörterte Ergebnis, dass bei den hier gegenständlichen Auswertungsmethoden grundsätzlich personenbezogene Daten verarbeitet werden.

2. Verarbeitung

Außerdem müssen für den Anwendungsbereich der DSGVO diese personenbezogenen Daten auch verarbeitet werden.[1808] Art. 4 Nr. 2 DSGVO definiert den Begriff der Verarbeitung als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“[1809]. Dementsprechend liegt grundsätzlich bei jedem Vorgang im Zusammenhang mit personenbezogenen Daten ein datenschutzrechtlich relevanter Verarbeitungsvorgang vor.[1810]

Insoweit liegt bereits durch das Herunterladen der jeweiligen Blockchain und durch die Teilnahme am *Peer-to-Peer*-Netzwerk der jeweiligen Blockchain ein datenschutzrechtlich relevanter Verarbeitungsvorgang vor, für den insbesondere ein Erlaubnistatbestand einschlägig sein muss.

Hieraus ergibt sich insoweit ein Unterschied zu der im Rahmen des RiS definierten Eingriffs-Grenze: Nach der Rechtsprechung des BVerfG ist diese bei öffentlich verfügbaren Daten erst erreicht, wenn allgemein zugängliche Informationen gezielt zusammengetragen, gespeichert oder unter Hinzuziehung weitere Daten ausgewertet werden und sich hieraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[1811] Ein derart rechtfertigungsbedürftiger Eingriff in das RiS liegt daher bei den

1808 Vgl. Art. 2 Abs. 1 DSGVO.
1809 So der Wortlaut des Art. 4 Nr. 2 DSGVO.
1810 BeckOK-DSR/*Schild*, Art. 4 Rn. 29; Simitis-Hornung-Spiecker/*Roßnagel*, DSGVO Art. 4 Nr. 2 Rn. 11; Ehmann-Selmayr/*Klabunde*, DSGVO Art. 4 Rn. 23.
1811 BVerfGE 120, 274 (345); siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

unmittelbaren Blockchain-Daten erst vor, wenn über ihr bloßes Herunterladen hinaus weitergehende Rückschlüsse gezogen werden.[1812]

Insoweit besteht ein Unterschied zwischen dem verfassungsrechtlichen Datenschutz und dem Datenschutz der DSGVO: während beim Datenschutz der DSGVO für jeden einzelnen Verarbeitungsvorgang personenbezogener Daten ein Erlaubnistatbestand erfüllt sein muss, ist eine verfassungsrechtliche Rechtfertigung im Rahmen des RiS nur erforderlich, wenn öffentlich verfügbare Informationen gezielt zusammengetragen und gespeichert werden.

Ein Grund für diesen Unterschied könnte darin liegen, dass die verfassungsrechtliche Rechtfertigung von Grundrechtseingriffen höhere Anforderungen voraussetzt als das Vorliegen eines Erlaubnistatbestandes der DSGVO. So ist etwa für eine verfassungsrechtliche Rechtfertigung von Eingriffen in das RiS eine gesetzliche Grundlage erforderlich, die das Zitiergebot beachtet, hinreichend bestimmt die Möglichkeiten und Grenzen des Eingriffs festlegt und ein angemessenes Verhältnis zwischen Zweck und Mittel des Eingriffs aufweist.[1813] Dagegen ist für die Rechtmäßigkeit von Datenverarbeitungen nach der DSGVO neben der Beachtung der Datenschutzgrundsätze des Art. 5 maßgeblich erforderlich, dass ein Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO einschlägig ist. Unter diese Erlaubnistatbestände fallen etwa auch das Vorliegen einer Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO), die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e) oder die Wahrnehmung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DSGVO). Für die Datenverarbeitung durch öffentliche Stellen hat der Gesetzgeber in Ausübung seiner Befugnis nach Art. 6 Abs. 3 lit. b) DSGVO eine allgemeine „Auffangnorm zur Rechtfertigung der Datenverarbeitung im öffentlichen Raum"[1814] geschaffen, die umfassend für alle Verarbeitungen innerhalb des Anwendungsbereichs des BDSG gilt.

Insoweit ließe sich annehmen, dass die Anforderungen für die Rechtfertigung von Eingriffen in das RiS höher sind als für die Rechtfertigung von Datenverarbeitungen nach der DSGVO, sodass die bereits benannten unterschiedlichen Grenzen hierin ihren Grund finden.

1812 Sieh zur Eingriffsgrenze bei den hier gegenständlichen Auswertungsmethoden insgesamt Kap. 4, B.II.2.c).

1813 Siehe zu den verfassungsrechtlichen Anforderungen von Eingriffen in das RiS im Einzelnen oben unter Kap. 5, C.

1814 BeckOK-DSR/*Wolff*, BDSG § 3 Rn. 1.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Grundsätzlich bleibt jedenfalls festzuhalten, dass bereits mit dem Herunterladen der Blockchain-Daten, ebenso wie mit allen weiteren Vorgängen der hier gegenständlichen Auswertungsmethoden eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO vorliegt.

II. Kein Ausnahmetatbestand des Art. 2 Abs. 2 DSGVO

Ausgenommen vom Anwendungsbereich der DSGVO sind jedoch Verarbeitungen personenbezogener Daten, die einen der vier genannten Ausnahmetatbestände erfüllen. Dies sind Verarbeitungen:

- „im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts [fallen],
- Durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
- Durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
- Durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit."[1815]

Insoweit sind vom Anwendungsbereich der DSGVO insbesondere Datenverarbeitungen im Rahmen der gemeinsamen Sicherheits- und Außenpolitik, sowie die Datenverarbeitung im Zusammenhang mit Straftaten ausgenommen.[1816]

1815 So der Wortlaut des Art. 2 Abs. 2 lit. a) – d) DSGVO.

1816 Darüber hinaus ist die Reichweite des Ausnahmetatbestandes Art. 2 Abs. 2 lit. a) DSGVO schwierig zu bestimmen. Wegen der weitreichenden Zuständigkeiten und Rechtssetzungskompetenzen der EU ist sowohl im privaten Bereich als auch bei Datenverarbeitungen durch öffentliche Stellen davon auszugehen, dass der Ausnahmetatbestand keine praktischen Auswirkungen hat, vgl. BeckOK-DSR/*Bäcker,* DSGVO Art. 2 Rn. 7ff. Ferner betrifft Art. 2 Abs. 2 lit. c) die sehr restriktiv auszulegende sog. Haushaltsausnahme, die Datenverarbeitungen vom Anwendungsbereich der DSGVO ausnimmt, wenn diese *ausschließlich* zu privaten oder familiären Zwecken erfolgt, vgl. BeckOK-DSR/*Bäcker,* DSGVO Art. 2 Rn. 12ff. Siehe zur umfassenden Reichweite des Ausnahmetatbestandes Art. 2 Abs. 2 lit. d) DSGVO bezüglich aller Datenverarbeitungen im Zusammenhang mit Straftaten, Specht/Mantz-HdB DSR/*Rogenkamp,* § 21 Rn. 5.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Für die hier gegenständlichen Auswertungsmethoden könnte insbesondere der Ausnahmetatbestand des Art. 2 Abs. 2 lit. d) DSGVO relevant sein, der Datenverarbeitungen von zuständigen Stellen im Zusammenhang mit Straftaten vom Anwendungsbereich der DSGVO ausnimmt.[1817] Dieser Ausnahmetatbestand verläuft insoweit parallel zum Anwendungsbereich der JI-RL.[1818] Denn neben der DSGVO hat die EU außerdem die JI-RL erlassen, die für die „Verarbeitung personenbezogener Daten durch die zuständigen Behörden"[1819] zum Zweck „der Verhütung, Ermittlung, Aufdeckung, oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit"[1820] gilt.[1821]

Der bereits diskutierte Einsatz der Auswertungsmethoden durch die Strafverfolgungsbehörden zum Zweck der Strafverfolgung[1822] kann insoweit nicht in den Anwendungsbereich der DSGVO fallen.

Fraglich ist, ob dies auch gelten kann, wenn Privatpersonen die Auswertungsmethoden einsetzen. Maßgeblich dürfte insoweit sein, dass der Ausnahmetatbestand des Art. 2 Abs. 2 lit. d) DSGVO nur einschlägig ist, wenn die „zuständigen Behörden"[1823] die Datenverarbeitung vornehmen.[1824] Zwar kann dies einerseits bedeuten, dass der Ausnahmetatbestand nicht einschlägig ist, wenn Behörden entgegen den Zuständigkeitsvorschriften agieren und insoweit die DSGVO anwendbar ist.[1825] Andererseits bedeutet dies aber auch, dass der Ausnahmetatbestand jedenfalls nicht bei der Datenverarbeitung durch Privatpersonen einschlägig ist.

Insoweit ist der sachliche Anwendungsbereich der DSGVO für den Einsatz der hier gegenständlichen Auswertungsmethoden durch Privatpersonen eröffnet.

1817 Kühling-Buchner/*Kühling/Raab,* DSGVO Art. 2 Rn. 29.
1818 Kühling-Buchner/*Kühling/Raab,* DSGVO Art. 2 Rn. 29.
1819 So der Wortlaut aus Art. 2 Abs. 1 JI-RL.
1820 So der Wortlaut aus Art. 1 Abs. 1 JI-RL.
1821 Simitis-Hornung-Spiecker/*Roßnagel,* DSGVO Art. 2 Rn. 38. Die Vorgaben der JI-RL wurden mittlerweile durch den deutschen Gesetzgeber in Teil 3 des BDSG umgesetzt, vgl. Simitis-Hornung-Spiecker/*Roßnagel,* DSGVO Art. 2 Rn. 42.
1822 Siehe hierzu ausführlich oben unter Kap. 4, 5.
1823 So der Wortlaut des Art. 2 Abs. 2 lit. d) DSGVO.
1824 Sydow-DSGVO/*Enöckl,* Art. 2 Rn. 15.
1825 Sydow-DSGVO/*Enöckl,* Art. 2 Rn. 15.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

III. Exkurs – Private Ermittlungen im Zusammenhang mit Straftaten und Kooperationen zwischen Strafverfolgungsbehörden und Privaten

Grundsätzlich stellen sich in diesem Zusammenhang aber auch zwei weitere Fragen: denn einerseits müssen private Ermittlungen auch grundsätzlich (strafprozess-)rechtlich zulässig sein. Andererseits kommt in der Praxis insbesondere in Betracht, dass derartige Ermittlungen von den Strafverfolgungsbehörden an Private ausgelagert werden. Daher stellt sich die weitere Frage, inwieweit eine derartige Auslagerung zulässig ist.

Weitgehende Einigkeit besteht zunächst dahingehend, dass auch Private befugt sind, Ermittlungen vorzunehmen und diesen Ermittlungen insbesondere kein staatliches Ermittlungsmonopol entgegensteht.[1826] Dies zeige sich bereits an der Zulässigkeit von Privat- und Nebenklage.[1827] Unterschiedlich werden allerdings die Grenzen privater Ermittlungen bewertet. So nimmt etwa *Bockemühl* an, dass verdeckte, technikgestützte Ermittlungen durch Private nicht zulässig seien, da die Vorschriften der §§ 100a, 100c, 100f StPO eine Sperrwirkung entfalten würden.[1828] Dem gegenüber nimmt die wohl überwiegende Auffassung in der Literatur an, dass die Grenze der Zulässigkeit privater Ermittlungen die allgemeinen Gesetze und insbesondere die Strafvorschriften darstellen.[1829] Dies könne im Einzelfall zwar zum gleichen Ergebnis führen, eine allgemeine Sperrwirkung der Befugnisse der Strafverfolgungsbehörden aus der StPO bestehe jedoch nicht.[1830]

1826 Löwe-Rosenberg/*Erb,* § 160, Rn. 9f.; MüKo-StPO/*Kölbel,* § 160 Rn. 25; Gercke/Julius/Temming/Zöller/*Zöller,* § 160, Rn. 8; *Hellmann,* Strafprozessrecht, Rn. 527ff.; SK-StPO/*Wohlers/Deiters,* § 160 Rn. 2; jeweils m.w.N. A.A. *Brunhöber* GA 2010, 571ff., die davon ausgeht, dass wegen des staatlichen Ermittlungsmonopols, die Zulässigkeit privater Ermittlungen positiv begründet werden müsse. Dies sei etwa bei privaten Ermittlungen durch den Beschuldigten und seine Vertreter der Fall, da der Beschuldigte nicht Objekt des Strafverfahrens werden dürfe. Dies gelte dem entgegen jedoch nicht für Verletzten einer Straftat. Siehe zur Zulässigkeit und Reichweite privater Ermittlungen ausführlich *Bockemühl,* Private Ermittlungen; *Stoffer,* Wie viel Privatisierung „verträgt" das strafprozessuale Ermittlungsverfahren.

1827 Löwe-Rosenberg/*Gössel,* Einleitung L , Rn. 183 m.w.N.

1828 *Bockemühl,* Private Ermittlungen, S. 86.

1829 *Hellmann,* Strafprozessrecht, Rn. 529; Löwe-Rosenberg/*Erb,* § 160 Rn. 10; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8.

1830 Zu beachten ist jedoch, dass den privaten Ermittlern die strafprozessualen Zwangsbefugnisse der StPO nicht zustehen, vgl. hierzu *Hellmann,* Strafprozessrecht, Rn. 529; Löwe-Rosenberg/*Erb,* § 160 Rn. 10; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Ähnlich ist auch die Rechtsprechung des BGH zur Beweisverwertung von privaten Zeugenaussagen zu verstehen.[1831] Der BGH stellte etwa fest, dass es dem Verteidiger nicht verwehrt sei, „eigene Ermittlungen zu führen, inbes. Zeugen oder Mitbesch. vor und außerhalb der Hauptverhandlung zu befragen"[1832]. Hieraus leitet etwa *Jahn* ab, dass private Ermittlungen auch parallel zu laufenden staatlichen Strafverfahren grundsätzlich zulässig seien.[1833]

Festzuhalten bleibt, dass Ermittlungen durch Private grundsätzlich zulässig sind und die Grenze der Zulässigkeit in den allgemeinen Gesetzen – insbesondere den Strafvorschriften – liegt. Dementsprechend können auch die hier gegenständlichen Auswertungsmethoden grundsätzlich zu privaten Ermittlungen eingesetzt werden. Darüber hinaus können Beweise, die rechtmäßig von Privaten ermittelt wurden, grundsätzlich auch verwendet und verwertet werden.[1834]

Fraglich ist allerdings, ob und inwieweit eine Kooperation der Strafverfolgungsbehörden mit privaten Ermittlern zulässig ist. Hier besteht ebenfalls weitgehende Einigkeit darüber, dass Kooperationen der Strafverfolgungsbehörden mit Privaten grundsätzlich zulässig sind.[1835] So stellt etwa das BVerfG fest, dass auf Grund des Legalitätsprinzips hohe Anforderungen an die Unparteilichkeit der Personen zu stellen sind, derer sich die Strafverfolgungsbehörden bedienen, grundsätzlich könnten die Strafverfolgungsbehörden aber private Personen etwa als Sachverständige einbeziehen.[1836] Die Grenze dieser zulässigen Kooperation liegt allerdings darin, dass die Vorschriften des Prozessrechts hierdurch nicht umgangen werden dürfen

1831 Vgl. BGH StV 2003, 602f.
1832 BGH StV 2003, 602.
1833 *Jahn,* StV 2009, 41 (43).
1834 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 28; Vgl. *Hellmann,* Strafprozessrecht, Rn. 530. Umstritten ist allerdings, „inwieweit unzulässig erlangte Erkenntnisse ein Verwertungsverbot auslösen" können. Siehe hierzu ausführlich m.w.N. Löwe-Rosenberg/*Gössel,* Einleitung L., Rn. 183 ff.; vgl. *Hellmann,* Strafprozessrecht, Rn. 530, der feststellt, dass rechtswidrig erlangte Beweismittel nicht generell zu einem Verwertungsverbot führen, sondern „im Einzelfall unter Berücksichtigung aller maßgeblichen Umstände eine Abwägung des öffentlichen Interesses an einer möglichst vollständigen Wahrheitsermittlung und der schutzwürdigen Interessen des Betroffenen" vorzunehmen ist.
1835 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 27; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8; *Brunhöber,* GA 2010, 571 (576).
1836 BVerfG BeckRS 2007, 26565.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

und die Staatsanwaltschaft die faktische Ermittlungsleitung nicht aus der Hand geben dürfen.[1837]

Insoweit dürfte bei einer Kooperation der Strafverfolgungsbehörden mit privaten Ermittlern, die die hier gegenständlichen Auswertungsmethoden einsetzen, nicht dazu führen, dass prozessrechtliche Vorschriften umgangen werden oder die faktische Leitung der Ermittlungshandlungen umgangen werden. Dementsprechend dürfen im Fall einer Kooperation die bereits dargestellten Grenzen des § 161 StPO[1838] für die hier gegenständlichen Auswertungsmethoden nicht umgangen werden.

IV. Zwischenergebnis

Der sachliche Anwendungsbereich der DSGVO setzt die Verarbeitung personenbezogener Daten durch eine private Stelle voraus. Da auch für private Stellen Möglichkeiten bestehen, die in der Blockchain enthaltenen Informationen einer Person zuzuordnen liegen hier personenbezogene Daten vor. Darüber hinaus liegt eine datenschutzrechtlich relevante Verarbeitung durch die bloße Teilnahme am *Peer-to-Peer*-Netzwerk der Blockchain und im Herunterladen der Blockchain-Daten vor. Darüber hinaus ist bei der hier betrachteten Anwendung der Auswertungsmethoden keiner der in Art. 2 Abs. 2 DSGVO enthaltenen Ausnahmetatbestände einschlägig. Schließlich sind auch private Ermittlungen und Kooperationen der Strafverfolgungsbehörden mit privaten Ermittlern grundsätzlich (strafprozess-)rechtlich zulässig, soweit nicht die Grenzen der allgemeinen Gesetze – insbesondere der Strafvorschriften – überschritten werden, die Vorschriften des Prozessrechtes hierdurch nicht umgangen werden und die faktische Ermittlungsleitung der Staatsanwaltschaft nicht abgegeben wird.

B. Rechtmäßigkeit der Datenverarbeitung

Wie bereits erwähnt, ist eine Datenverarbeitung nach der DSGVO nur rechtmäßig, wenn einer der insgesamt sechs in Art. 6 Abs. 1 DSGVO ab-

1837 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 27; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8; *Brunhöber,* GA 2010, 571 (576ff.).

1838 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

schließend aufgezählten Erlaubnistatbestände erfüllt ist.[1839] Dies sind die Einwilligung des Betroffenen (Art. 6 Abs. 1 lit. a) DSGVO), die Erfüllung eines Vertrages oder Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 lit. b) DSGVO), die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO), der Schutz lebenswichtiger Interessen ((Art. 6 Abs. 1 lit. d) DSGVO), die Erfüllung öffentlicher Aufgaben ((Art. 6 Abs. 1 lit. e) DSGVO) und die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DSGVO).[1840]

Im Rahmen der Datenverarbeitung bei Blockchains werden bisher insbesondere der Erlaubnistatbestand der Einwilligung des Betroffenen (hierzu unter I.) und die Wahrnehmung berechtigter Interessen (hierzu unter II.) diskutiert.[1841]

I. Art. 6 Abs. 1 lit. a) – Einwilligung des Betroffenen

Nach Art. 6 Abs. 1 lit. a) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die betroffene Person „ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke“[1842] erteilt hat. Dies wird grundsätzlich auch im Zusammenhang mit der Datenverarbeitung bei Blockchains in Betracht gezogen.[1843]

Für eine wirksame Einwilligung ist grundsätzlich erforderlich, dass sie in „informierter Weise“[1844] erfolgt.[1845] Dabei ist es auch möglich, dass eine

1839 Simitis-Hornung-Spiecker/*Roßnagel,* Einführung zu Art. 6 Rn. 1.

1840 Vgl. zur Aufzählung dieser Erlaubnistatbestände insbesondere *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 147.

1841 Darüber hinaus diskutiert *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 155ff. für den Vollzug von Transaktionen, ob der Erlaubnistatbestand der Erfüllung einer vertraglichen Pflicht oder Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 lit. b) DSGVO) bei einer privaten Blockchain einschlägig sein kann. Ausgeschlossen ist dies nach *Peitz* aber beim Betrieb der hier gegenständlichen öffentlichen Blockchains (siehe zur Begrenzung des Untersuchungsgegenstandes oben unter Kap. 2, B.IV.).

1842 So der Wortlaut des Art. 6 Abs. 1 lit. a) DSGVO.

1843 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149; vgl. zum BDSG etwa *Hofert,* ZD 2017, 161 (164); *Böhme/Pesch,* DuD 2017, 473 (479);

1844 So der Wortlaut des Art. 4 Nr. 11 DSGVO.

1845 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149; Auernhammer/*Kramer,* DSGVO Art. 6 Rn. 21.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Einwilligung konkludent erfolgt.[1846] Eine Willigung setzt nach Erwägungsgrund Nr. 42 S. 4 DSGVO voraus, „dass die betroffene Person mindestens weiß, ‚wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen'"[1847].

Insoweit käme grundsätzlich das Vorliegen einer konkludenten Einwilligung in die Datenverarbeitung zum Fortschreiben der Transaktionshistorie[1848] in Betracht. Dies wird aber aus mehreren Gründen abgelehnt[1849]:

So ist für das Vorliegen einer konkludenten Einwilligung erforderlich, dass eine eindeutig bestätigende Handlung vorliegt.[1850] Hierzu genügt es nicht, wenn lediglich eine Transaktionsnachricht an das Blockchain-Netzwerk versendet wird.[1851] Darüber hinaus dürfte es in der Regel an der nach Art. 4 Nr. 11 DSGVO erforderlichen Informiertheit bezüglich der Datenverarbeitung beim Versenden einer Transaktionsnachricht fehlen.[1852] Ferner bestehen grundsätzlich Zweifel am Vorliegen der erforderlichen Freiwilligkeit.[1853] Schließlich ist es auf Grund der technischen Funktionsweise von Blockchains[1854] in der Regel nicht möglich, die Einwilligung später zu widerrufen, da die einmal in die Datenblöcke aufgenommenen Transaktionen faktisch nachträglich nicht mehr verändert werden können.[1855]

Insoweit kann der in Art. 6 Abs. 1 lit. a) DSGVO enthaltene Erlaubnistatbestand der Einwilligung schon nicht für die Datenverarbeitung, die lediglich für das Fortschreiben der Transaktionshistorie erforderlich ist, herangezogen werden. Die hier gegenständlichen Datenverarbeitungen durch die Auswertungsmethoden können dementsprechend keinesfalls einer Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO unterfallen – zumal selbst beim

1846 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 150 m.w.N.

1847 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149.

1848 Sieh zur technischen Funktionsweise bereits ausführlich oben unter Kap. 2, A.III.1.c).

1849 Siehe hierzu ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 150ff.

1850 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151.

1851 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151.

1852 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151f.

1853 Diese setzt nämlich auch voraus, dass die „Einwilligung ohne jeglichen Druck oder Zwang abgegeben […] [und] ohne Nachteile wieder zurückgenommen werden kann", *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 152 mit Verweis auf Erwägungsgrund Nr. 42 S. 5 DSGVO.

1854 Siehe hierzu ausführlich oben unter Kap. 2, A., B.

1855 Siehe zur technischen Funktionsweise oben unter Kap. 2, A.III.2.; *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 154.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Vorliegen einer Einwilligung in die Datenverarbeitung zum Fortschreiben der Blockchain sich diese nicht auf die hier gegenständlichen Auswertungsmethoden beziehen würde.[1856]

II. Art. 6 Abs. 1 lit. f) DSGVO – Wahrnehmung berechtigter Interessen

Ein weiterer Erlaubnistatbestand ist in Art. 6 Abs. 1 lit. f) DSGVO enthalten und berechtigt zur Verarbeitung personenbezogener Daten, wenn dies zur „Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist"[1857], „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen"[1858].

Die berechtigten Interessen des Art. 6 Abs. 1 lit. f) DSGVO sind grundsätzlich weit zu verstehen, so dass sowohl wirtschaftliche als auch ideelle und rechtliche Interessen hiervon erfasst sind.[1859] Dementsprechend sind jedenfalls die grundrechtlich geschützten Interessen des Verantwortlichen erfasst.[1860]

Kern dieses Erlaubnistatbestandes ist eine Abwägung der widerstreitenden Interessen – also der Interessen des für die Datenverarbeitung Verantwortlichen und des von der Datenverarbeitung Betroffenen.[1861] Maßgeblich für diese Interessenabwägung ist insoweit, zu welchem Zweck der Verantwortliche die jeweiligen Daten verarbeitet. So dürfte jedenfalls ein deutlicher Unterschied zwischen dem Fortschreiben der jeweiligen Blockchain-Transaktionen[1862] und den hier gegenständlichen Auswertungsmethoden bestehen.

So spricht etwa bei der Verarbeitung zum Zwecke des Fortschreibens der Blockchain grundsätzlich für ein überwiegendes Interesse des Verantwortli-

1856 Vgl. *Hofert,* ZD 2017, 161 (165).
1857 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 158.
1858 So der Wortlaut des Art. 6 Abs. 1 lit. f) DSGVO.
1859 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Abs. 1 Rn. 98; BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 68; Auernhammer/*Kramer,* DSGVO Art. 6 Rn. 72; Rücker-Kugler/*Dienst,* Rn. 399.
1860 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Abs. 1 Rn. 99; m.w.N; Paal-Pauly/*Frenzel,* DSGVO Art. 6 Rn. 28; vgl. Ehmann-Selmayr/*Heberlein,* DSGVO Art. 6 Rn. 25f.
1861 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 158.
1862 Siehe zur technischen Funktionsweise bereits ausführlich oben unter Kap. 2, A.III.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

chen, dass der Nutzer einer Blockchain in der Regel mit der Datenverarbeitung rechnen muss.[1863]

Fraglich ist, ob dies auch für die hier gegenständlichen Auswertungsmethoden gelten kann. So nimmt etwa *Peitz* an, dass ein Nutzer von Blockchains nicht mit der systematischen Auswertung der Blockchain-Daten rechnen muss und dies nicht erkennbar sei und insoweit eine derartige Verarbeitung nicht nach Art. 6 Abs. 1 lit. f) DSGVO zulässig sei.[1864] Zu beachten ist allerdings, dass einerseits eine Verarbeitung nicht unmittelbar dadurch unzulässig wird, dass sie für den Betroffenen nicht erkennbar ist.[1865] Andererseits muss beachtet werden, dass mit den hier gegenständlichen Auswertungsmethoden zwar auch Profilbildung möglich ist, dies aber im Zusammenhang mit Straftaten vorgenommen werden soll und insoweit wohl kein kommerzieller Werbezweck mit der Datenverarbeitung verfolgt wird.[1866]

Dementsprechend stellt sich zunächst die Frage, zu welchem Zweck die hier gegenständlichen Auswertungsmethoden eingesetzt werden sollen.

Der bisher betrachtete Zweck lag in der Strafverfolgung, nachdem der Verdacht einer Straftat bestand.[1867] Zu beachten ist jedoch, dass von Art. 6 Abs. 1 lit. f) DSGVO in Abgrenzung zu Art. 6 Abs. 1 lit. e) DSGVO nicht die Wahrnehmung öffentlicher Interessen, die keinen Bezug zur einzelnen Person haben, erfasst sind.[1868] Öffentliche Interessen (wie etwa die Terro-

1863 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159; vgl. insoweit insbesondere das Bitcoin zugrundeliegende White-Paper *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6, worin bereits auf die datenschutzrechtliche Relevanz hingewiesen wird; siehe insoweit etwa auch https://bitcoin.org/de/ (letzter Abruf: 20. Dezember 2021), wo etwa die technische Funktionsweise der Bitcoin-Blockchain erklärt wird. Siehe insoweit vergleichbar auch die hier bestimmte Grenze des Grundrechtseingriffs im Rahmen des RiS bei öffentlich verfügbaren Daten oben unter Kap. 4, B.II.2.b)(3).

1864 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159.

1865 So *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159; vgl. insoweit insbesondere Art. 14 Abs. 5 lit. b) DSGVO, nach dem die Informationspflichten gegenüber dem Betroffenen u.a. auch entfallen, wenn hierdurch die Ziele der Verarbeitung unmöglich gemacht werden oder ernsthaft beeinträchtigt werden.

1866 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159f, stellt abweichend maßgeblich auf die systematische Analyse von Blockchain-Daten zu Werbezwecken ab.

1867 Siehe hierzu insbesondere bereits oben unter Kap. 5, A; siehe zum Erfordernis des Anfangsverdachts bereits oben unter Kap. 5, D.I.

1868 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

rismusabwehr oder Volksgesundheit) können den berechtigten Interessen des Verantwortlichen zwar ein „stärkeres Gewicht verleihen oder sich mit den berechtigten Interessen des Verantwortlichen oder Dritten decken“[1869], „[a]usgeschlossen ist jedoch, dass private Stellen eine Verarbeitung mit der Wahrnehmung von Allgemeininteressen […] rechtfertigen“[1870].

Als berechtigtes Interesse ist jedoch die Eigentums- und Beweissicherung zulässig. So kann etwa ein präventiver Zweck zur Sicherung des Eigentums verfolgt werden sowie auch ein repressiver Zweck zur Sicherung von Beweismaterial zur Aufklärung und Verfolgung von Straftaten sowie zur gerichtlichen Geltendmachung.[1871] Insoweit sind auch die „Aufklärung und Verfolgung von Straftaten und die Sicherung von Beweismaterial zur gerichtlichen Durchsetzung zivilrechtlicher Schadensersatzansprüche als berechtigte Interessen grundsätzlich anzuerkennen.“[1872] Explizit nennt Erwägungsgrund Nr. 47 DSGVO etwa „die Verhinderung von Betrug“ als berechtigtes Interesse. Anerkannt ist neben diesem vorrangig präventiven Zweck aber auch, die Verfolgung von Straftaten. So nimmt etwa das OVG Lüneburg an, dass die Videoüberwachung in Fahrzeugen um etwa „‘Vandalismusschäden und/oder Straftaten in den Fahrzeugen unter Beibringung von Beweismitteln zur Anzeige bringen zu können“[1873] ein berechtigtes Interesse darstellt.[1874] So käme bei den hier gegenständlichen Auswertungsmethoden etwa ein berechtigtes Interesse in Betracht, wenn der Betroffene von Ransomware[1875] die Auswertungsmethoden einsetzt, um den Täter zu ermitteln oder Anhaltspunkte zur Täteridentifizierung zu erhalten.

1869 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99; so auch *Art. 29 Datenschutzgruppe*, WP 217, S. 45.

1870 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99.

1871 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 75ff.

1872 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78 m.w.N. Ähnlich auch Sydow-DSGVO/*Reimer,* Art. 6 Rn. 57, der darauf abstellt, dass nach Erwägungsgrund Nr. 50 Abs. 2 S. 3 DSGVO die Übermittlung personenbezogener Daten zur Aufklärung von Straftaten ein berechtigtes Interesse ist, selbst, wenn die Straftat den Übermittler selbst nicht betrifft.

1873 OVG Lüneburg, BeckRS 2017, 123619 Rn. 29.

1874 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78, der unter Verweis auf die zuvor genannte Entscheidung des OVG Lüneburg feststellt, dass auch die Verfolgung und Aufklärung von Straftaten ein berechtigtes darstellt.

1875 Ransomware bezeichnet eine Schadsoftware, mit der in der Regel der Zugang zu Daten oder technischen Geräten erschwert oder gänzlich verhindert wird, vgl. *Grzywotz/Köhler/Rückert,* StV 2016, 753 (756). In der Regel fordern die „Erpresser“ eine Art Lösegeld, um den Zugang wieder herzustellen. Das Lösegeld wird häufig mit Kryptowährungen bezahlt.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Zur Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 lit. f) DSGVO ist darüber hinaus erforderlich, dass die Datenverarbeitungen zu dem verfolgten Zweck erforderlich sind und die Interessen der Betroffenen nicht das berechtigte Interesse des Verantwortlichen überwiegen.[1876]

Erforderlich ist eine Datenverarbeitung, wenn die berechtigten Interessen nicht auf einem anderen, weniger intensiven Weg genauso effektiv verfolgt werden können.[1877] So nimmt etwa der BGH für den Einsatz von Dash-Cams ans, dass „jedenfalls die permanente anlassloses Aufzeichnung des gesamten Geschehens entlang der Fahrstrecke […] zur Wahrnehmung [der| Interessen […] nicht erforderlich"[1878] sei, da ihr Ziel etwa durch andere privacy-by-design Ansätze erreicht werden könne.[1879] Insoweit muss beim Einsatz der hier gegenständlichen Auswertungsmethoden darauf geachtet werden, welche der konkreten Auswertungsmethoden eine möglichst geringe Eingriffsintensität aufweisen.[1880]

Darüber hinaus muss eine Abwägung der widerstreitenden Interessen stattfinden, bei der die Interessen des Betroffenen nicht überwiegen dürfen. Hierbei müssen nicht nur die konkret eingetretenen Folgen, sondern auch die möglichen Risiken, die mit der Datenverarbeitung einhergehen, berücksichtigt werden.[1881] Zur Bewertung der Eingriffsintensität werden dabei folgende Faktoren herangezogen:

– Art und Umfang der verarbeiteten Daten[1882]: so kann es einerseits insbesondere intensitätserhöhend sein, wenn auf Grund des Umfangs der erhobenen Daten die Möglichkeit besteht, dass diese zusammengeführt und verknüpft werden und sich so umfangreiche Informationen ergeben, aus denen ein Profil des Betroffenen erstellt werden kann. Dies führt in der Regel zum Überwiegen der Interessen des Betroffenen.[1883] Andererseits kann auch die Art der verarbeiteten Daten besonders intensitätser-

1876 BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 69.
1877 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 100.
1878 BGH NJW 2018, 2883 (2885 Rn. 19).
1879 BGH NJW 2018, 2883 (2885 Rn. 25).
1880 Vgl. *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (7).
1881 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 101.
1882 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 105.
1883 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 106, der allerdings darauf abstellt, dass nur dann in der Regel ein überwiegendes Interesse des Betroffenen vorliegt, wenn ein Profil des Betroffenen zu kommerziellen Zwecken erstellt wird.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

höhend sein, etwa wenn der „Aussagegehalt über eine Person besonders hoch ist."[1884]

- Anlass und Umstände der Verarbeitung[1885]: so kann sich etwa die verdeckte[1886], die dauerhafte oder anlasslose Datenerhebung intensitätserhöhend auswirken.[1887]
- Mögliche Folgen der Datenverarbeitung: So werden Datenverarbeitungen, durch die negative Folgen für den Betroffenen drohen als besonders risikoreich eingestuft.[1888]
- Kontext der Datenverarbeitung: so erhöht sich die Intensität etwa, wenn der Betroffene nicht mit der Datenverarbeitung rechnen musste. Insoweit sind auch die Vertraulichkeitserwartungen des Betroffenen zu berücksichtigen.[1889] Andersherum ist es intensitätsverringernd zu berücksichtigen, wenn der Betroffene mit der Verarbeitung rechnen musste.[1890] So muss der Betroffene bei öffentlich verfügbaren Daten in „sehr viel stärkerem Maß"[1891] mit der Verarbeitung dieser Daten rechnen.

Auf der anderen Seite hängt die Interessenabwägung natürlich auch von der Gewichtung der Interessen, die der Verantwortliche mit der Datenverarbeitung verfolgt, ab.[1892] Zwar lassen sich der DSGVO keine unmittelbaren Kriterien für die Abwägung entnehmen[1893], aus der Systematik der DSGVO ergibt sich allerdings, dass etwa die Durchsetzung zivilrechtlicher Ansprüche wohl einen privilegierten Zweck darstellt, da die DSGVO Datenverarbeitungen zu diesem Zweck mehrfach privilegiert.[1894]

Die vorstehend dargestellten Kriterien zur Bewertung der Intensität der Datenverarbeitung sind dabei fast vollständig deckungsgleich mit den zur Bewertung der Grundrechtsintensität herangezogenen Kriterien.[1895] So

1884 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 105.
1885 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111.
1886 Bzw. die heimliche Datenerhebung, Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111.
1887 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111; vgl. BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 72.
1888 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 107.
1889 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 109.
1890 BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 72; Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 108.
1891 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 110.
1892 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103.
1893 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103.
1894 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103, 123.
1895 Siehe hierzu ausführlich oben unter Kap. 5, D.II.1., 2.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

wurde auch im grundrechtsrelevanten Bereich die Art und der Umfang der erhobenen Daten für die Bewertung der Intensität berücksichtigt werden.[1896] Darüber hinaus wurden auch im grundrechtsrelevanten Bereich die Umstände der Datenerhebung relevant. So wurde etwa intensitätssteigernd berücksichtigt werden, wenn anlasslos Daten erhoben werden oder wenn hierbei Vertraulichkeitserwartungen verletzt werden.[1897]

Insoweit kann hinsichtlich der Intensität der hier gegenständlichen Auswertungsmethoden auf die bereits erfolgte Einordnung verwiesen werden.[1898]

Zu beachten ist jedoch, dass anders als im Rahmen von § 161 StPO nach Art. 6 Abs. 1 lit. f) DSGVO nicht nur geringfügige Grundrechtseingriffe rechtmäßig sind. Erforderlich ist im Rahmen der Interessenabwägung des Art. 6 Abs. 1 lit. f) DSGVO vielmehr, dass die Intensität der Beeinträchtigung nicht die Interessen der verantwortlichen Stelle überwiegen.[1899] Dementsprechend führt es nicht zwangsläufig zur Unrechtmäßigkeit der Auswertungsmethoden nach Art. 6 Abs. 1 lit. f) DSGVO, wenn bei diesen ein nicht mehr nur geringfügiger Grundrechtseingriff vorliegt.

Ob und in welchen Fallkonstellationen diese Interessenabwägung beim Einsatz der hier gegenständlichen Auswertungsmethoden im Einzelfall zu dem Ergebnis kommen kann, dass eine rechtmäßige Datenverarbeitung vorliegt, muss einer gesonderten, ausführlichen Prüfung vorbehalten bleiben. Dabei dürfte sich etwa die Frage stellen, ob und inwieweit die Schwere der Straftat zu deren Aufklärung die Auswertungsmethoden eingesetzt werden sollen, in die Interessenabwägung einbezogen werden kann und, ob sich ein Unterschied daraus ergibt, dass bereits bei der Erhebung von Blockchain-Daten ein rechtfertigungsbedürftiger Datenverarbeitungsvorgang vorliegt.[1900]

III. Zwischenergebnis

Festzuhalten bleibt, dass im Datenschutzrecht der DSGVO für die hier gegenständlichen Auswertungsmethoden nur der Rechtmäßigkeitstatbestand des Art. 6 Abs. 1 lit. f) DSGVO einschlägig sein kann. Erforderlich ist in die-

1896 Siehe hierzu etwa bereits Kap. 5, D.II.1.e), D.II.2.a).
1897 Siehe hierzu etwa bereits Kap. 5, D.II.1.e), D.II.2.b).
1898 Siehe hierzu ausführlich oben unter Kap. 5, D.II.3.
1899 Paal-Pauly/*Frenzel,* DSGVO Art. 6 Rn. 27.
1900 Siehe hierzu bereits oben unter Kap. 6, A.I.2.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

sem Rahmen, dass der Verantwortliche der Datenverarbeitung ein berechtigtes Interesse mit der Datenverarbeitung verfolgt, die Datenverarbeitung hierzu erforderlich ist und die Interessen der Betroffenen nicht überwiegen. Dabei bleibt insbesondere festzuhalten, dass die Kriterien zur Abwägung der Interessen fast deckungsgleich mit den Kriterien sind, die zur Bewertung der Grundrechtsintensität herangezogen wurden. Unterschiedlich ist jedoch, dass im Rahmen von Art. 6 Abs. 1 lit. f) DSGVO jedoch auch eine nicht nur geringfügige Intensität der Beeinträchtigung rechtmäßig sein kann. Ob dies beim Einsatz der hier gegenständlichen Auswertungsmethoden der Fall sein kann, muss allerdings einer weitergehenden Untersuchung vorbehalten bleiben.

C. Zusammenfassung

Aus dem Vorstehenden ergibt sich, dass der Anwendungsbereich der DSGVO für die hier gegenständlichen Auswertungsmethoden eröffnet ist. Denn grundsätzlich ist bei den in der Blockchain enthaltenen Daten ebenfalls von personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO auszugehen und andererseits liegt bereits durch die bloße Teilnahme am Blockchain-Netzwerk und dem Herunterladen der in der Blockchain enthaltenen Daten grundsätzlich eine nach Art. 4 Nr. 2 DSGVO relevante Datenverarbeitung vor. Insoweit besteht hier ein Unterschied zwischen der Grenze eines verfassungsrechtlich rechtfertigungsbedürftigen Eingriffs in das RiS und eines datenschutzrechtlich erlaubnispflichtigen Datenverarbeitungsvorgangs.

Darüber hinaus ist nach Art. 6 Abs. 1 DSGVO für die Rechtmäßigkeit einer Datenverarbeitung erforderlich, dass einer der abschließenden Rechtmäßigkeitstatbestände erfüllt ist. Für die hier gegenständlichen Auswertungsmethoden kommt nur die Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 lit. f) DSGVO in Betracht. Ein hierzu erforderliches berechtigtes Interesse kann auch in der „Aufklärung und Verfolgung von Straftaten Strafverfolgung und [der] Sicherung von Beweismaterial zur gerichtlichen Durchsetzung zivilrechtlicher Schadensersatzansprüche“[1901] liegen. Allerdings muss die Datenverarbeitung hierzu erforderlich sein und

1901 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78 m.w.N. Ähnlich auch Sydow-DSGVO/*Reimer,* Art. 6 Rn. 57, der darauf abstellt, dass nach Erwägungsgrund Nr. 50 Abs. 2 S. 3 DSGVO die Übermittlung personenbezogener Daten

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

es dürfen keine Interessen der Betroffenen überwiegen. Interessant ist dabei insbesondere, dass die Kriterien, die zur Bewertung der Interessen der Betroffenen herangezogen werden, fast deckungsgleich mit den Kriterien zur Bewertung der Grundrechtsintensität sind. Ein Unterschied besteht allerdings dahingehend, dass Art. 6 Abs. 1 lit. f) DSGVO – anders als § 161 StPO – nicht für die Rechtmäßigkeit der Datenverarbeitung voraussetzt, dass nur eine geringfügige Grundrechtsintensität vorliegt. Die für Art. 6 Abs. 1 lit. f) DSGVO erforderliche Interessenabwägung muss allerdings einer gesonderten Prüfung vorbehalten bleiben.

zur Aufklärung von Straftaten ein berechtigtes Interesse ist, selbst, wenn die Straftat den Übermittler selbst nicht betrifft.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

Kapitel 7 – Schlussbetrachtung

Die vorstehende Untersuchung hat gezeigt, dass die Blockchain-Technologie zwar eine sehr einfach verfügbare Datengrundlage für systematische Auswertungen bietet. Der Einsatz dieser Auswertungsmöglichkeiten ist allerdings trotz der öffentlichen Verfügbarkeit der ausgewerteten Daten nur teilweise zu Strafverfolgungszwecken zulässig. Denn die einschlägige Ermittlungsbefugnis des § 161 Abs. 1 StPO ermächtigt nur zu geringfügigen Grundrechtseingriffen. Die hier untersuchten Auswertungsmethoden überschreiten allerdings teilweise diese Grenze der Geringfügigkeit. Empfehlenswert ist es daher, in § 98a Abs. 2 StPO eine Befugnis zur Erhebung von öffentlich zugänglichen Daten aufzunehmen.[1902]

A. Die Blockchain-Technologie und ihre Auswertbarkeit

Grundsätzlich wird der Blockchain-Technologie ein enormes Entwicklungspotenzial zugeschrieben, da durch ihren Einsatz einerseits fälschungssicher und andererseits ohne eine zentrale Verwaltungsstelle Daten verwaltet werden können.[1903]

In der öffentlichen Wahrnehmung ist die Blockchain-Technologie zwar vor allem im Zusammenhang mit Bitcoin und anderen Kryptowährungen bekannt, sie ist aber gerade nicht auf diesen Anwendungskontext beschränkt.[1904] Sie kann vielmehr als eine Form dezentraler Datenverwaltung verstanden werden.[1905] So kann die Blockchain-Technologie etwa für Smart-Contracts, die öffentliche Verwaltung, das Crowdfunding oder die digitale Zuweisung von Rechten eingesetzt werden.[1906]

Bei Kryptowährungen wird die Blockchain-Technologie zur Kontobuchführung eingesetzt. Vereinfacht kontrollieren dabei alle Teilnehmer des Blockchain-Netzwerkes, ob neue Transaktionen mit der bisherigen Trans-

1902 Siehe hierzu ausführlich oben unter Kap. 5, F.
1903 Siehe zur technischen Funktionsweise der Blockchain-Technologie im Einzelnen oben unter Kap. 2 m.w.N.
1904 Siehe hierzu oben unter Kap. 2, B.I.
1905 Siehe hierzu oben unter Kap. 2, B.III.
1906 Siehe hierzu mit weiteren Nachweisen und Beispielen oben unter Kap. 2, C.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

aktionshistorie übereinstimmen.[1907] Da Bitcoin – wie andere Kryptowährungen auch – als offenes Netzwerk ausgestaltet ist, führt die dezentrale Datenverwaltung dazu, dass alle in der Blockchain enthaltenen Transaktionsdaten öffentlich verfügbare Daten sind.[1908] Dies ist relevant, da Kryptowährungen häufig auch im Zusammenhang mit illegalen Aktivitäten verwendet werden und die in der Blockchain enthaltenen Transaktionsdaten insoweit einen einfach verfügbaren Ansatz für strafrechtliche Ermittlungen bieten. So ist es in der Praxis ohne Umstände möglich, eine *Bitcoin-Adresse* bei Google einzugeben und in der Regel über einen der ersten drei angezeigten Links alle Transaktionen einzusehen, die jemals mit dieser *Bitcoin-Adresse* getätigt wurden, und weitere Informationen zu erhalten.

Die verwendeten *Bitcoin-Adressen* geben grundsätzlich keine Anhaltspunkte über die hinter ihnen stehenden Personen.[1909] Denn einerseits fehlt es auf Grund der Dezentralität eben gerade an einer zentralen Verwaltungsstelle, durch die eine derartige Zuordnung erfolgen könnte. Andererseits ist es bei Bitcoin möglich, sich unzählig viele *Bitcoin-Adressen* zu erstellen.[1910] Die Transaktionsdaten in der Blockchain können aber als Anhaltspunkte für weitere Ermittlungen verwendet werden – etwa um zu ermitteln, ob eine verdächtige *Bitcoin-Adresse* in der Vergangenheit mit einem Diensteanbieter für Kryptowährungen interagiert hat, der zur Identifizierung seiner Kunden verpflichtet ist.

Daher wurden mittlerweile verschiedenste Auswertungsmöglichkeiten entwickelt, mit denen die Transaktionsdaten der Blockchain systematisch ausgewertet werden können. So ist es etwa durch die sog. *Entitäts-Clustering*-Verfahren möglich, mehrere *Bitcoin-Adressen* einer einzelnen sog. *Entität* zuzuordnen.[1911] Darüber hinaus ist es möglich, die Transaktionsdaten der *Bitcoin-Adressen* und *Entitäten* systematisch auszuwerten und zu ermitteln, welches Transaktionsverhalten typisch ist und welches Transaktionsverhalten hiervon abweicht.[1912] Außerdem können auch Transaktionsmuster ermittelt werden, die auf einen bestimmten Hintergrund der Transaktionen hindeuten.[1913] Ferner können auch die Daten über die Weiterleitung von Transaktionsnachrichten im Netzwerk der Blockchain und sog. *Bloom-*

1907 Siehe hierzu im Einzelnen oben unter Kap. 2, A.III.
1908 Siehe hierzu im Einzelnen oben unter Kap. 2, A.IV.
1909 Siehe hierzu oben unter Kap. 2, A.II. m.w.N.
1910 Siehe hierzu oben unter Kap. 2, A.II. m.w.N.
1911 Siehe hierzu oben unter Kap. 3, A.I. m.w.N.
1912 Siehe hierzu oben unter Kap. 3, A.II. m.w.N.
1913 Siehe hierzu oben unter Kap. 3, A.III. m.w.N.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Filter ausgewertet werden, um *Bitcoin-Adressen* einer IP-Adresse zuzuordnen.[1914] Schließlich ist es auch möglich, diese Daten auch mit anderweitig verfügbaren Daten zu verknüpfen, um so weitere Informationen zu erhalten.[1915]

Dabei muss allerdings berücksichtigt werden, dass die hier dargestellten Auswertungsmöglichkeiten nur eine Momentaufnahme sind, denn die technische Funktionsweise von Bitcoin und anderen Kryptowährungen wird fortlaufend angepasst – auch, um derartige Auswertungsmöglichkeiten zu verhindern. So haben sich mittlerweile schon mehrere weitere Kryptowährungen herausgebildet, bei denen eine Auswertung der Transaktionsdaten noch schwieriger ist. Insoweit unterliegt sowohl die technische Funktionsweise von Blockchains und Kryptowährungen als auch die technische Funktionsweise von Ermittlungsmöglichkeiten einem fortlaufenden Wandel. Die herausgearbeiteten rechtlichen Bewertungsmaßstäbe können aber bei technischer Vergleichbarkeit entsprechend angewendet werden.

B. Die Auswertungsmethoden als Eingriff in das Recht auf informationelle Selbstbestimmung

Zunächst lässt sich festhalten, dass beim Einsatz der hier untersuchten Auswertungsmethoden nur ein Eingriff in das Recht auf informationelle Selbstbestimmung (nachfolgend als „RiS" bezeichnet) vorliegt.[1916]

Denn einerseits liegen auch bei den ausgewerteten Daten personenbezogene Daten vor.[1917] Andererseits kann auch bei öffentlich verfügbaren Daten ein Eingriff in das RiS vorliegen.[1918]

Der Personenbezug liegt nach hier vertretener Auffassung vor, wenn die jeweils verarbeitende Stelle rechtlich und tatsächlich dazu in der Lage ist, einen Personenbezug mit einem nicht unverhältnismäßigen Aufwand herzustellen.[1919] Dies ist für die von Auswertungsmethoden betroffenen Daten insoweit der Fall, als dass die in einer Blockchain enthaltenen Transaktionsdaten etwa nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG

1914 Siehe hierzu oben unter Kap. 3, B. m.w.N.
1915 Siehe hierzu oben unter Kap. 3, C. m.w.N.
1916 Siehe hierzu insgesamt unter Kap. 4, B.II. m.w.N.
1917 Siehe hierzu unter Kap. 4, B.II.1. m.w.N.
1918 Siehe hierzu unter Kap. 4, B.II.2. m.w.N.
1919 Siehe hierzu unter Kap. 4, B.II.1.b)(4) m.w.N.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

einer Person zugeordnet werden können.[1920] Dieses Ergebnis wird auch von der datenschutzrechtlichen Einordnung unterstützt, die überwiegend davon ausgeht, dass die in Blockchains enthaltenen Daten personenbezogene Daten sind.[1921] Soweit darüber hinaus (dynamische) IP-Adressen von den Auswertungsmethoden betroffen sind, liegen eindeutig personenbezogene Daten vor.

Der Eingriff in das RiS bei öffentlich verfügbaren Daten liegt nach hier vertretener Auffassung vor, 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 sich durch weitergehende Datenverarbeitungsmaßnahmen ergeben können.[1922] Dies ist bei allen hier untersuchten Auswertungsmethoden der Fall. Eine Besonderheit ergibt sich allerdings für das Herunterladen der jeweiligen Blockchain-Daten. Dies stellt noch keinen Eingriff in das RiS dar, da zwar umfangreiche Daten, die bereits chronologisch geordnet sind, den Strafverfolgungsbehörden verfügbar gemacht werden, dies hat aber lediglich den technischen Hintergrund der Funktionsweise der Blockchain-Technologie und darf insoweit rechtlich nicht anders bewertet werden als die bloße Kenntnisnahme öffentlich verfügbarer Daten.[1923] Anders ist dies jedoch im Rahmen des Datenschutzrechts der DSGVO zu bewerten, da hier nach Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 2 DSGVO bereits in der bloßen Teilnahme an dem *Peer-to-Peer*-Netzwerk der Blockchain und dem Herunterladen der Blockchain-Daten ein datenschutzrechtlich relevanter Verarbeitungsvorgang vorliegt, für den ein Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO erfüllt sein muss.[1924] Zu beachten ist allerdings, dass das Datenschutzrecht der DSGVO nur für den Einsatz der Auswertungsmethoden durch Private gilt.[1925]

Zwar kommt auch ein Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses und des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (nachfolgend als „IT-Grundrecht" bezeichnet) in Betracht.[1926]

1920 Siehe hierzu unter Kap. 4, B.II.1.c) m.w.N.
1921 Siehe hierzu im Einzelnen unter Kap. 6, A.I.1. m.w.N.
1922 Siehe hierzu im Einzelnen unter Kap. 4, B.II.2.b). m.w.N.
1923 Siehe hierzu im Einzelnen unter Kap. 4, B.II.2.c)(1).
1924 Siehe hierzu oben unter Kap. 6, A.I.1.
1925 Siehe zum Anwendungsbereich der DSGVO bereits oben unter Kap. 6, A.I., II.
1926 Siehe hierzu insgesamt oben unter Kap. 4, B.I., III.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Allerdings ist vom Schutzbereich des Telekommunikationsgeheimnisses nur Individualkommunikation erfasst. Nicht von Art. 10 Abs. 1 GG geschützt wird dagegen Massenkommunikation. Problematisch kann diese Abgrenzung zwar bei der Telekommunikation im Internet auf Grund der zu unterscheidenden Kommunikationsebenen sein.[1927] Für die hier gegenständliche Untersuchung wurde die geschützte Individualkommunikation von der nicht geschützten Massenkommunikation dahingehend abgegrenzt, ob auf die jeweilige Kommunikation ohne weitere Autorisierung von außen zugegriffen wurde.[1928] Für die Auswertungsmethoden bedeutet das, dass jedenfalls die in der Blockchain enthaltenen Daten keine geschützte Individualkommunikation sind, sondern nicht geschützte Massenkommunikation darstellen.[1929] Dies gilt auch für die Auswertung anderweitig verfügbarer Daten, soweit nicht von außen unautorisiert auf Telekommunikation zugegriffen wird. Gleiches gilt für die Auswertung der Verbreitung von Transaktionsnachrichten, die sog. Bloom-Filter-Attacks und die Auswertung des Datenverkehrs durch das Tor-Netzwerk, da auch bei diesen nicht von außen auf individuelle Telekommunikationsvorgänge zugegriffen wird.[1930] Da außerdem nach hier vertretener Auffassung vom Schutzbereich des Telekommunikationsgeheimnisses nicht das Verschlüsseln von Telekommunikation erfasst ist, kann in entsprechender Anwendung auch das Verschleiern von Telekommunikationsumständen nicht vom Schutzbereich des Telekommunikationsgeheimnis erfasst sein, sodass der Schutzbereich nicht eröffnet ist, wenn die Nutzung des Tor-Netzwerkes unterbunden wird.[1931]

Ebenfalls nicht eröffnet ist der Schutzbereich des IT-Grundrechts, da bei dem staatlichen Zugriff auf eine Blockchain weder Vertraulichkeits- noch Integritätserwartungen verletzt werden. Maßgeblicher Grund hierfür ist, dass die Daten aus offenen Netzwerken zur Kenntnis genommen werden.[1932]

1927 Siehe hierzu Kap. 4, B.I.1.c)(1).
1928 Siehe hierzu Kap. 4, B.I.1.c)(5).
1929 Siehe hierzu Kap. 4, B.I.2.a).
1930 Siehe hierzu Kap. 4, B.I.2.b).
1931 Siehe hierzu Kap. 4, B.I.2.b)(3).
1932 Siehe hierzu Kap. 4, B.III.3.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

C. Verfassungsrechtliche Rechtfertigung dieses Eingriffs

Als Rechtfertigung für diesen Grundrechtseingriff kann zum Zweck der Strafverfolgung nur § 161 Abs. 1 StPO herangezogen werden, der jedoch einen Anfangsverdacht voraussetzt und nur zu geringfügigen Grundrechtseingriffen ermächtigt.

I. § 161 Abs. 1 StPO als einschlägige Ermittlungsbefugnis

§ 161 Abs. 1 StPO ist als Ermächtigungsgrundlage einschlägig, da keine der speziellen Ermittlungsbefugnisse der StPO einschlägig ist und auch keine Vergleichbarkeit mit besonders geregelten Ermittlungsbefugnissen vorliegt.[1933]

So ermächtigen etwa die Vorschriften zur Sicherstellung und Beschlagnahme nach §§ 94ff. StPO zwar auch zur Auswertung von sichergestellten Daten. Bei den hier gegenständlichen Auswertungsmethoden steht allerdings nicht das Verfügbarmachen von Daten im Vordergrund steht, sondern deren Auswertung.[1934]

Ebenfalls nicht einschlägig ist die Ermittlungsbefugnis zur Rasterfahndung nach § 98a StPO. Zwar ermächtigt § 98a StPO grundsätzlich zu einem maschinellen Datenabgleich personenbezogener Daten, erforderlich ist jedoch, dass sich dieser Datenabgleich auf Daten bezieht, die entweder zuvor freiwillig herausgegeben wurden oder nach § 98a Abs. 2 StPO erhoben wurden. Für die von den Auswertungsmethoden betroffenen Daten ist keine dieser Varianten auf Grund des begrenzten Wortlauts von § 98a Abs. 2 StPO der Fall.[1935]

Schließlich sind auch §§ 98c StPO, 100a, 100b, 100g, 100j StPO nicht einschlägig. § 98c StPO bezieht sich nur auf den internen maschinellen Datenabgleich.[1936] § 100a StPO ist nicht einschlägig, da bereits der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet ist.[1937] § 100b StPO ermächtigt nur zu einem Zugriff auf informationstechnische Systeme auf einem technisch nicht dafür vorgesehenen Weg.[1938] Schließlich liegen in den erhobenen Da-

1933 Siehe hierzu insgesamt Kap. 5, B.
1934 Siehe hierzu im Einzelnen unter Kap. 5, B.I.
1935 Siehe hierzu im Einzelnen unter Kap. 5, B.II.
1936 Siehe hierzu im Einzelnen unter Kap. 5, B.III.
1937 Siehe hierzu im Einzelnen unter Kap. 5, B.IV.
1938 Siehe hierzu im Einzelnen unter Kap. 5, B.V.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ten weder Verkehrs- noch Bestandsdaten im Sinne der §§ 100g, 100j StPO vor, sodass auch diese nicht einschlägig sind.[1939]

II. Einsatz der Auswertungsmethoden nur bei bestehendem Anfangsverdacht

Auf Grund des für § 161 Abs. 1 StPO erforderlichen Anfangsverdachts können die Auswertungsmethoden jeweils nur dann eingesetzt werden, wenn bereits aus anderen Gründen der Verdacht einer Straftat besteht.[1940] Ein Einsatz zur (unmittelbaren) Begründung eines Anfangsverdachts ist dagegen nicht zulässig – selbst wenn die Blockchain-Daten nach Transaktionsmustern durchsucht werden, die mit sehr hoher Wahrscheinlichkeit im Zusammenhang mit illegalen Aktivitäten stehen.[1941] Denn grundsätzlich ist für den Anfangsverdacht das Vorliegen zureichender tatsächlicher Anhaltspunkte erforderlich, die auf eine Straftat hindeuten.

Dies ist weder beim proaktiven Aufklären von Dunkelfeldern noch bei sog. Vorermittlungen der Fall.[1942] Darüber hinaus nahm das BVerfG im MIKADO-Fall zwar einen Anfangsverdacht für die Abfrage von bestimmten Kreditkartendaten an, die sich auf konkrete Tatumstände, wie etwa ein bestimmter Buchungsbetrag zugunsten eines bestimmten Zahlungsempfängers unter Angabe einer bestimmten Merchant-ID, bezog.[1943] Dies kann jedoch hier keine Anwendung auf die Suche nach Transaktionsmustern finden, da im MIKADO-Fall des BVerfG nach Tätern bei bereits bestehendem Anfangsverdacht gesucht wurde, wohingegen bei der Suche nach bestimmten Transaktionsmustern eine *Tat-* und keine *Tätersuche* vorliegt.[1944]

III. Nur geringfügige Grundrechtseingriffe nach § 161 Abs. 1 StPO

Ein noch geringfügiger Grundrechtseingriff liegt vor, wenn beim sog. *Entitäts-Clustering* lediglich eine bereits aus anderen Gründen verdächtige

1939 Siehe hierzu im Einzelnen unter Kap. 5, B.VI., VII.
1940 Siehe hierzu unter Kap. 5, D.I.2.b).
1941 Siehe hierzu unter Kap. 5, D.I.2.a), c).
1942 Siehe hierzu unter Kap. 5, D.I.1.a), d).
1943 Siehe hierzu unter Kap. 5, D.I.1)g).
1944 Siehe hierzu unter Kap. 5, D.I.2.c).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Transaktion oder *Bitcoin-Adresse* betrachtet wird.[1945] Hinsichtlich der Auswertungsmethoden, die darüber hinaus Transaktionsverhalten und -muster ermitteln und vergleichen, liegt ein geringfügiger Grundrechtseingriff allenfalls vor, wenn diese in der Form eines „Treffer-/Nichttreffer-Modells" eingesetzt werden, um zu vermeiden, dass eine große Anzahl Unbeteiligter von weiteren strafrechtlichen Ermittlungen betroffen wird.[1946] Nicht mehr geringfügig sind die mit diesen Auswertungsmethoden verbundenen Grundrechtseingriffe allerdings, wenn die Blockchain-Daten insgesamt anlassunabhängig durch eine dieser Auswertungsmethoden systematisch analysiert werden.[1947]

Denn bei der Auswertung von unmittelbaren Blockchain-Daten ist die Grundrechtsintensität zwar insbesondere dadurch erhöht, dass bei den ausgewerteten Blockchain-Daten eine insgesamt große Datenmenge vorliegt, die heimlich erhoben wird, systematisch und technikgestützt ausgewertet wird und auf Grund ihrer Nähe zu Kontoinformationen wohl eine besondere Persönlichkeitsrelevanz aufweisen kann.[1948] Intensitätsverringernd ist jedoch zu beachten, dass die Erhebung der Blockchain-Daten selbst noch keinen Grundrechtseingriff begründet, die Blockchain-Daten öffentlich verfügbar sind und erst durch Zusatzwissen einer Person zugeordnet werden können.[1949]

Unterschiedlich ist bei den einzelnen Auswertungsmethoden allerdings die Streubreite zu berücksichtigen, die mit der jeweiligen technischen Funktionsweise einhergeht.[1950]

So kann etwa das einfache *Entitäts-Clustering,* soweit es bezogen auf eine bestimmte *Bitcoin-Adresse* oder Transaktion stattfindet, mit einer einfachen Suchfunktion verglichen werden. Hierbei werden nur Transaktionen und weitere *Bitcoin-Adressen* ermittelt, die im Zusammenhang mit dieser bestimmten Bitcoin-Adresse oder Transaktion stehen.[1951] Insoweit findet zwar grundsätzlich ein Datenabgleich aller in der Blockchain enthaltenen Transaktionen statt, ein Grundrechtseingriff liegt jedoch bei den Nichttreffern

1945 Siehe hierzu im Einzelnen unter Kap. 5, D.II.3.a).
1946 Siehe hierzu im Einzelnen unter Kap. 5, D.II.3.b), c).
1947 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1948 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1949 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1950 Siehe hierzu jeweils unter Kap. 5, D.II.3.a), b), c).
1951 Siehe hierzu unter Kap. 5, D.II.3.a).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nicht vor, da diese anonym und spurenlos wieder ausgeschieden werden und sich auch kein spezifisches Interesse an diesen Daten verdichtet hat.[1952]

Anders muss dies bewertet werden bei den Auswertungsmethoden, die Transaktionen und *Bitcoin-Adressen* mit bestimmten Transaktionsmustern vergleichen. Denn hierbei ist jeweils erforderlich, dass vor dem Abgleich, ob eine bestimmte Transaktion einem bestimmten Muster ähnelt oder nicht, durch eine systematische Analyse ein entsprechendes Muster überhaupt erst ermittelt wird.[1953] Die derart erhöhte Streubreite führt dazu, dass grundsätzlich kein geringfügiger Grundrechtseingriff mehr vorliegt. Geringfügig kann der Grundrechtseingriff daher allenfalls noch sein, wenn lediglich ein „Treffer-/Nichttreffer-Modell" verwendet wird.[1954]

Zu einem anderen Ergebnis gelangt die Bewertung der Grundrechtsintensität der Auswertungen des Netzwerkverhaltens. Bei diesen Auswertungsmethoden liegt grundsätzlich kein geringfügiger Grundrechtseingriff mehr vor, sodass sie nicht auf § 161 Abs. 1 StPO gestützt werden können.[1955] Denn bei der Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten liegt bereits ein Grundrechtseingriff durch die Erhebung der Daten vor, sodass insoweit auch eine erhöhte Streubreite vorliegt.[1956] Ähnlich gilt dies für die sog. *Bloom-Filter-Attacks,* da dies in der Ermittlungspraxis nur sinnvoll einsetzbar ist, wenn in einem konkreten Verdachtsfall bei allen *SPV-Clients* abgefragt werden müsste, ob eine verdächtige *Bitcoin-Adresse* in dem jeweiligen *Bloom-Filter* enthalten ist.[1957] Nur so kann die Zuordnung einer verdächtigen *Bitcoin-Adresse* zu einer bestimmten IP-Adresse vorgenommen werden.

Schließlich hängt die Grundrechtsintensität der Auswertung anderweitig verfügbarer Daten wohl von deren konkretem Einsatz ab.[1958] So dürfte ein noch geringfügiger Grundrechtseingriff vorliegen, wenn lediglich im öffentlich verfügbaren Internet nach einer bestimmten *Bitcoin-Adresse* gesucht wird.[1959] Anders ist dies jedoch zu beurteilen, wenn anlassunabhängig mittels *Web-Crawler* die öffentlich verfügbaren Inhalte im Internet nach möglichst vielen Hintergrundinformationen durchsucht werden, um so

1952 Siehe hierzu unter Kap. 5, D.II.3.a).
1953 Siehe hierzu jeweils unter Kap. 5, D.II.3.b), c).
1954 Siehe hierzu jeweils unter Kap. 5, D.II.3.b), c).
1955 Siehe hierzu insgesamt unter Kap. 5, D.II.3.d).
1956 Siehe hierzu unter Kap. 5, D.II.3.d).
1957 Siehe hierzu unter Kap. 5, D.II.3.d)(4).
1958 Siehe hierzu insgesamt unter Kap. 5, D.II.3.e)
1959 Siehe hierzu unter Kap. 5, D.II.3.e)(1).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

hierauf im Verdachtsfall zurückgreifen zu können.[1960] Hinsichtlich der Auswertung von Dritt-Anbieter-Cookies und IoT-Blockchain-Anwendungen hängt die jeweilige Grundrechtsintensität grundsätzlich von deren konkreter Umsetzung ab.[1961] Dabei dürfte insbesondere relevant werden, ob und welche Rückschlüsse auf die Persönlichkeit gezogen werden können und ob und wie viele Unbeteiligte von den Auswertungsmethoden betroffen werden.

D. Empfehlung und Ausblick

Zusammenfassend lässt sich festhalten, dass die Blockchain-Technologie neben dem Entwicklungspotenzial, das ihr zugeschrieben wird, auch viele Ansatzpunkte für strafrechtliche Ermittlungen bieten kann. Einige dieser Auswertungsmethoden lassen sich zwar als geringfügige Grundrechtseingriffe noch auf die strafprozessualen Ermittlungsgeneralklauseln stützten, andere Auswertungsmethoden übersteigen dagegen die Grenze der Geringfügigkeit. Dies kann zur Rechtsunsicherheit führen. Denn die Untersuchung hat auch gezeigt, dass die Bewertung der Grundrechtsintensität einerseits aufwändig ist und andererseits von vielen einzelnen Faktoren abhängt. Das könnte zur Folge haben, dass bereits bei geringfügigen technischen Anpassungen sowohl der jeweils ausgewerteten Blockchain als auch der eingesetzten Auswertungsmethode der Einsatz der Auswertungsmethoden als nicht mehr nur geringfügiger Grundrechtseingriff zu bewerten ist. Insoweit müsste bei jeder technischen Anpassung auch eine angepasste Bewertung der Grundrechtsintensität vorgenommen werden – immer mit der Gefahr verbunden, dass eine nicht mehr nur geringfügige Intensität vorliegt.

Empfehlenswert ist daher die Neuregelung derartiger Ermittlungsmöglichkeiten in der vorgeschlagenen Form eines § 98a Abs. 2 S. 2 StPO:

> *„Zu diesem Zweck sind die Strafverfolgungsbehörden außerdem ermächtigt, allgemein zugängliche Daten zu erheben und für den Abgleich zu verarbeiten.“*[1962]

Denn hierdurch würde Rechtssicherheit dahingehend geschaffen, dass auch öffentlich verfügbare personenbezogene Daten unter bestimmten Voraus-

1960 Siehe hierzu unter Kap. 5, D.II.3.e)(1).
1961 Siehe hierzu unter Kap. 5, D.II.3.e)(2), (3).
1962 Siehe hierzu im Einzelnen unter Kap. 5, F.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

setzungen zur Strafverfolgung maschinell abgeglichen werden dürfen. Das wäre zugleich ein erster Schritt in Richtung auf die grundlegende Frage, wie öffentlich verfügbare Daten zur Strafverfolgung ausgewertet werden dürfen. Denn im Rahmen der vorstehenden Untersuchung ist unter anderem auch aufgefallen, dass die Ermittlungsbefugnisse der StPO vorrangig an die Art und Weise der Datenerhebung anknüpfen. Dagegen stellen sie nicht auf die Art und Weise der Auswertung von Daten ab. Die Art und Weise der Auswertung von Daten kann jedoch – wie die vorstehende Untersuchung gezeigt hat – ähnlich ausschlaggebend für die Intensität von Grundrechtseingriffen sein. Und sie ist erst recht relevant angesichts der technischen Dynamik und der damit verbundenen Möglichkeiten, die in diesem Bereich zu erwarten sind.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

Stichwortverzeichnis zu technischen Begriffen

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" bezeichnet wird.
Bloom-Filter-Attack	– Verknüpfung einer IP-Adresse zu einer oder mehreren Bitcoin-Adressen durch Abfrage bei dem von SPV-Clients verwendeten Bloom-Filtern, die einen schnellen Abgleich ermöglichen, ob ein bestimmter Datensatz in einer Datenstruktur enthalten ist
Candidate-block	– Datenblock, der von einem *miner* erstellt wurde, aber noch nicht vom Netzwerk als Teil der Blockchain bestätigt wurde
Classifier	– Algorithmus, der typischen Eigenschaften von bestimmtem Transaktionsverhalten ermittelt
Clustering	– Auswertung von großen Datensätzen, um Ähnlichkeiten und Unterschiede aufzudecken
Denial-of-Service (kurz: DoS)	– Nichtverfügbarkeit eines Netzwerks; regelmäßig auf Grund von Überlastung durch zu viele Anfragen
Distributed-Ledger (-Technologie)	– „verteiltes Kontobuch" (öffentlich), dezentral geführtes Register
DNS-Blockade	– Sperrmaßnahme, die am *Domain Name System* ansetzt. Bei bestimmten Domain-Namen findet keine Weiterleitung mehr an die jeweilige IP-Adresse mehr statt
Domain Name System	– Zentraler Server, der für die Kommunikation im Internet bestimmte Domain-Namen einzelnen IP-Adressen zuordnet
Double Spending	– Doppelte Ausgabe der gleichen Werteinheit
Entität	– Person oder Organisation, die über eine oder mehrere Bitcoin-Adressen verfügen kann
Ethereum	– Weiterentwicklung der Bitcoin-Blockchain – Erlaubt Nutzern, eigene Anwendungen – insbesondere *Smart Contracts* – auf ihr abzulegen und ist entwicklungsoffen
Exit-Relay	– Server im Tor-Netzwerk, über den auf das tatsächliche Kommunikationsziel zugegriffen wird

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Guard-Relay	– Server im Tor-Netzwerk, mit dem sich der Tor-Nutzer zuerst verbindet
Hashfunktion	– Rechnerische Funktion, durch die eine Zeilenfolge beliebiger Länge in eine Zeichenfolge mit einheitlicher Länge dargestellt wird
Hashwert	– Ergebnis einer *Hashfunktion*
IMSI-Catcher	– Ermittlungsinstrument, mit dem eine virtuelle Funkzelle simuliert werden kann und so die IMSI oder IMEI eines bestimmten Gerätes erhoben werden kann
Input	– Absendeadresse einer Bitcoin-Transaktion
Internet-of-Things (kurz: IoT)	– Sammelbegriff für Technologien, die es ermöglichen, dass Gegenstände miteinander kommunizieren
IP-Adressen-Sperre	– Weiterleitung von Telekommunikation wird dadurch verhindert, dass bestimmte IP-Adressen aus den Routing-Tabellen, die zur Weiterleitung von Kommunikation eingesetzt werden, gelöscht werden
Labelling	– Kategorisierung einer Bitcoin-Entität
Memory-pool	– Pool der Transaktionsnachrichten, die noch nicht in die Blockchain aufgenommen wurden
Middle-Relay	– Server im Tor-Netzwerk, der zwischen den Beginn und das Ende der Kommunikation geschaltet wird (siehe Guard- und Exit-Relay)
Miner	– *Node,* der die Blockchain fortschreibt
Node	– Knotenpunkt von Kommunikationsnetzen – In dezentralen Kommunikationsnetzen läuft die Kommunikation darüber, dass die *nodes* die Kommunikation an die anderen *nodes* verteilen
Output	– Empfangsadresse einer Bitcoin-Transaktion
Peer-to-Peer-Netzwerk	– Dezentrales Kommunikationsnetzwerk über das Internet, in dem die Kommunikation nicht über zentrale Knoten läuft, sondern zwischen den Teilnehmern direkt erfolgt
Private und Public key	– Asymmetrisches Schlüsselpaar mit dem Bitcoin-Nutzer im Netzwerk aktiv werden – *Public key* dient zum Empfang von Transaktionen – *Private key* dient zur Authentifizierung von Transaktionsnachrichten
Route	– Ablauf der Netzwerkverbindung, über die die Kommunikation im Tor-Netzwerk abläuft

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Simplified Payment Verification (kurz: SPV)	– Vereinfachte Transaktionsbestätigung zur Datenreduzierung
Smart Contract	– Software, die rechtlich relevante Handlungen in Abhängigkeit von digital überprüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert[1963]
Token	– Ausschließlicher, einzigartiger und nicht vervielfältigbarer Eintrag in einer Datenbank[1964] – Kann Forderungen und Rechte abbilden
Tor-Netzwerk/ -Browser	– Verschleierung von IP-Adressen durch mehrfache Weiterleitung der Kommunikation
Unspent transaction output	– Nicht weitergeleitete Transaktionen
URL-Sperre	– Sperrmaßnahme, bei der Anfragen von bestimmten URLs nicht weitergeleitet werden
Vehicular Ad Hoc Network (kurz: VANET)	– Kommunikationssystem für KfZ, um andere Verkehrsteilnehmer über Verkehrsverhältnisse zu informieren
Wallets	– Digitale Brieftasche, in der die *public* und *private keys* eines Nutzers gespeichert werden – Häufig von Nutzern verwendet, da sie häufig mehr als nur einen *public key* verwenden
Web-Crawler	– Algorithmus, der das Internet oder bestimmte Internetseiten automatisch nach vorher festgelegten Daten durchsucht
Webtracker	– Analyseprogramm, das das Nutzungsverhalten von Internetnutzern auswertet

1963 *Kaulartz/Heckmann*, CR 2016, 618 (618).
1964 *Kaulartz/Matzke*, NJW 2018, 3278 (3278).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY - https://www.nomos-elibrary.de/agb

Literaturverzeichnis

Androulaki, Elli/ Karame, Ghassan O./ Roeschlin, Marc/ Scherer, Tobias/ Capkun, Srdjan: Evaluating user privacy in Bitcoin, in: *Sadeghi, Ahmad-Reza* (Hrsg.) Financial Cryptography and Data Security, 17th International Conference, FC2013, Revised Selected Papers, Lecture Notes in Computer Science, vol 7859, Berlin Heidelberg 2013, S. 34–51, abrufbar unter: https://doi.org/10.1007/978-3-642-39884-1_4 (letzter Abruf: 20. Dezember 2021).

Antonopoulos, Andreas: Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Sebastopol, CA 95472, 2014.

Art. 29 Datenschutzgruppe: WP 216, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216, 10. April 2014 abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/wp216_de.pdf (letzter Abruf: 20. Dezember 2021).

Art. 29 Datenschutzgruppe: WP 217, Stellungnahme 6/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09. April 2014, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf (letzter Abruf 20. Dezember 2021).

Axer, Peter: § 67 Zitiergebot, in: *Merten, Detlef/ Papier, Hans-Jürgen* (Hrsg.): Handbuch der Grundrechte in Deutschland und Europa, Band III, 1. Auflage, Heidelberg 2009 (zitiert als: HGR Bd. III/*Axer*).

Bäcker, Matthias: Die Vertraulichkeit der Internetkommunikation, in: Linien der Rechtsprechung des Bundesverfassungsgerichts Band 1, Brink/Rensen, Berlin 2009.

Bär, Wolfgang: Die Neuregelung zur Erhebung von Verkehrsdaten (§ 100g StPO) – Inhalt und Auswirkungen, Neue Strafrechtszeitschrift 2017, S. 81–86.

Bauer, Sebastian: Soziale Netzwerke und Strafprozessuale Ermittlungen, Strafrechtliche Abhandlungen. Neue Folge – Band 281, Schroeder/Hoyer, Berlin 2018.

Bechtholf, Hans/ Vogt, Niklas: Datenschutz in der Blockchain – Eine Frage der Technik, Zeitschrift für Datenschutz 2018, S. 66–71.

Becker, Jörg-Peter/ Erb, Volker/ Esser, Robert/ Graalmann-Scheerer, Kirsten/ Hilger, Hans/ Ignor, Alexander (Hrsg.): Löwe/Rosenberg Die Strafprozeßordnung und das Gerichtsverfassungsgesetz Großkommentar, 27. Auflage, Berlin 2018 (zitiert als: Löwe-Rosenberg/*Bearbeiter*).

Bergt, Matthias: Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, Zeitschrift für Datenschutz 2015, S. 365–371.

Beulke, Werner/ Rogat, Stefan: Anmerkungen zum Urteil des BGH v. 7.7.1995 – 1 StR 685/94, Juristische Rundschau 1996, S. 515–521.

Biryukov, Alex/ Khovratovich, Dmitry/ Pustogarov, Ivan: Deanonymisation of clients in Bitcoin P2P network, arXiv:1405.7418 [cs.CR] 2014, S. 1–15, abrufbar unter: https://arxiv.org/pdf/1405.7418.pdf (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Biryukov, Alex/ Pustogarov, Ivan: Bitcoin over tor isn't a good idea, arXiv:1410.6079 [cs.CR] 2015, S. 122–134, abrufbar unter: https://arxiv.org/pdf/1410.6079.pdf (letzter Abruf: 20. Dezember 2021).

Blechschmitt, Lisa: Strafverfolgung im digitalen Zeitalter, Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, Multimedia und Recht 2018, S. 361–366.

BMWi/ BMF: Blockchain-Strategie der Bundesregierung, Wir stellen die Weichen für die Token-Ökonomie, 2019, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=22 (letzter Abruf: 20. Dezember 2021).

Bock, Dennis: Zur Antizipation künftiger Strafverfolgung als Teil einer modernen Strafrechtspflege, Zeitschrift für Internationale Strafrechtsdogmatik 2006, S. 129–133.

Bockemühl, Jan: Private Ermittlungen im Strafprozeß, Ein Beitrag zu der Lehre von den Beweisverboten, Baden-Baden 1996.

Böckenförde, Thomas: Die Ermittlung im Netz, Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003.

Böckenförde, Thomas: Auf dem Weg zur elektronischen Privatsphäre, JuristenZeitung 2008, S. 925–939.

Böse, Martin: Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, Göttingen 2007.

Bode, Thomas A.: Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin Heidelberg 2012.

Boehm, Franziska/ Pesch, Paulina: Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, Eine erste juristische Einordung, Multimedia und Recht 2014, S. 75–78.

Böhme, Rainer/ Grzywotz, Johanna/ Pesch, Paulina/ Rückert, Christian/ Safferling, Christoph: Prävention von Straftaten mit Bitcoins und Alt-Coins, Handlungsempfehlung zur Regulierung virtueller Kryptowährungen, Stand: 2017, https://www.bitcrime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf (letzter Abruf: 20. Dezember 2021).

Böhme, Rainer/ Pesch, Paulina: Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, Datenschutz und Datensicherheit 2017, S. 473–481.

Börner, René: Kryptowährungen und strafbarer Marktmissbrauch, Neue Zeitschrift für Wirtschaftsstrafrecht 2018, S. 48–54.

Breidenbach, Stephan/ Glatz, Florian (Hrsg.): Rechtshandbuch Legal Tech, 2. Auflage, München 2021 (zitiert als: Breidenbach-Glatz RhdB-Legal-Tech/*Bearbeiter*).

Brian, Ilka/ Frey, Tobias/ Krais, Tobias: Umsetzung der Fünften Geldwäsche-Richtlinie in Deutschland, Corporate Compliance Zeitschrift 2019, S. 245–262.

Brink, Stefan/ Wolff, Heinreich Amadeus (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 38. Edition, München 2021 (zitiert als: BeckOK-DSR/*Bearbeiter*).

Britz, Gabriele: Vertraulichkeit und Integrität informationstechnischer Systeme – Einige Fragen zu einem „neuen Grundrecht", Die Öffentliche Verwaltung 2008, S. 411–416.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Brunhöber, Beatrice: Privatisierung des Ermittlungsverfahrens im Strafprozess, Goltdammer's Archiv für Strafrecht, 2010, S. 571–588.

Buermeyer, Ulf: Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug, Verwirklichungsbedingungen im Vollzug von Freiheitsentziehungen, Baden-Baden 2019.

Buterin, Vitalik: Ethereum White Paper, Stand: 2015, abrufbar unter http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (letzter Abruf: 20. Dezember 2021).

Chan, Wren/ Olmsted, Aspen: Ethereum Transaction Graph Analysis, 2017 12th International Conference for Internet Technology and Secured Transactions 2017, S. 498–500, abrufbar unter: https://doi.org/10.23919/ICITST.2017.8356459 (letzter Abruf: 20. Dezember 2021).

Chen, Weili/ Zheng, Zibin/ Ngai, Edith/ Zheng, Peilin/ Zhou, Yuren, Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum, IEEE Access vol. 7, 2019, S. 37575–37586, abrufbar unter https://doi.org/10.1109/ACCESS.2019.2905769 (letzter Abruf: 20. Dezember 2021).

Dreier, Horst (Hrsg.): Grundgesetz-Kommentar Band 1, 3. Auflage, Tübingen 2013,

(zitiert als: Dreier Bd. 1/*Bearbeiter*).

Durner, Wolfgang: Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet*?, Zeitschrift für Urheber- und Medienrecht 2010, S. 833–846.

Ehmann, Eugen/ Selmayr, Martin (Hrsg.): DS-GVO Datenschutzgrundverordnung Kommentar, 2. Auflage, München 2018 (zitiert als: Ehmann-Selmayr/*Bearbeiter*).

Eisenberg, Ulrich/ Singelnstein, Tobias: Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS", Neue Strafrechtszeitschrift 2005, S. 62–67.

Eisenmenger, Florian: Die Grundrechtsrelevanz „virtueller Streifenfahrten" – dargestellt am Beispiel ausgewählter Kommunikationsdienste des Internets, Strafrechtliche Abhandlungen, Neue Folge, Band 276, Berlin 2017.

Epping, Volker/ Hillgruber, Christian (Hrsg.): Beck'scher Online-Kommentar Grundgesetz, 49. Edition, München 2021 (zitiert als: BeckOK-GG/*Bearbeiter*).

Esser, Martin/ Kramer, Philipp/ Lewinski, Kai (Hrsg.): Auernhammer DSGVO BDSG, 7. Auflage, Köln 2020 (zitiert als: Auernhammer/*Bearbeiter*).

Feld, Sebastian/ Schönfeld, Mirco/ Werner, Martin: Analyzing the deployment of bitcoin's P2P network under an as-level perspective, Procedia Computer Science vol. 32, 2014, S. 1121–1126, abrufbar unter: https://doi.org/10.1016/j.procs.2014.05.542 (letzter Abruf: (letzter Abruf: 20. Dezember 2021).

Finck, Michèle: Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, PE 634.445, 2019, abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU%282019%29634445_EN.pdf (letzter Abruf: (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Fleder, Michael/ Kester, Michael S./ Pillai, Sudeep: Bitcoin Transaction Graph Analysis, arXiv:1502.01657 [cs.CR] 2015, S. 1–8, abrufbar unter: https://arxiv.org/pdf/1502.01657.pdf (letzter Abruf: 20. Dezember 2021).

Foley, Sean/ Karlsen, Jonathan R./ Putnins, Talis J.: Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?, The Review of Financial Studies, Volume 32, Issue 5, 2019, S. 1798–1853, abrufbar unter: https://doi.org/10.1093/rfs/hhz015 (letzter Abruf: 20. Dezember 2021).

Frey, Dieter/ Rudolph, Matthias/ Oster, Jan: Internetsperren und der Schutz der Kommunikation im Internet, Multimedia und Recht, Beilage 2012, Heft 3, S. 1–26.

Frey, Tobias/ Pelz, Christian (Hrsg.): Beck'scher Online-Kommentar Geldwäschegesetz, 7. Edition, München 2021 (zitiert als: BeckOK-GwG/*Bearbeiter*).

Fröwis, Michael/ Gottschalk, Thilo/ Haslhofer, Bernhard/ Rückert, Christian/ Pesch, Paulina: Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations, arXiv:1906.12221 [cs.CY] 2019, S. 1–23, abrufbar unter: https://arxiv.org/pdf/1906.12221v1.pdf (letzter Abruf: 20. Dezember 2021).

Gercke, Björn: Rechtliche Probleme durch den Einsatz des IMSI-Catchers, Multimedia und Recht 2003, S. 453–456.

Gercke, Björn: Gesetzliche Regelung des Einsatzes von V-Leuten im Rahmen der Strafverfolgung? Von Verfassungs wegen geboten, Der Strafverteidiger 2017, S. 615–626.

Gercke, Björn/ Julius, Karl-Peter/ Temming, Dieter/ Zöller, Mark A. (Hrsg.): Strafprozessordnung, 6. Auflage, Heidelberg 2019 (zitiert als: Gercke/Julius/Temming/Zöller/*Bearbeiter*).

Gerhards, Julia: (Grund-)Recht auf Verschlüsselung?, Der elektronische Rechtsverkehr, Band 23, Baden-Baden 2010.

Gersdorf, Hubertus/ Paal, Boris P. (Hrsg.): Beck'scher Online-Kommentar Informations- und Medienrecht, 34. Edition, München 2021 (zitiert als BeckOK-InfoMedienR/*Bearbeiter*).

Gervais, Arthur/ Karame, Ghassan O/ Gruber, Damian/ Capkun, Srdjan: On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients, ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference, 2014, S. 326–335, abrufbar unter: https://doi.org/10.1145/2664243.2664267 (letzter Abruf: 20. Dezember 2021).

Glatz, Florian: Blockchain – Bitcoin – Smart Contracts – Anwendungsmöglichkeiten, DGRI Jahrbuch 2016, Köln 2017, S. 81–93.

Goldfeder, Steven/ Kalodner, Harry/ Reisman, Dillon/ Narayanan, Arvind: When the cookie meets the blockchain, Privacy risks of web payments via cryptocurrencies, arXiv:1708.04748v1 [cs.CR] 2017, S. 1–19, abrufbar unter: https://arxiv.org/pdf/1708.04748.pdf (letzter Abruf: 20. Dezember 2021).

Graf, Jürgen (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 41. Edition, München 2021 (zitiert als: BeckOK-StPO/*Bearbeiter*).

Graulich, Kurt: Strafverfolgungsvorsorge, Gegenstand und rechtliche Verortung, Neue Zeitschrift für Verwaltungsrecht 2014, S. 685–691.

Greve, Holger, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, Beiträge zum Informationsrecht Band 30, Berlin 2012.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Grünwald, Andreas/ Nüßing: Christoph: Kommunikation over the Top, Regulierung für Skype, WhatsApp oder Gmail?, Multimedia und Recht 2016, S. 91–97.

Grzywotz, Johanna: Virtuelle Kryptowährungen und Geldwäsche, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2018.

Grzywotz, Johanna/ Köhler, Olaf Markus/ Rückert, Christian: Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, Der Strafverteidiger 2016, S. 753–759.

Haas, Günter: Vorermittlungen und Anfangsverdacht, Schriften zum Prozessrecht, Band 178, Berlin 2003.

Harlev, Mikkel Alexander/ Sun Yin, Haohua/ Langenheldt, Klaus Christian/ Mukkamala, Raghava/ Vatrapu, Ravi: Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning, Proceedings of the 51st Hawaii International Conference on System Sciences 2018, S. 3497–3506, abrufbar unter: http://hdl.handle.net/10125/50331 (letzter Abruf: 20. Dezember 2021).

Heckelmann, Martin: Zulässigkeit und Handhabung von Smart Contracts, Neue Juristische Wochenschrift 2018, S. 504–510.

Hefendehl, Roland: Die neue Ermittlungsgeneralklausel der §§ 161, 163 StPO: Segen oder Fluch?, Der Strafverteidiger 2001, S. 700–706.

Hellmann, Uwe: Strafprozessrecht, 2. Auflage, Heidelberg 2006.

Herbst, Tobias: Was sind personenbezogene Daten?, Neue Zeitschrift für Verwaltungsrecht 2016, S. 902–906.

Herzog, Felix/ Achtelik, Olaf (Hrsg.): Geldwäschegesetz (GwG), 4. Auflage, München 2020, (zitiert als: Herzog-GwG/*Bearbeiter*).

Herzog, Roman/ Herdegen, Matthias/ Scholz, Rupert/ Klein, Hans H. (Hrsg.): Grundgesetz Kommentar begründet von Theodor Maunz und Günter Dürig, 95. Ergänzungslieferung, München 2021, (zitiert als: Dürig/Herzog/Scholz/*Bearbeiter*).

Hilger, Hans: Zum Strafverfahrensrechtsänderungsgesetz 1999 (StVÄG 1999) – 1. Teil, Neue Strafrechtszeitschrift 2000, S. 561–565.

Hillgruber, Christian: § 201 Grundrechtsschranken, in: *Isensee, Josef/ Kirchhof, Paul* (Hrsg.): Handbuch des Staatsrechts, Band IX, 3. Auflage, Heidelberg 2011 (zitiert als: HStR Bd. IX/*Hillgruber*).

Hirshman, Jason/ Huang, Yifei/ Macke, Stephen: Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network, 2013, abrufbar unter: http://cs229.stanford.edu/proj2013/HirshmanHuangMacke-UnsupervisedApproachesToDetectingAnomalousBehaviorInTheBitcoinTransactionNetwork.pdf (letzter Abruf: 20. Dezember 2021).

Hofert, Eduard: Blockchain-Profiling Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke, Zeitschrift für Datenschutz 2017, S. 161–165.

Hofert, Eduard: Regulierung der Blockchains, Hoheitliche Steuerung der Netzwerke im Zahlungskontext, Internet und Gesellschaft, Band 14, Tübingen 2018.

Hoffer, Raoul/ Mirtchev, Kristina: Erfordert die Blockchain ein neues Kartellrecht ? – Die Anwendung von Art. 101 und 102 AEUV sowie der Zusammenschlusskontrolle im Kontext der Blockchain-Technologie, Neue Zeitschrift für Kartellrecht 2019, S. 239–247.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Hoven, Elisa: Die Grenzen des Anfangsverdachts – Gedanken zum Fall Edathy, Neue Strafrechtszeitschrift 2014, S. 361–367.

Hufen, Friedhelm: Staatsrecht II – Grundrechte, 8. Auflage, München 2020.

Ihwas, Saleh Ramadan: Strafverfolgung in Sozialen Netzwerken, Facebook & Co. Als moderne Ermittlungswerkzeuge, Baden-Baden 2014.

Jahn, Matthias: Anmerkungen zu BVerfG NJW 2009, 1405ff., Juristische Schulung 2009, S. 664–665.

Jahn, Matthias: Ermittlungen in Sachen Siemens/SEC, Legitimer Baustein des globalisierten Wirtschaftsstrafverfahrens oder rechtswidriges Parallelverfahren zur Strafprozeßordnung? – Eine Problemskizze, Der Strafverteidiger 2009, S. 41–46.

Janicki, Thomas/ Saive, David: Privacy by Design in Blockchain-Netzwerken, Zeitschrift für Datenschutz 2019, S. 251–256.

Kahler, Thomas; Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten, Baden-Baden 2017.

Kaulartz, Markus: Die Blockchain-Technologie, Computer und Recht 2016, S. 474–480.

Kaulartz, Markus/ Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie, Computer und Recht 2016, S. 618–624.

Kaulartz, Markus/ Matzke, Robin: Die Tokenisierung des Rechts, Neue Juristische Wochenschrift 2018, S. 3278–3283.

Kielmansegg, Sebastian Graf von: Die Grundrechtsprüfung, Juristische Schulung 2008, S. 23–29.

Kielmansegg, Sebastian Graf von: Grundfälle zu den allgemeinen Grundrechtslehren, Juristische Schulung 2009, S. 118–124.

King, Sunny/ Nadal, Scott: PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, Stand: 2012, abrufbar unter: https://peercoin.net/whitepapers/peercoin-paper-de.pdf (letzter Abruf: 20. Dezember 2021).

Klesczewski, Diethelm: Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, Zeitschrift für die gesamte Strafrechtswissenschaft Band 123, 2011, S. 737–766.

Klöhn, Lars/ Parhofer, Nicolas/ Resas, Daniel: Initial Coin Offerings (ICOs), Markt, Ökonomik und Regulierung, Zeitschrift für Bankrecht und Bankwirtschaft 2018, S. 89–106.

Knaier, Ralf/ Wolf, Lothar: Die Blockchain-Technologie als Entwicklungsoption für das Handelsregister?, Betriebs-Berater 2018, S. 2253–2260.

Knauer, Christoph/ Kudlich, Hans/ Schneider, Hartmut (Hrsg.): Münchener Kommentar zur StPO, 1. Auflage, München 2014 (zitiert als: MüKo-StPO/*Bearbeiter*).

Kochheim, Dieter: Buchbesprechungen zu *Thomas Kahler:* Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten, Kriminalpolitische Zeitschrift, 2018, S. 314–320.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Koshy, Philip/ Koshy, Diana/ McDaniel, Patrick: An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, in: *Christin Nicolas/ Safavi, Reihaneh* (Hrsg.) Financial Cryptography and Data Security, 18th International Conference, FC 2014, Revised Selected Papers, Lecture Notes in Computer Science, vol 8437, Berlin Heidelberg 2014, S. 469–485, abrufbar unter: https://doi.org/10.1007/978-3-662-45472-5_30 (letzter Abruf: 20. Dezember 2021).

Körffer, Barbara: Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr – genügen die gesetzlichen Grundlagen zum Schutz des Rechts auf informationelle Selbstbestimmung?, Datenschutz Nachrichten 2014, S. 146–150.

Krause, Benjamin: Ermittlungen im Darknet – Mythos und Realität, Neue Juristische Wochenschrift 2018, S. 678–681.

Krausnick, Daniel: Grundfälle zu Art. 19 I und II GG, Juristische Schulung 2007, S. 1088–1093.

Krey, Volker/ Jaeger, Stefan: Einsatz eines verdeckten Ermittlers, Anm. zum BGH Urteil vom 07.03.1995 – 1 StR 985/94, Neue Strafrechtszeitschrift 1995, S. 516–519.

Krügel, Tina: Das personenbezogene Datum nach der DS-GVO – Mehr Klarheit und Rechtssicherheit?, Zeitschrift für Datenschutz 2017, S. 455–459.

Kudlich, Hans: Straftaten und Strafverfolgung im Internet, Der Strafverteidiger 2012, S. 560–566.

Kühling, Jürgen/ Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG Kommentar, 3. Auflage, München 2020 (zitiert als: Kühling-Buchner/*Bearbeiter*).

Kühling, Jürgen/ Schall, Tobias: WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, Computer und Recht 2015, S. 641–655.

Kühling, Jürgen/ Schall, Tobias: E-Mail-Dienste sind Telekommunikationsdienste i.S.d. § 3 Nr. 24 TKG, Computer und Recht 2016, S. 185–198.

Kütük, Merih Erdem/ Sorge, Christoph: Bitcoin im deutschen Vollstreckungsrecht, Von der „Tulpenmanie" zur „Bitcoinmanie", Multimedia und Recht 2014, S. 643–645.

Leistner, Matthias/ Grisse, Karina: Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), Gewerblicher Rechtsschutz und Uhrheberrecht 2015, S. 19–27.

Leonhardt, Andrea: Die Europäische Ermittlungsanordnung in Strafsachen, Umsetzungsanforderungen für den deutschen Gesetzgeber, Wiesbaden 2017.

The Libra Association Members: Cover Letter, White Paper, v2.0, Stand: 2020, abrufbar unter: https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf (letzter Abruf: 20. Dezember 2021).

Mann, Maximilian: Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp? Gesellschaftsrechtliche und kollisionsrechtliche Implikationen, Neue Zeitschrift für Gesellschaftsrecht 2017, S. 1014–1020.

Marberth-Kubicki, Annette: Der Beginn der Internet-Zensur – Zugangssperren durch Access-Provider, Neue Juristische Wochenschrift 2009, S. 1792–1796.

Martini, Mario: Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, Juristische Arbeitsblätter 2009, S. 839–845.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Martini, Mario/ Weinzierl: Quirin, Die Blockchain-Technologie und das Recht auf Vergessenwerden, Neue Zeitschrift für Verwaltungsrecht 2017, S. 1251–1259.

Maume, Philipp/ Maute, Lena/ Fromberger, Mathias (Hrsg.): Rechtshandbuch Kryptowerte, 1. Auflage, München 2020 (zitiert als: Maume/Maute Kryptowerte HdB/ *Bearbeiter*).

Meiklejohn, Sarah/ Pomarole, Marjori/ Jordan, Grant/ Levchenko, Kirill/ McCoy, Damon/ Voelker, Geoffrey M./ Savage, Stefan: A fistful of Bitcoins: Characterizing payments among men with no names, IMC '13: Proceedings of the 2013 conference on Internet measurement Conference, 2013, S. 127–140, abrufbar unter: https://doi.org/10.1145/2504730.2504747 (letzter Abruf: 20. Dezember 2021).

Meinel, Christoph/ Sack, Harald: Digitale Kommunikation, Vernetzen, Multimedia, Sicherheit, Berlin 2009.

Menges, Lea: Datenschützer äußern Bedenken zu Facebooks Libra, Stand: 2019, abrufbar unter: https://www.horizont.net/planung-analyse/nachrichten/kryptowaehrung-datenschuetzer-aeussern-bedenken-zu-facebooks-libra-176633 (letzter Abruf: 20. Dezember 2021).

Michael, Lothar/ Morlok, Martin: Grundrechte, 7. Auflage, Baden-Baden 2020.

Michl, Fabian: Sicherstellung von Daten durch die Polizei, Neue Zeitschrift für Verwaltungsrecht 2019, S. 1631–1637.

Middel, Stefan: Innere Sicherheit und präventive Terrorismusbekämpfung, Baden-Baden 2007.

Monamo, Patrick/ Marivate, Vukosi/ Twala, Bheki: Unsupervised Learning for Robust Bitcoin Fraud Detection, Information Security for South Africa ISSA 2016, S. 129–134.

Nachbaur, Andreas: Standortfeststellung und Art. 10 GG: Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", Neue Juristische Wochenschrift 2007, S. 335–337.

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, Stand: 2008, abrufbar unter: https://bitcoin.org/bitcoin.pdf (letzter Abruf: 20. Dezember 2021).

Nick, Jonas David: Data-Driven De-Anonymization in Bitcoin, Master Thesis 2015, abrufbar unter: https://jonasnick.github.io/papers/thesis.pdf (letzter Abruf: 20. Dezember 2021).

Oermann, Markus/ Staben, Julian: MITTELBARE GRUNDRECHTSEINGRIFFE DURCH ABSCHRECKUNG ? Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, Der Staat 2013, S. 630–661.

Ostapowicz, Michal/ Zbikowski, Kamil: Detecting Fraudulent Accounts on Blockchai : A Supervised Approach, arXiv:1908.07886 [cs.CR] 2019, S. 1–14, abrufbar unter: https://arxiv.org/pdf/1908.07886.pdf (letzter Abruf: 20. Dezember 2021).

Ostendorf, Heribert/ Frahm, Lorenz Nicolai/ Doege, Felix: Internetaufrufe zur Lynchjustiz und organisiertes Mobbing, Neue Strafrechtszeitschrift 2012, S. 529–538.

Ossenbühl, Fritz: § 101 Vorrang und Vorbehalt des Gesetzes, in: *Isensee, Josef/ Kirchhof, Paul* (Hrsg.): Handbuch des Staatsrechts, Band V, 3. Auflage, Heidelberg 2007 (zitiert als: HStR Bd. V/*Ossenbühl*).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Owen, Gareth/ Savage, Nick: The Tor Dark Net, Global Commission on Internet Governance, Paper Series No. 20, 2015, S. 1–9, abrufbar unter: https://www.cigionline.org/sites/default/files/no20_0.pdf (letzter Abruf: 20. Dezember 2021).

Paal, Boris P./ Pauly, Daniel A. (Hrsg.): Beck'sche Kompakt-Kommentare Datenschutzgrundverordnung, 3. Auflage, München 2021 (zitiert als Paal-Pauly/*Bearbeiter*).

Park, Tido, Durchsuchung und Beschlagnahme, 4. Auflage, München 2018.

Pesch, Paulina/ Böhme, Rainer: Datenschutz trotz öffentlicher Blockchain?, Datenschutz und Datensicherheit, S. 93–98.

Peitz, Carlo: Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, Wiesbaden 2020.

Petri, Thomas: Auskunftsverlangen nach § 161 StPO gegenüber Privaten – eine verdeckte Rasterfahndung?, Der Strafverteidiger 2007, S. 266–269.

Pham, Thai/ Lee, Steven, Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods, arXiv:1611.03941 [cs.LG] 2016, S. 1–5, abrufbar unter: https://arxiv.org/pdf/1611.03941v2.pdf (letzter Abruf: 20. Dezember 2021).

Recca, Angelo/ Ricli, Rosario/ Anghelin, Lulian/ Farruggio, Salvatore: The first decentralized music streaming platform a new era in music streaming, Stand: 2017, abrufbar unter: https://drive.google.com/file/d/10wXsS-6fAJ0EomzdqdcFt4iwLPE1F9t-/view (letzter Abruf: 20. Dezember 2021).

Reid, Fergal/ Harrigan, Martin: An analysis of anonymity in the bitcoin system, in: *Altshuler, Yaniv/ Elovici, Yuval/ Cremers, Armin B./ Aharony, Nadav/ Pentland, Alex* (Hrsg.), Security and Privacy in Social Networks, New York 2013, S. 197–223, abrufbar unter: https://doi.org/10.1007/978-1-4614-4139-7_10 (letzter Abruf: 20. Dezember 2021).

Rogall, Klaus: Zum Einsatz Verdeckter Ermittler: BGH 7.3.1995 – 1 StR 685/94, Juristen-Zeitung 1996, S. 259–264.

Rosengarten, Carsten/ Römer, Sebastian: Der „virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards, Neue Juristische Wochenschrift 2012, S. 1764–1767.

Roßnagel, Alexander: Die neue Vorratsdatenspeicherung, Neue Juristische Wochenschrift 2016, S. 533–538.

Roxin, Claus: Zum Einschleichen polizeilicher Scheinaufkäufer in Privatwohnungen (BGH, StV 1997, 233 [455]), Der Strafverteidiger 1998, S. 43–45.

Rudolf, Walter: § 90 Recht auf informationelle Selbstbestimmung, in: *Merten, Detlef/ Papier, Hans-Jürgen* (Hrsg.): Handbuch der Grundrechte in Deutschland und Europa, Band III, 1. Auflage, Heidelberg 20011 (zitiert als: HGR Bd. IV/*Walter*).

Rücker, Daniel/ Kugler, Tobias (Hrsg.): New European General Data Protection Regulation, A Practitioners's Guide, 1. Auflage, München 2018 (zitiert als: Rücker-Kugler/ *Bearbeiter*).

Rückert, Christian: Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, Zeitschrift für die gesamte Strafrechtswissenschaft Band 129, 2017, S. 302–333.

Sachs, Michael (Hrsg.): Grundgesetz Kommentar, 9. Auflage, München 2021 (zitiert als: Sachs-GG/*Bearbeiter*).

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Safferling, Christoph/ Rückert: Christian, Telekommunikationsüberwachung bei Bitcoins, Multimedia und Recht 2015, S. 788–794.

Sattler, Andreas: Der Einfluss der Digitalisierung auf das Gesellschaftsrecht, Betriebs-Berater 2018, S. 2243–2253.

Satzger, Helmut/ Schluckebier, Wilhelm (Hrsg.): Satzger, Schluckebier, Widmaier Strafprozessordnung Mit GVG und EMRK Kommentar, 4. Auflage, Köln 2020 (zitiert als: SSW-StPO/*Bearbeiter*).

Schaefer, Torsten: Rasterfahndung „light" – Abfrage von Kreditkartendaten, NJW-Spezial 2009, S. 280.

Schmidt-Bleibtreu, /Hofmann/Henneke (Hrsg.): GG Grundgesetz, 15. Auflage, Köln 2022 (zitiert als: SHH-GG/*Bearbeiter*).

Schlund, Albert/ Pongratz, Hans: Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, Deutsches Steuerrecht 2018, S. 598–604.

Schmitt, Bertram/ Köhler, Marcus: Meyer-Goßner/Schmitt Strafprozessordnung, 64. Auflage, München 2021 (zitiert als Meyer-Goßner/Schmitt/*Bearbeiter*).

Schneider, Hartmut: Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz -, Neue Strafrechtszeitschrift 2004, S. 359–367.

Schrey, Joachim/ Thalhofer, Thomas: Rechtliche Aspekte der Blockchain, Neue Juristische Wochenschrift 2017, S. 1431–1436.

Schulz, Sönke/ Hoffmann, Christian: Staatliche Datenerhebung in sozialen Netzwerken, Datenschutz und Datensicherheit 2012, S. 7–13.

Schuster, Fabian: E-Mail-Dienste als Telekommunikationsdienste?, Computer und Recht 2016, S. 173–185.

Shahid, Abdur/ Pissinou, Niki/ Njilla, Laurent/ Alemany, Sheila/ Imteaj, Ahmed/ Makki, Kia/ Aguilar, Edwin: Quantifying Location Privacy in Permissioned Blockchain-Based Internet of Things, MobiQuitous '19: Proceedings of 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2019, S. 116–125, abrufbar unter: https://doi.org/10.1145/3360774.3360800 (letzter Abruf: 20. Dezember 2021).

Siebrecht, Michael: Rasterfahndung, Eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, Berlin 1997.

Simitis, Spiros/ Hornung, Gerrit/ Spiecker genannt Döhmann, Indra (Hrsg.): Datenschutzrecht, 1. Auflage, Baden-Baden 2019 (zitiert als: Simitis-Hornung-Spieker/*Bearbeiter*).

Simmchen, Christoph: Blockchain (R)Evolution, Verwendungsmöglichkeiten und Risiken, Multimedia und Recht 2017, S. 162–165.

Singelnstein, Tobias: Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, Neue Strafrechtszeitschrift 2018, S. 1–15.

Singelnstein, Tobias: Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Datenverarbeitung & Co, Neue Strafrechtszeitschrift 2012, S. 593–606.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Singelnstein, Tobias/ Derin, Benjamin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens Was aus der StPO-Reform geworden ist, Neue Juristische Wochenschrift 2017, S. 2646–2652.

Stoffer, Hannah: Wie viel Privatisierung „verträgt" das strafprozessuale Ermittlungsverfahren?, Eine Untersuchung zur Zulässigkeit privater Beweisbeschaffung und zur Verwertbarkeit auf diese Weise erlangter Beweismittel im Strafverfahren, Tübingen 2016.

Soiné, Michael: Kriminalistische List im Ermittlungsverfahren, Neue Strafrechtszeitschrift 2010, S. 596–602.

Soiné, Michael: Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, Neue Strafrechtszeitschrift 2014, S. 248–251.

Specht, Louisa/ Mantz, Reto (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht, Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, 1. Auflage, München 2019 (zitiert als: Specht/Mantz-HdB DSR/*Bearbeiter*).

Spindler, Gerald: Gesellschaftsrecht und Digitalisierung, Zeitschrift für Gesellschaftsrecht 2018, S. 17–55.

Spindler, Gerald/ Bille, Martin: Rechtsprobleme von Bitcoin als virtuelle Währung, Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen, S. 1357–1369.

Stern, Klaus (Hrsg.): Staatsrecht: Die einzelnen Grundrechte Bd. IV/1, 1. Auflage, München 2006 (zitiert als Stern/*Bearbeiter,* Staatsrecht: Die einzelnen Grundrechte Bd. IV/1).

Stern, Klaus/ Becker, Florian (Hrsg.): Grundrechte-Kommentar, 3. Auflage, Köln 2019 (zitiert als: Stern-Becker-GG/*Bearbeiter*).

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung Handkommentar, 2. Auflage, Baden-Baden 2018 (zitiert als: Sydow-DSGVO/*Bearbeiter*).

Tschorsch, Florian/ Scheuermann, Björn: Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys and Tutorials 2016, Vol. 18, S. 2084–2123, abrufbar unter: https://doi.org/10.1109/COMST.2016.2535718 (letzter Abruf: 20. Dezember 2021).

Von Heintschel-Heinegg, Bernd/ Bockemühl, Jan (Hrsg.): KMR – Kommentar zur Strafprozessordnung, Loseblattsammlung, Stand: 107. Ergänzungslieferung, Köln 2021 (zitiert als: KMR-StPO/Bearbeiter).

Vordermayer, Helmut/ von Heintschel-Heinegg, Bernd/ Schnabl, Robert (Hrsg.): Handbuch für den Staatsanwalt, 6. Auflage, Köln 2018 (zitiert als: Hdb-StA/*Bearbeiter*).

Voßkuhle, Andreas: Grundwissen – Öffentliches Recht: Der Grundsatz des Vorbehalts des Gesetzes*, Juristische Schulung 2007, S. 118–119.

Weisser, Niclas-Frederic: Zum Betretungsrecht von Wohnungen bzw. Hotelzimmern durch einen nicht offen ermittelnden Polizeibeamten (noeP), Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 2018, S. 59–63.

Wittig, Petra: Schleppnetzfahndung, Rasterfahndung und Datenabgleich, Juristische Schulung 1997, S. 961–970.

Wittmer, Sandra/ Steinebach, Martin: Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet Rechtliche Rahmenbedingungen und technische Umsetzbarkeit, Multimedia und Recht 2019, S. 650–653.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Wolter, Jürgen (Hrsg.): Systematischer Kommentar zur Strafprozessordnung, Mit GVG und EMRK, 5. Auflage, Köln 2016 (zitiert als: SK-StPO/*Bearbeiter*).

Ziemann, Sascha: Strafprozessualer Eingriff und Gesetzesbindung, Ein Beitrag zur Lehre von der Annexkompetenz im Strafverfahren, Zeitschrift für die gesamte Strafrechtswissenschaft Band 130, 2018, S. 762–803.

Zola, Francesco/ Eguimendia, Maria/ Bruse, Jan Lukas/ Urrutia, Raul Orduna: Cascading Machine Learning to Attack Bitcoin Anonymity, arXiv:1910.06560 [cs.CR] 2019, S. 1–15, abrufbar unter: https://arxiv.org/abs/1910.06560v1 (letzter Abruf: 20. Dezember 2021).

Zöller, Mark Alexander: Heimliche und verdeckte Ermittlungsmaßnahmen im Strafverfahren, Zeitschrift für die gesamte Strafrechtswissenschaft Band 124, 2012, S. 411–439.

Zöller, Mark Alexander: Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Zur Vernetzung von Strafverfolgung Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, Heidelberg 2002.

https://doi.org/10.5771/9783748941248, am 15.10.2024, 11:09:36
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb