CHRISTIAN RÜCKERT

# Digitale Daten als Beweismittel im Strafverfahren

*Jus Poenale*
*24*

Mohr Siebeck

JUS POENALE

Beiträge zum Strafrecht

Band 24

Christian Rückert

# Digitale Daten als Beweismittel im Strafverfahren

Mohr Siebeck

*Christian Rückert*, geboren 1986; Studium der Rechtswissenschaft an der Universität Erlangen-Nürnberg; Wissenschaftlicher Mitarbeiter an den Universitäten Erlangen-Nürnberg, Marburg und dem Karlsruher Institut für Technologie; 2011 Erstes Juristisches Staatsexamen; Rechtsreferendariat im Oberlandesgerichtsbezirk Nürnberg; 2013 Zweites Juristisches Staatsexamen; 2017 Promotion; Akademischer Rat a. Z. an der Universität Erlangen-Nürnberg; Post-Doc im DFG-Graduiertenkolleg „Cyberkriminalität und Forensische Informatik"; 2022 Habilitation; Lehrstuhlvertretung der Professur für Deutsches, Europäisches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht an der Universität Mannheim; Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und IT-Strafrecht an der Universität Bayreuth.

Die Veröffentlichung dieser Habilitationsschrift wurde finanziell gefördert durch das DFG Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik.

ISBN 978-3-16-162216-8 / eISBN 978-3-16-162217-5
DOI 10.1628/978-3-16-162217-5

ISSN 2198-6975 / eISSN 2568-8499 (Jus Poenale)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.



Das Buch wurde von Gulde Druck in Tübingen aus der Stempel Garamond gesetzt und auf alterungsbeständiges Werkdruckpapier gedruckt. Es wurde von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

# Vorwort

Die vorliegende Arbeit wurde im Mai/Juni 2022 als habilitationswürdige Leistung vom Fachbereich Rechtswissenschaft der Rechts- und Wirtschaftswissenschaftlichen Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg anerkannt. Für die Drucklegung konnten Rechtsänderungen, Rechtsprechung und Literatur bis Anfang Februar 2023 berücksichtigt werden. Angesichts der Länge des Werks und der daraus resultierenden Überarbeitungsdauer des Manuskripts wurden bei einigen nur online und periodisch erscheinenden Werken Ergänzungslieferungen und Neuauflagen nur bis Ende 2022 berücksichtigt. Details lassen sich dem Literaturverzeichnis entnehmen. Kolleg*innen, deren einschlägige Veröffentlichungen erst nach diesen Zeitpunkten erschienen sind oder aktualisiert wurden, mögen mir dies nachsehen.

"The whole concept of the self-made man or woman is a myth" (Arnold Schwarzenegger).

In diesem Sinne bin ich so vielen Menschen zu Dank verpflichtet. Nennen kann ich hier leider nur ein paar wenige. Dank gilt zunächst meinen akademischen Lehrern, Mentoren und Förderern Christoph Safferling, Hans Kudlich, Felix Freiling und Rainer Böhme sowie meinem „Entdecker" Matthias Jahn und dem „Retter" meiner akademischen Karriere Georg Caspers. Besonders hervorheben möchte ich Mustafa Oglakcioglu, den ich im wahrsten Sinne des Wortes als meinen Bruder im Geiste betrachte. Mustafa hat mich nicht nur gefördert und unterstützt, als guter Freund hat er auch großen Anteil daran, dass ich nicht zwischendurch die Flinte ins Korn geworfen habe. Dank gilt außerdem Gabriele Kett-Straub und Tobias Singelnstein für die äußerst zügige Erstellung der weiteren Habilitationsgutachten sowie meinem Onkel, Horst Rückert, für seinen unermüdlichen Einsatz bei den orthographischen Korrekturen dieser Arbeit.

Großen Einfluss auf die Forschung, die diesem Buch zugrunde liegt, hatten außerdem alle Mitglieder des DFG-Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik, allen voran meine Mitstreiter*innen aus der AG StPO und IT-Forensik, Janine Schneider, Nicole Scheler, Dominic Deuber, Florian Nicolai, Benedikt Lorch, Jens Trautmann und Jenny Ottmann. Dankbar bin ich auch für wertvollen Input aus der Praxis der Strafverfolgung und Strafverteidigung. Hervorheben möchte ich hier vor allem die vertrauensvolle Zusammenarbeit mit der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, namentlich vertreten durch Thomas Goger, dessen scharfsinnige Argumente aus unseren Diskussionen häufig Eingang in meine eigenen Überlegungen gefunden haben.

Besonderer Dank gilt der Deutschen Forschungsgemeinschaft (DFG), die im Rahmen ihres Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik sowohl die Erstellung als auch die Veröffentlichung dieser Arbeit – insbesondere auch als Open Access-Veröffentlichung – so großzügig gefördert und damit ermöglicht hat.

Für die Erhaltung meiner mentalen und emotionalen Stabilität während der Habilitationszeit, aber auch darüber hinaus, bedanke ich mich schließlich bei meiner Frau, meinen Eltern und meinen Freunden am Eisen und am Spielbrett.

Widmen möchte ich diese Arbeit meinem Sohn, der mich täglich daran erinnert, dass unsere Welt voller Wunder steckt, die es zu entdecken gilt.

Bayreuth, im Oktober 2023 Christian Rückert

# Inhaltsübersicht

# Inhaltsverzeichnis

Kapitel 1

# Die Erhebung und Verwertung digitaler Beweismitteldaten als Herausforderung für das Strafverfahrensrecht

Die Digitalisierung hat – das kann man ohne Zweifel behaupten – mittlerweile alle Lebensbereiche der Menschen erfasst und verändert. Die Geschwindigkeit der Entwicklung von Datenverarbeitungs- und Datenübertragungstechnologie ist beeindruckend. „Neue" Technologien können innerhalb weniger Jahre wieder veraltet, aus der Mode gekommen oder technisch erneut vollkommen umgestaltet sein. Dies betrifft nicht nur Hardwarekomponenten wie Prozessoren, Bildschirmtechnologien oder Übertragungsleitungen, sondern auch ganze Technologiekonzepte. So hat sich die Nutzung des Internets innerhalb relativ kurzer Zeit von einer reinen Kommunikationsinfrastruktur über die bloße Rezeption von Informationen von Internetseiten und Newslettern zu einer umfassenden Parallelrealität mit Teilhabe und Teilnahmemöglichkeiten für (fast) jedermann entwickelt (sog. user generated content oder Web 2.0).

Disruptive Technologien und Konzepte wie Suchmaschinen, Smartphones, soziale Medien, Machine Learning bzw. sog. künstliche Intelligenz (KI) und das sog. Internet of Things (IoT) bringen vollkommen neue Geschäftsmodelle hervor und verändern das Arbeits- und Freizeitleben von (fast) allen Menschen. Auch Kriminelle machen sich die neuen Technologien zunutze, um Straftaten zu begehen. Teilweise werden neue digitale Technologien lediglich als Werkzeuge genutzt, um bekannte Straftaten „effektiver" zu begehen, z. B. die Nutzung moderner Telekommunikations- und Verschlüsselungstechnologie durch die Organisierte Kriminalität zur Abwicklung von Geschäften in der „Realwelt".[1] In anderen Fällen ermöglicht die neue Technik die Begehung völlig neuer Arten von Straftaten oder zumindest die Neugestaltung der Begehungsweise von Straftaten. Besonders deutlich und prominent ist dies etwa beim Handel mit illegalen Gütern und Dienstleistungen im sog. Darknet[2] und der Verwendung von Kryptotrojanern zur Verschlüsselung von

---

[1] Siehe etwa zum sog. EncroChat-Verfahren: OLG Hamburg BeckRS 2021, 2226; OLG Schleswig NStZ 2021, 693; LG Berlin NStZ 2021, 696; KG MMR 2021, 917; *Singelnstein/Derin* NStZ 2021, 449.

[2] Umfassend hierzu *Wüst,* Die Underground Economy des Darknets – Die Strafbarkeit des Betreibens „illegaler" Handelsplattformen, Berlin 2022; siehe auch bereits *Bachmann/Arslan* NZWiSt 2019, 241; *Bäcker/Golla* VerfBlog, 2019/3/21; *Bartl/Moßbrucker/Rückert,* Angriff auf die Anonymität im Internet, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Dokumente/Internetfreiheit/20190630_Darknet_Paragraf_StN-Bartl-Mossbrucker-Rueckert.pdf; *Beck/Nussbaum* HRRS 2020, 112; *Ceffinato* JuS 2017, 403; *ders.* ZRP 2019, 161; *Gercke* ZUM

Daten und Kryptowährungen als Bezahlungsmittel bzw. als erpresstes Lösegeld in den sog. Ransomware-Fällen.[3]

Für die Strafverfolgung besonders misslich ist dabei der zunehmende Einsatz von Verschleierungs- und Anti-Forensik-Methoden durch Kriminelle, um einer Entdeckung oder zumindest einer Überführung zu entgehen. Neben moderner Verschlüsselungstechnologie sind hier auch Methoden der Identitätsverschleierung und gezielte Anti-Forensik-Maßnahmen, wie versteckte Speicherpartitionen oder automatische Datenvernichtung, zu nennen.

Die Durchdringung aller Lebensbereiche durch digitale Technologien erzeugt auf der anderen Seite eine nie zuvor dagewesene Menge an Informationen über die Aktivitäten und das Leben der Bürger*innen in digitaler Form. Die Daten entstehen – in vielen Fällen ohne „aktuelles" Bewusstsein der Nutzer*innen – durch die Nutzung digitaler Technologien und werden in vielen Fällen von den Anbieter*innen der jeweiligen Technologien (wie Telekommunikations- und Mediendienstanbietern, aber auch den Herstellern und Betreibern von IoT-Geräten) erhoben, verarbeitet, gespeichert und mit anderen Unternehmen geteilt. Doch auch die Bürger*innen selbst verarbeiten, speichern und teilen Daten über sich selbst und andere in digitalen Terminkalendern, Notizen, Social Media Accounts, elektronischen Dokumenten, Bildern, Videos und Aktivitätenprotokollen (z. B. mittels sog. Wearables wie Fitness Trackern und Navigationsgeräten). Dies führt zu einer riesigen Menge an (prinzipiell) verfügbaren Daten mit Informationen über zahlreiche Aktivitäten der Bürger*innen. Diese Daten sind in vielen Fällen von Interesse für die Strafverfolgungsbehörden und können zur Aufklärung von Straftaten beitragen. Die Datenmengen, die in einem Strafverfahren hierbei verfahrensrelevante Informationen enthalten können, sind mittlerweile oft so groß geworden, dass die Strafverfolgungsbehörden auf den Einsatz von moderner Datenerhebungs- und Datenverarbeitungstechnologie bis hin zu Machine Learning Tools und künstlicher Intelligenz angewiesen sind.

Die Bedeutung von digitalen Daten als Spurenansatz und Beweismittel im Strafverfahren hat aufgrund der oben genannten Phänomene bereit spürbar zugenommen, in den kommenden Jahren und Jahrzehnten wird sich kaum mehr ein (über Bagatelldelikte hinausgehendes) Strafverfahren finden lassen, in dem digitale Daten nicht in irgendeiner Weise – und sei es nur als erster Spurenansatz – zur Aufklärung beigetragen haben.[4] Dies gilt dabei nicht nur für die Delikte der sog. Cyberkrimi-

---

2019, 798; *Gerhold* ZRP 2021, 44; *Greco* ZIS 2019, 435; *Kubiciel,* Augsburger Papier zur Kriminalpolitik 1/2019*; Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1; *Kusche* JZ 2021, 27; *Oehmichen/Weißenberger* KriPoz 2019, 174; *Rückert* Politische Studien Bd. 69 (2018 Mai/Juni), 479, S. 12; *ders.* StV 2019, I; *ders.* LTO v. 15.03.2019; *Safferling/Rückert* Analysen & Argumente 291 (2018); *Zöller* LTO v. 11.03.2021; *ders.* KriPoz 2019, 274.

[3] *Europol* IOCTA 2021, S. 14 ff. und 20 ff.; *Beukelmann* NJW-Spezial 2017, 376; *Vogelsang/Möllers* jM 2016, 381; *Kreikemeyer* Kriminalistik 2018, 627; *Ceffinato* NZWiSt 2016, 464 (466 f.); *Herzog/Hoch* StV 2019, 412 (414); Überblick bei *Rückert* in Maume/Maute (Hrsg.), HdB Kryptowerte, § 20 Rn. 7 f.

[4] *Momsen/Hercher* Digitale Beweismittel im Strafprozess: Eignung, Gewinnung, Verwer-

nalität, sondern auch für Delikte der „Realwelt" und des täglichen Lebens. Einige Ermittlungsmaßnahmen, die digitale Daten erheben und verarbeiten, gehören mittlerweile zum „Standardrepertoire" der Strafverfolgungsbehörden. Hierzu zählen etwa Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO, die Abfrage von Verkehrs-, Bestands- und Nutzungsdaten nach §§ 100g, 100j, 100k StPO, der Einsatz des sog. IMSI-Catchers nach § 100i StPO und die Funkzellenabfrage nach § 100g Abs. 3 StPO. Es lassen sich darüber hinaus bereits jetzt spektakuläre Beispielsfälle nennen, in denen digitale Daten als Beweismittel in einem Strafverfahren wegen „Realwelt"-Delikten im Wege „kreativer" Datenerhebung und Datenverarbeitung herangezogen wurden: So wurde ein Ehemann in Griechenland des Mordes an seiner Ehefrau überführt, weil die Daten eines sog. Fitness Trackers den von ihm dargestellten Geschehensablauf widerlegten.[5] Das Landgericht Regensburg verurteilte unlängst einen Mann wegen Totschlags, dem es die Tötung aufgrund der Aufnahmen eines Sprach- und Heimassistenzsystems nachweisen konnte.[6] Mehrere Verfahren wegen Terrorismusstraftaten stützen sich auf die Auswertung von Chatdateien aus Messengerdiensten (wie etwa WhatsApp); teilweise wurden diese Daten im Wege des sog. Account-Clonings erlangt.[7]

Die Bedeutungszunahme von digitalen Daten als Spurenansatz und Beweismittel stellt das gesamte Strafverfahrensrecht vor neue Herausforderungen. Die oftmals für eine rein „analoge" Welt konzipierten Normen der StPO müssen auf „digitale" Sachverhalte angewendet werden. Besonders relevant erscheinen dabei zwei Problemkreise in unterschiedlichen Stadien des Strafverfahrens. Zum einen stellt sich die Frage, ob das strafprozessuale Instrumentarium der Ermittlungsbefugnisse zur Datenerhebung und Datenverarbeitung im Ermittlungsverfahren hinreichend ausgestaltet ist, um alle praxisrelevanten Arten der strafprozessualen Dateneingriffe zur Beweisdatengewinnung abzudecken und gleichzeitig die verfassungs- und europarechtlichen Grenzen einzuhalten. Zum anderen muss die Strafprozessordnung Lösungen für den Umgang mit digitalen Daten als Beweismittel in der Hauptverhandlung bereithalten. Digitale Daten weisen im Vergleich zu anderen Beweismitteln einige spezifische Besonderheiten – wie etwa ihre Flüchtigkeit und („spurenlose") Manipulierbarkeit – auf, die im Beweisrecht der Strafprozessordnung berücksichtigt werden müssen. Besondere Probleme stellen sich diesbezüglich auch hinsichtlich der Verwendung von Ergebnissen von komplexen Datenverarbeitungsvorgängen als Beweismittel. Soweit hierfür auf sog. statistische oder sogar selbstlernende Methoden der Datenverarbeitung („KI") zurückgegriffen wird, muss sich das Tatgericht mit der Zuverlässigkeit und Nachvollziehbarkeit dieser Methoden

---

tung, Revisibilität, Beitrag zum 37. Strafverteidigertag, Freiburg 2013, S. 173 (S. 175); *Momsen*, FS Beulke, S. 871 (873 ff.).

[5] https://www.stern.de/panorama/stern-crime/griechenland--smartwatch-enthuellt-luegen--ehemann-gesteht-mord-30577726.html (Stand: 29.12.2021).

[6] https://www.tagesschau.de/investigativ/wdr/ermittlungen-digitalisierung-101.html (Stand: 29.12.2021).

[7] Siehe hierzu BGH BeckRS 2019, 2677; BGH BeckRS 2020, 49703.

auseinandersetzen, wenn es deren Ergebnisse als Beweismittel verwenden will. Beiden Problemkreisen widmet sich die nachfolgende Untersuchung.

## I. Allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung

Wollen die Strafverfolgungsbehörden „vor der Lage bleiben" bzw. – wie es *Jürgen Gause* vor einigen Jahren auf dem Erlanger Cybercrime Tag ausgedrückt hat – „die Lage nicht vollständig aus dem Blick verlieren",[8] müssen sie sowohl Zugang zu den o.g. Datenbeständen erhalten als auch moderne Technologien zu deren Erhebung und Verwertung einsetzen.

Das Legalitätsprinzip (§ 152 Abs. 2 StPO) und die Aufklärungspflicht bzw. die Plicht zur Erforschung der materiellen Wahrheit (§ 244 Abs. 2 StPO), verfassungsrechtlich abgesichert durch den sog. staatlichen Straf(verfolgungs-)anspruch[9], geraten angesichts dieser Gemengelage in besonderem Maße in Konflikt mit dem Datenschutz und den Grund- und Menschenrechten, in denen dieser verankert ist (v. a. Art. 10 GG, Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie Recht auf informationelle Selbstbestimmung jeweils nach Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG; Art. 8 EMRK, Art. 7, 8 GRC). Die Auflösung dieses Spannungsfeldes bzw. der Ausgleich zwischen Grundrechtseingriff und staatlichem Strafverfolgungsanspruch obliegt nach der Konzeption des Verfassungsrechts (Vorbehalt des Gesetzes und Wesentlichkeitsvorbehalt)[10] vorrangig dem Gesetzgeber. Er muss die notwendigen Eingriffsbefugnisse für Grundrechtseingriffe durch Datenerhebungen- und -verarbeitungen schaffen und ausgestalten.

### *1. Mangel an gesetzlichen Dateneingriffsbefugnissen*

#### *a) Zu eng und zu spät geregelte Eingriffsbefugnisse*

Dieser Verpflichtung kommt der Gesetzgeber im Bereich strafprozessualer Dateneingriffe nur bedingt nach. Zwar existieren mit den §§ 100a – 101b StPO zahlreiche und überaus detaillierte Regelungen für die Erhebung verschiedener Datenarten. Einerseits sind diese Regelungen jedoch (auch um dem Grundsatz der Normenklarheit und Bestimmtheit Rechnung zu tragen) teilweise auf erstaunlich eng gefasste Fallkonstellationen zugeschnitten. Zu nennen sind hier beispielhaft die §§ 100a Abs. 1 S. 2, S. 3, 100b StPO, welche ausschließlich den Eingriff in informa-

[8] Vgl. *Rückert/Wüst* KriPoz 2018, 247 (249 ff.).

[9] BGHSt 52, 110 = NStZ 2008, 356; BGH NJW 2013, 1827 (1830); Meyer-Goßner/*Schmitt* Einl. Rn. 55a; *Paul* NStZ 2013, 489 (491).

[10] BVerfGE 49, 89 (126 f.); 98, 128 (251); guter Überblick bei v. Münch/Kunig/*Kotzur* Art. 20 Rn. 156 ff. mwN.

tionstechnische Systeme regeln, die in der Praxis seit ihrer Einführung 2017 so gut wie keine Rolle spielen,[11] § 100i StPO, der – bis zur allerdings verfassungsrechtlich zweifelhaften Ausdehnung des Anwendungsbereichs der Vorschrift durch den BGH[12] auf die Versendung der Stillen SMS – nahezu ausschließlich den Einsatz des sog. IMSI Catchers regelt(e) und die §§ 100g, 100j und 100k StPO, welche jeweils die Erhebung ganz bestimmter Arten von Daten, die von ganz bestimmten Dienstleistern erhoben werden, regeln. Andererseits sind durch technologische Entwicklungen entstandene und teilweise äußerst praxisrelevante Konstellationen nicht, unzureichend oder in verfassungswidriger Weise geregelt. So hat es der Gesetzgeber über Jahrzehnte hinweg (die erste E-Mail der Welt wurde 1971 versendet,[13] die erste Mail in Deutschland 1984[14]) Rechtsprechung und Wissenschaft überlassen, eine Rechtsgrundlage für die Erhebung des lange Zeit wichtigsten elektronischen Kommunikationsmediums zu „finden".[15] In der vor Kurzem erfolgten „Neuregelung" (in der Sache handelt es sich um eine Verfahrensregelung, welche die Zurückstellung von Benachrichtigungen betrifft) u. a. der „heimlichen E-Mail-Beschlagnahme" in § 95a StPO wird die in der Wissenschaft über die richtige Rechtsgrundlage geführte Debatte vollständig ignoriert und eine verfassungswidrige Regelung geschaffen (die Regelung erfüllt nicht die Anforderungen des BVerfG an heimliche Eingriffe in das Telekommunikationsgeheimnis und das IT-System-Grundrecht).[16]

Auch der praktisch bedeutsame Bereich der Erhebung von sog. Nutzungsdaten iSv § 2 Abs. 2 Nr. 3 TTDSG war bis vor Kurzem nicht geregelt, obwohl die Abfrage der Nutzungsdaten von Telemediendienstanbietern bereits seit Jahren vielfach durchgeführt wird. In der Praxis wurde sich mit der Anwendung von §§ 161, 163 StPO geholfen,[17] was allerdings angesichts der in vielen Fällen bestehenden sachlichen Nähe von Nutzungs- zu Inhalts- und Verkehrsdaten (§§ 100a, 100b, 100g StPO) mehr als nur zweifelhaft war: In der Regel handelt es sich nicht um einen nur „geringfügigen" Grundrechtseingriff, wie es für die Anwendung der Ermittlungsgeneralklauseln jedoch notwendig ist.[18] Besonders kurios ist in der Konstellation der Nutzungsdatenabfrage, dass während der langen Zeit der „Nichtregulierung"

---

[11] Bundesamt für Justiz, Übersichten für 2019 Telekommunikationsüberwachung – Anordnungen nach § 100a StPO (korrigierte Fassung), Stand 12.02.2021 und Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung für 2019 (Maßnahmen nach § 100b StPO), korrigierte Fassung, Stand: 19.02.2021.

[12] BGH NStZ 2018, 611 mit ablehnender Anmerkung *Rückert*.

[13] https://thenextweb.com/news/the-first-email-was-sent-40-years-ago-this-month (Stand: 12.07.2021).

[14] https://web.archive.org/web/20110605072324/; http://www.tagesschau.de/inland/email102.html (Stand: 12.07.2021).

[15] Siehe etwa die „Leitentscheidung" des BVerfG in NJW 2009, 2431; Überblick über den Meinungsstand der Literatur bei MüKoStPO/*Rückert* § 100a Rn. 96 ff.

[16] Siehe hierzu MüKoStPO/*Rückert* § 100a Rn. 104.

[17] KMR/*Bär* § 100g Rn. 68; *Eckel/Rottmeier* NStZ 2021, 1 (9); zuneigend KK/*Bruns,* 8. Auflage, § 100g Rn. 3; siehe auch BT Drs. 19/17741, 38.

[18] *Karg* DuD 2015, 85 (88); *Warken* NZWiSt 2017, 329 (337); *Bauer,* Soziale Netzwerke und strafprozessuale Ermittlungen, S. 358 f.; MüKoStPO/*Rückert* § 100k Rn. 2.

dieser Maßnahme eine größere praktische Bedeutung zukam, als er in Zukunft der nun geschaffenen Regelung in § 100k StPO zukommen wird. Vor der Änderung des TMG, der Einführung des TTDSG und der Reform des TKG in Umsetzung der Richtlinie 2018/1972/EU zum 1. Dezember 2021 war die Gruppe der Dienstleister, welche Nutzungsdaten (damals noch nach § 15 TMG aF) verarbeitete, viel größer und praktisch bedeutsamer als nach der Reform. Dies betraf vor allem sog. Over-the-top-Dienstleister (OTT), welche zwar Kommunikationsdienste im weiteren Sinne erbrachten, wie z. B. Webmail-Provider, Voice-over-IP-Dienste und Messengerdienste, aber keine Telekommunikationsdienstleister nach § 3 Nr. 24 TKG aF und damit Telemediendienste iSv § 1 TMG waren. Nach der Reform des TKG fallen diese OTT-Dienstleister nun als sog. interpersonelle Telekommunikationsdienste in den Anwendungsbereich des Telekommunikationsrechts gem. § 3 Nr. 61, Nr. 24 TKG und verarbeiten damit keine Nutzungsdaten mehr, sondern jetzt Verkehrsdaten iSv §§ 9, 12 TTDSG. Der Gesetzgeber hat also pünktlich zur Abnahme der praktischen Bedeutung der Nutzungsdatenabfrage eine – im Detail auch verfassungsrechtlich problematische[19] – Befugnisnorm eingeführt.

### *b) Praktisch bedeutsame, aber ungeregelte Dateneingriffe*

Daneben gibt es zahlreiche Beispiele für bereits von Strafverfolgungsbehörden eingesetzte Ermittlungsmethoden zur Datenerhebung, welche keine eigenständige Regelung in der StPO erfahren haben, obwohl es sich teilweise um erhebliche Grundrechtseingriffe handelt. Hier bemühen sich die Strafverfolgungsbehörden, die Gerichte, soweit sie überhaupt mit diesen Fragen befasst werden, und (allerdings mit bislang zu wenig Beachtung) die Strafrechtswissenschaft darum, eine geeignete Rechtsgrundlage in den Vorschriften der Strafprozessordnung zu finden. Beispielhaft zu nennen sind hier etwa das IP-Catching,[20] das IP-Tracking,[21] das WLAN-Catching,[22] die sog. Stille SMS,[23] die Erhebung von Daten aus Cloud-Servern[24] und die Erhebung von Daten aus IoT-Geräten[25] (v. a. aus Heimassistenzsys-

---

[19] Details bei MüKoStPO/*Rückert* § 100k Rn. 5 f.

[20] BeckOK StPO/*Bär* § 100g Rn. 26; *Bär* NZWiSt 2017, 81 (84); KK/*Henrichs/Weingast* § 100g Rn. 20; *von der Grün,* Verdeckte Ermittlungen S. 76 f.; MüKoStPO/*Rückert* § 100g Rn. 127 ff.

[21] BGH wistra 2015, 395; zustimmend Meyer-Goßner/Schmitt/*Köhler* § 100g Rn. 45; Löwe/Rosenberg/*Hauck* § 100g Rn. 41; HeiKo/*Gercke* § 100g Rn. 13 aE; *Warken* NZWiSt 2017, 329 (336); *Krause* NStZ 2016, 139; BeckOK StPO/*Bär* § 100g Rn. 24 f.; *Bär* NZWiSt 2017, 81 (84); *Ceffinato* JuS 2019, 337 (342); wohl auch BeckOK StPO/*Graf* § 100a Rn. 253; MüKoStPO/*Rückert* § 100g Rn. 124 ff.

[22] *Ulbrich,* Die Überwachung lokaler Funknetzwerke („WLAN-Catching"), S. 226 ff.; MüKoStPO/*Rückert* § 100b Rn. 25 ff.

[23] BGH NStZ 2018, 611; *Krüger* ZJS 2012, 606 (609) mN; *Rückert* NStZ 2018, 613; SK-StPO/*Wolter/Greco* § 100h Rn. 29; *Eisenberg/Singelnstein* NStZ 2005, 62.

[24] *Grözinger,* Die Überwachung von Cloud-Storage, S. 157 ff.; *ders.* StV 2019, 406; MüKoStPO/*Rückert* § 100b Rn. 33 ff.

[25] *Janovsky/Goger* RAW 2019, 99 (101 f.); *Marosi/Skobel* DÖV 2018, 837 (843 f.); *Warken* NZWiSt 2017, 329 (335); *Heinrich* ZIS 2020, 421 (422); MüKoStPO/*Rückert* § 100a Rn. 131 f.

temen). Auch im Bereich der Massendatenerhebung und -auswertung ist keine nennenswerte Tätigkeit des Gesetzgebers zu beobachten, obwohl OSINT und Data Mining (auch unter Einsatz von Machine Learning Tools und künstlicher Intelligenz) mehr und mehr Einzug in die tägliche Ermittlungsarbeit nehmen[26] und das BVerfG vor Kurzem die besondere Eingriffsintensität von Data Mining-Methoden festgestellt hat.[27]

*c) „Kreative" Rechtsauslegung vor den Schranken des Grundgesetzes*

Der Gesetzgeber – so kann ein Zwischenfazit lauten – tut jedenfalls bislang wenig, um strafprozessual „vor die Lage" zu kommen. Freilich wird es niemals möglich sein, angesichts der langsamen Prozesse demokratischer Gesetzgebung mit der rasanten technischen Entwicklung mitzuhalten. Ob dies jedoch jahrzehntelange Nichtregulierung von Standardmaßnahmen rechtfertigt, steht auf einem anderen Blatt. Die strafprozessuale Praxis weiß sich aufgrund dieser gesetzgeberischen Untätigkeit nicht anders zu helfen, als die von ihr als notwendig empfundenen Ermittlungsmethoden mehr oder weniger „gewaltsam" unter die in der StPO regulierten Eingriffsbefugnisse zu subsumieren. Nicht selten gerät sie dabei mit dem Wesentlichkeitsvorbehalt, den Grundsätzen der Normenklarheit und Bestimmtheit und/oder der Verhältnismäßigkeit in Konflikt. Ein Beispiel hierfür ist die Subsumtion des Versandes einer sog. Stillen SMS unter § 100i StPO, obwohl der Gesetzgeber selbst davon ausging, dass mit Schaffung des „neuen" § 100g StPO der Versand Stiller SMS nicht mehr notwendig sein würde[28] und die Bundesregierung auf Anfrage §§ 100a, 100b (aF) und 100g StPO als Rechtsgrundlage für die Datenerhebung und §§ 161, 163 StPO als Grundlage für die Versendung nannte.[29] Ähnlich verhält es sich beim zweiten Beispiel, der Anwendung der §§ 161, 163 StPO als Grundlage der Nutzungsdatenerhebung bei Telemediendiensten[30] bis zur Neuregelung in § 100k StPO (siehe hierzu bereits oben). Aufgrund der Vergleichbarkeit von Nutzungsdaten mit Verkehrsdaten und – teilweise – sogar Inhaltsdaten (z. B. konkret aufgerufene URLs, Eingaben in Formularen und Suchmaschinen), kam eine Anwendung der Ermittlungsgeneralklauseln nie in Betracht – die wesentliche Frage, ob und unter welchen Voraussetzungen mittels einer Nutzungsdatenauskunft in Art. 10 Abs. 1 GG eingegriffen werden darf (siehe zur Frage, welches Grundrecht bei Nutzungsdatenabfragen betroffen ist, noch ausführlich Kapitel 2, III. 1. c) dd), S. 54), musste vom Gesetzgeber beantwortet werden (was nunmehr in § 100k StPO geschehen ist).[31] Beim heimlichen Zugriff auf LAN- und WLAN-

[26] Meyer-Goßner/Schmitt/*Köhler* § 163 Rn. 28a; *Rückert* ZStW 129 (2017), 302 ff.
[27] BVerfG NVwZ 2021, 226 (233 Rn. 109).
[28] BT-Drs. 16/5846, 51.
[29] BT-Drs. 17/8544, 17.
[30] KMR/*Bär* § 100g Rn. 68; *Eckel/Rottmeier* NStZ 2021, 1 (9); zuneigend KK/*Bruns,* 8. Auflage, § 100g Rn. 3.
[31] *Karg* DuD 2015, 85 (88); *Warken* NZWiSt 2017, 329 (337); *Bauer,* Soziale Netzwerke und strafprozessuale Ermittlungen, S. 358 f.; MüKoStPO/*Rückert* § 100k Rn. 2.

Netzwerke (sog. WLAN-Catching) sorgt die vom Gesetzgeber den Gerichten und der Wissenschaft überlassene Ausfüllung des Begriffs der „Telekommunikation" (§ 100a StPO) und des „informationstechnischen Systems" für Schwierigkeiten. Wer einen rein technischen Telekommunikationsbegriff zugrunde legt, gelangt hier leicht zu einer Anwendung von § 100a StPO für das heimliche Mitschneiden des Netzwerkverkehrs,[32] während andere – unter Verwendung eines an Art. 10 GG angelehnten Telekommunikationsbegriffs – danach differenzieren, ob „nach außen gehender" Netzwerkverkehr oder Netzwerkverkehr von Nutzer*innen, die nicht gleichzeitig Betreiber*innen des Netzwerks sind, überwacht wird (dann § 100a StPO), während im Übrigen (also bei Überwachung des netzwerkinternen Datenverkehrs des Betreibers des Netzwerks) § 100b StPO zur Anwendung gelangt.[33] Beim Einsatz virtueller verdeckter Ermittler im Internet ist zwar richtigerweise davon auszugehen, dass dieser ebenfalls nach den §§ 110a ff. StPO zulässig ist, weil dies sowohl vom Wortlaut der Vorschrift gedeckt ist als auch die sich grundsätzlich stellenden grundrechtlichen Fragen nicht „wesentlich" anders sind als beim Einsatz in der Realwelt.[34] Allerdings ist unklar, wie im virtuellen Raum „echte" verdeckte Ermittler von nicht öffentlich ermittelnden Polizeibeamten (noePs) abgegrenzt werden müssen. Auch hier kommt es maßgeblich auf die Intensität des Grundrechtseingriffs an, weil die §§ 161, 163 StPO (Einsatz von noePs) nur zu geringfügigen Grundrechtseingriffen berechtigen.[35] Bislang nicht in der StPO vorgesehen ist dagegen die Übernahme von „beschlagnahmten" Accounts von Tatverdächtigen, um so deren digitale Identität zu übernehmen. Da es sich hierbei um eine wesentlich andere Eingriffsart handelt (Verwendung einer fremden Identität gegen den Willen des Identitätsinhabers statt Verwendung einer erfundenen Identität) muss hierfür eine neue gesetzliche Grundlage geschaffen werden. Ein im IT-Sicherheitsgesetz 2.0-Entwurf (§ 163g StPO-Entwurf) vorgesehener Vorschlag wurde bislang vom Bundestag nicht wieder aufgegriffen.[36] Im Rahmen der Anwendung von § 100a StPO ist zwar die Anwendung auf zahlreiche „neue" Wege der Datenübertragung vom Wortlaut („Telekommunikation") gedeckt, allerdings stellt sich nicht selten die Frage, ob die Eingriffsschwellen und Schutzmechanismen der §§ 100a, 100d, 100e StPO angesichts der Informationstiefe und -vielfalt, welche sich aus der Erhebung der entsprechenden übertragenen (oder im Fall des Zugriffs auf Webmail-Provider und andere Cloud-Services: zwischenzeitlich ruhenden) Daten ergeben können, ausreichend sind. Mit anderen Worten: Ob die konkrete Anwendung im Einzelfall dem Grundsatz der Verhältnismäßigkeit genügt. Dies betrifft beispielsweise die Überwachung des vollständigen Internetverkehrs (inklusive des

[32] *Ulbrich,* Die Überwachung lokaler Funknetzwerke („WLAN-Catching"), S. 226 ff.; *Kleih,* Die strafprozessuale Überwachung der Telekommunikation, S. 115 ff.

[33] Für Details hierzu siehe MüKoStPO/*Rückert* § 100b Rn. 25 ff.

[34] *Rückert* in Maume/Maute (Hrsg.), HdB Kryptowerte, § 23 Rn. 15 ff.

[35] Siehe hierzu *Rückert* in Maume/Maute (Hrsg.), HdB Kryptowerte, § 23 Rn. 18 ff.

[36] https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (Stand: 14.07.2021).

Surfverhaltens),[37] den heimlichen Zugriff auf vollständige E-Mail-Postfächer bei Webmail-Providern,[38] den Zugriff auf Cloud-Server[39] (soweit hier nicht – richtigerweise – die Anwendung von § 100b StPO bevorzugt wird[40]) und den Datenverkehr von IoT-Geräten wie Heimassistenz-Systemen.[41] Ein letztes Beispiel, das hier detaillierter dargestellt werden soll (es lassen sich zahlreiche weitere Beispiele finden, um das Problem zu illustrieren genügen jedoch mE die hier genannten), betrifft das sog. IP-Catching, bei dem die Ermittlungsbehörden durch technische Maßnahmen (mit oder ohne Kooperation des Betreibers) die IP-Adressen der Nutzer*innen bestimmter Internetdienstleistungen über einen begrenzten Zeitraum hinweg erheben bzw. protokollieren (in letzter Zeit medial und im politischen Diskurs auch gelegentlich als „Login-Falle" bezeichnet). Im Regelfall wird im Anschluss eine Bestandsdatenabfrage bei Telekommunikationsdienstleistern nach § 100j StPO durchgeführt, um die Identitäten der Nutzer*innen zu ermitteln.[42] Unabhängig davon, ob die Rechtsgrundlage für eine solche Maßnahme stets in § 100g StPO[43] zu sehen ist oder danach differenziert wird, bei welchem Internetdienstleister (Telekommunikationsdienstleister iSd TKG, dann § 100g StPO, oder Telemediendienstleister iSd TMG, dann § 100k StPO) die Maßnahme durchgeführt wird,[44] weist das IP-Catching jedenfalls eine sehr große Streubreite auf, da eine Vielzahl von IP-Adressen und damit eine große Menge personenbezogener Daten einer Vielzahl von Nutzer*innen erhoben werden. Die Maßnahme steht damit in sachlicher Nähe zu einer Funkzellenerhebung nach § 100g Abs. 3 StPO. Letztere Vorschrift wird wegen der großen Grundrechtsintensität von der Instanzrechtsprechung eng ausgelegt[45] und enthält zu Recht strengere Eingriffsschwellen im Vergleich zu § 100g Abs. 1, Abs. 2 und § 100k StPO (wenn auch wohl nicht streng genug[46]). Da § 100g Abs. 3 StPO jedoch eine analogiefeindliche Spezialnorm für Funkzellenabfragen ist, wird von der Literatur eine Anwendung auf das IP-Catching abgelehnt;[47] wie der *Verfasser* an anderer Stelle dargelegt hat, müssen jedoch Verhältnismäßigkeit und Maßnahmerichtung aufgrund der sachlichen Nähe

---

[37] BVerfG ZD 2017, 132; so nun auch BGHSt 62, 22 = NJW 2017, 2631; ausführlich *Hiéramente* HRRS 2016, 448; aA *Heinrich* ZIS 2020, 421 (422 ff.).

[38] BGH BeckRS 2020, 36910; Überblick über den Meinungs- und Streitstand bei MüKoStPO/*Rückert* § 100a Rn. 96 ff.

[39] Löwe/Rosenberg/*Hauck* § 100a Rn. 85; *Bär* MMR 2013, 700 (703); siehe auch *Kudlich* GA 2011, 193 (207 f.).

[40] Ausführliche Begründung bei MüKoStPO/*Rückert* § 100b Rn. 33.

[41] *Marosi/Skobel* DÖV 2018, 837 (843 f.); offengelassen von *Warken* NZWiSt 2017, 329 (335); aA *Heinrich* ZIS 2020, 421 (422).

[42] Weitere Details zur technischen Durchführung der Maßnahme bei BeckOK StPO/*Bär* § 100g Rn. 26; KMR/*Bär* § 100g Rn. 66; MüKoStPO/*Rückert* § 100g Rn. 127.

[43] So BeckOK StPO/*Bär* § 100g Rn. 26; *Bär* NZWiSt 2017, 81 (84); KK/*Henrichs/Weingast* § 100g Rn. 20.

[44] Details und Begründung bei MüKoStPO/*Rückert* § 100g Rn. 128 ff.

[45] AG Dortmund 06.01.2016 – 701 Gs 18/16, juris; LG Dortmund 23.02.2016 – 36 Qs-121 UJs 60/16-25/16, juris; siehe auch LG Arnsberg 29.04.2019 – 2 Qs – 410 UJs 254/19 – 43/19, juris.

[46] Zu diesem Problem, vgl. MüKoStPO/*Rückert* § 100g Rn. 87.

[47] BeckOK StPO/*Bär* § 100g Rn. 26.

zur Funkzellenabfrage besonders streng geprüft werden.[48] Die Anwendung von §§ 100g, 100k StPO steht vor diesem Hintergrund jedenfalls aber auf sehr wackligen Füßen, da der Gesetzgeber die „wesentlichen" Grundrechtsfragen aufgrund der großen Streubreite eigentlich selbst hätte beantworten müssen.

Noch mehr „alleingelassen" werden die Rechtsanwender*innen vom Gesetzgeber im Bereich moderner Datenerhebungs- und Datenverarbeitungsmaßnahmen. Ein besonders praxisrelevantes Beispiel sind hier Open Source Intelligence-Maßnahmen (OSINT) und Data Mining-Methoden bzw. die Kombination aus beidem (sog. Forensic Web Mining).[49] Unter OSINT wird dabei die manuell oder automatisiert (mittels sog. Scraper oder Crawler) durchgeführte Erhebung von öffentlich zugänglichen Daten aus dem Internet (z. B. soziale Medien, Foren, Marktplätze, Webpages etc.) verstanden.[50] Der Begriff Data Mining fasst dagegen Methoden zusammen, bei denen mit Datenanalyseprogrammen (oftmals auch unter Einsatz von statistischen Methoden und/oder Machine Learning bis hin zu künstlicher Intelligenz) extrem große Datenmengen durchsucht, ausgewertet und mit anderen Daten verknüpft werden.[51] Mangels gesetzgeberischer Regelung werden OSINT-Maßnahmen in der Praxis pauschal auf §§ 161, 163 StPO gestützt. In der Literatur wird dagegen überwiegend danach differenziert, ob die Maßnahme manuell oder automatisiert durchgeführt wird[52] oder ob die Maßnahme auf die Erhebung von sog. Beweisdaten (also zur Überführung einzelner Tatverdächtiger) oder sog. Rasterdaten (zur Gewinnung eines Kreises von möglichen Tatverdächtigen) abzielt.[53] Die Verwendung von Data Mining-Methoden ist in der StPO nicht im Besonderen geregelt. Die §§ 483 ff. StPO regeln lediglich die Datenverarbeitung im Allgemeinen, ohne jedoch im Besonderen auf die Verwendung von Data Mining-Methoden einzugehen. Außerdem entspricht es der zutreffenden hM, dass die §§ 483 ff. StPO gerade nicht auf solche Daten angewendet werden können, die als Beweismittel erhoben und sichergestellt wurden.[54] §§ 98a und 98c StPO regeln dagegen spezifisch den „maschinellen Abgleich" von Daten aus unterschiedlichen Quellen (§ 98a StPO) bzw. von Daten, über welche die Strafverfolgungsbehörden bereits verfügen (§ 98c StPO). Allerdings wird in der Literatur zu Recht eingewandt, die voraussetzungslose Norm des § 98c StPO könne nur „geringfügige Grundrechtseingriffe" rechtfertigen und erfasse nicht das sog. Data Mining.[55] Außerdem wird – aus demselben Grund – eine Beschränkung der Anwendung von § 98c StPO auf den maschinellen Abgleich von Daten vorgeschlagen, die in demselben Strafverfahren (iSv § 264 StPO) erhoben wurden, zu dessen Aufklärung der maschinelle Abgleich er-

[48] MüKoStPO/*Rückert* § 100g Rn. 128 ff.
[49] Vgl. *Rückert* ZStW 129 (2017), 302 (327 f.).
[50] Siehe *Grützner/Jakob*, Compliance von A-Z, Stichwort „OSINT".
[51] Siehe BVerfG NVwZ 2021, 226; *Golla* NJW 2021, 667.
[52] KK /*Moldenhauer* § 163f Rn. 13.
[53] Meyer-Goßner/Schmitt/*Köhler* § 163 Rn. 28a; *Rückert* ZStW 129 (2017), 302 ff.
[54] *Basar/Hiéramente* NStZ 2018, 681 (684); OLG Karlsruhe NStZ 2015, 606 (608); OLG Rostock BeckRS 2017, 119395; BeckOK StPO/*Wittig* § 483 Rn. 1.
[55] BeckOK StPO/*Gerhold* § 98c Rn. 11; *Körffer* DANA 2014, 146 (149).

# Stichwortverzeichnis