Beiträge zum Strafrecht –
Contributions to Criminal Law

5

Elisa Hoven | Hans Kudlich (Hrsg.)

Digitalisierung und Strafverfahren

Nomos

Beiträge zum Strafrecht –
Contributions to Criminal Law

Band 5

Elisa Hoven | Hans Kudlich (Hrsg.)

Digitalisierung und Strafverfahren

Nomos

Onlineversion
Nomos eLibrary

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

ISBN 978-3-8487-6766-3 (Print)

ISBN 978-3-7489-0870-8 (ePDF)

1. Auflage 2020

Inhalt

Einführung

Digitalisierung ist längst mehr als ein Modewort: Der digitale Wandel verändert kontinuierlich unsere Lebenswirklichkeit und erfasst nahezu alle gesellschaftlichen Bereiche – auch das Strafverfahren. Wissenschaft und Praxis müssen sich darüber Gedanken machen, wie man den Gefahren der digitalen Transformation begegnet und gleichzeitig ihre Chancen für den Strafprozess nutzt.

Die Möglichkeiten der Digitalisierung stellen die Strafverfolgungsbehörden vor neue Herausforderungen. Straftaten werden nicht nur im Internet begangen, auch die Kommunikation der Beteiligten erfolgt immer häufiger über Emails und Messengerdienste. Die Verfügbarkeit einer Vielzahl von Daten eröffnet den Behörden neue Wege der Überwachung und Kontrolle – allein über das Smartphone lassen sich die Aufenthaltsorte von Beschuldigten weitgehend präzise rekonstruieren. Allerdings sind die Eingriffsbefugnisse der StPO auf die Nutzung von Mobiltelefonen und Aktivitäten im Darknet nicht zugeschnitten – und helfen den ErmittlerInnen nicht immer weiter.

Ein modernes Strafverfahren muss sich an die Realitäten des digitalen Zeitalters anpassen. Auch wenn der Abschied von Altbekanntem schwer fallen mag – die Digitalisierung bietet erhebliche Chancen nicht nur für eine Effektivierung und Vereinfachung des Strafprozesses (etwa durch die Elektronische Akte), sondern auch für Wahrheitsfindung und Gerechtigkeit. Die Aufzeichnung der Hauptverhandlung oder die Einrichtung von Datenbanken für Strafzumessungsfragen ermöglichen es, Entscheidungen im Strafverfahren nachvollziehbarer und transparenter zu gestalten. Nicht zuletzt kann auch der Strafvollzug von der Digitalisierung profitieren. Die Nutzung des Internets – etwa durch eigene Laptops – erlaubt den Gefangenen Zugang zu Bildungs- und Berufsangeboten im Internet und erleichtert es, den Kontakt mit der Familie zu halten.

Diesen und anderen Themen widmete sich die Tagung „Strafverfahren und Digitalisierung“, die am 5. und 6. Juli 2019 an der Universität Leipzig stattfand. Die Veranstalter danken den ReferentInnen der Tagung herzlich für ihre hoch interessanten Beiträge, den MitarbeiterInnen des Lehrstuhls Hoven (allen voran Frau Barbara Wiedmer) für die gelungene Organisati-

on und den zahlreichen TeilnehmerInnen aus Justiz, Anwaltschaft, Politik und Medien für die spannenden Diskussionen.

Elisa Hoven
Hans Kudlich

Herausforderungen der Digitalisierung für das Strafverfahren

Christian Rückert[1]

I. Neue und alte Fragestellungen des Strafverfahrensrechts im Lichte der Digitalisierung

Die Durchdringung aller Lebensbereiche durch elektronische und digitale Informationstechnologie hat große Auswirkungen auf das Strafverfahren. Dies betrifft zum einen den Einsatz neuer technischer Instrumente durch die Verfahrensbeteiligten, zum anderen die zunehmende Menge von Beweismitteln, die in digitaler Form vorliegen. Beide Bereiche betreffen (in unterschiedlicher Intensität) alle Verfahrensstadien vom Ermittlungsverfahren über Zwischen- und Hauptverfahren bis hin zum Rechtsmittelverfahren und der Strafvollstreckung. Die neuen Technologien und Beweismittel führen zu neuen Herausforderungen für Polizei, Justiz und Anwaltschaft. In einigen Fällen stellen sich völlig neuartige Fragestellungen – wie beispielsweise bei der Erhebung von Daten als Beweismittel über nationale Grenzen hinweg –, in anderen Fällen erfordern technologische Entwicklungen eine Neuevaluierung bekannter Problemkonstellationen (z.B. die „Aufwärmung" der bereits in der 1990er/2000ern geführten sog. Kryptodebatte durch die starke Verbreitung von Verschlüsselungstechnologien). Bisher liegt der Schwerpunkt der juristischen und rechtspolitischen Diskussion auf der Regelung von Einzelfragen. Dies zeigt sich u.a. daran, dass der Gesetzgeber stetig einzelne Eingriffsnormen für den Einsatz neuer technischer Möglichkeiten „nachliefert", von einer umfassenden – und einheitlichen – Neuregelung der strafprozessualen Datenerhebung und -verarbeitung jedoch bislang absieht. Durch die – gerade im Bereich der Datenerhebung, -verarbeitung und -übermittlung auftretenden – Gemengelage mit nachrichtendienstlichen und sicherheitsrechtlichen Eingriffsgrundlagen wird die Lage auch nicht übersichtlicher.[2] Entscheidungen der

---

1 Die Arbeiten wurden gefördert mit Mitteln der Deutschen Forschungsgemeinschaft (DFG) als Teil des Graduiertenkollegs 2475 „Cyberkriminalität und Forensische Informatik" (Projektnummer 393541319/GRK2475/1-2019).

2 Vgl. hierzu ausführlich *Brodowski,* Verdeckte technische Überwachungsmaßnahmen, 2016, S. 253 ff.

höchsten Gerichte zu grundlegenden Fragestellungen sind ebenfalls Mangelware – überwiegend werden dort Einzelfragen eines spezifischen Falles[3] oder einer spezifischen Rechtsgrundlage[4] behandelt. Der strafrechtswissenschaftliche Diskurs besteht vornehmlich aus Beiträgen zu punktuellen Fragestellungen.[5] Die wenigen breiter angelegten (überwiegend monographischen) Auseinandersetzungen mit der Digitalisierung des Strafverfahrens weisen entweder einen sehr starken Praxisbezug auf,[6] beschränken sich ebenfalls auf Spezialprobleme[7] oder sind durch Zeitablauf und den rasanten Technikfortschritt teilweise überholt[8].

Dieser Beitrag will daher – gleichsam wie die breit gefächerte Tagung insgesamt – den (grobkörnigen) Blick auf übergeordnete Herausforderungen der Digitalisierung für das deutsche Strafverfahrensrecht richten. Der Schwerpunkt liegt auf dem Ermittlungsverfahren. Zum einen, um nicht dem Beitrag von *Matthias Jahn* und *Dominik Brodowski* zu sehr vorzugreifen, zum anderen, weil dort ein Großteil der Datenerhebung, -verarbeitung und -speicherung stattfindet. Für die Behandlung von IT-Beweismit-

---

3 Vgl. z.B. BGH MMR 2015, 839; LG Mannheim, NStZ 2018, 430; BGH NStZ 2018, 410 m. Anm. *Safferling*.

4 Vgl. z.B. BGH wistra 2015, 295; BGH NStZ 2018, 611 m. Anm. *Rückert;* BVerfG NJW 2007, 351; BVerfG NJW 2009, 2431.

5 Z.B. *Stoklas/Wendorf*, ZD-Aktuell 2017, 05725 sowie *Großmann,* GA 2018, 439, *Freiling/Safferling/Rückert,* JR 2018, 9 und *Soiné,* NStZ 2018, 497 zu Quellen-TKÜ und Online-Durchsuchung; *Krause*, NStZ 2016, 139 zum IP-Tracking; *ders.,* NJW 2018, 678 zu Darknet-Ermittlungen; *Bäumerich,* NJW 2017, 2718 zur Entschlüsselung von Smartphones; *Zerbes/El-Ghazi*, NStZ 2015, 425 zur „Durchsuchung" in der Cloud; *Safferling/Rückert,* MMR 2015, 788 zur Strafverfolgung bei virtuellen Währungen; BeckOK-StPO/*Graf*, 34. Edition 2019, § 100a Rn 210 ff.: „Aktuelle Einzelfälle und Problemlagen"; MüKo-StPO/*Günther*, 1. Aufl. 2014, § 100a Rn 223 ff.: „Besondere Ermittlungsmaßnahmen".

6 Z.B. *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018.

7 Z.B. *Ihwas,* Strafverfolgung in sozialen Netzwerken, 2014; *Heinson,* IT-Forensik, 2015; *Wicker,* Cloud Computing und staatlicher Strafanspruch, 2016; *Eisenmenger,* Die Grundrechtsrelevanz »virtueller Streifenfahrten«, 2017; *Bauer,* Soziale Netzwerke und strafprozessuale Ermittlungen, 2018; *Warken,* Klassifizierung elektronischer Beweismittel für strafprozessuale Zwecke, 2019; *Müller,* Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts-)Strafverfahren, NZWiSt 2020, 96.

8 Z.B. *Bär,* Der Zugriff auf Computerdaten im Strafverfahren, 1992; *Ernst,* Verarbeitung und Zweckbindung von Informationen im Strafprozeß, 1993; *Böckenförde,* Die Ermittlung im Netz, 2003.

teln in Hauptverfahren und Revision sei auf den gerade genannten Beitrag weiter hinten in diesem Tagungsband (S. 67) verwiesen.

II. Der Ausgangspunkt: Materielle Wahrheit vs. Datenschutz

Ausgangspunkt der Betrachtungen soll dabei ein Spannungsfeld sein, das durch die Kollision eines zentralen Anliegens des Strafverfahrens mit Geheimhaltungsinteressen der Bürgerinnen und Bürger hinsichtlich „ihrer" Daten entsteht: Das Strafverfahren hat zum Ziel, die Wahrheit zu erforschen (vgl. § 244 Abs. 2 StPO).[9] Das (europa-, verfassungs- und einfachrechtliche) Datenschutzrecht will bestimmte Daten dem staatlichen Zugriff entziehen oder nur teilweise (oder zeitweise) zugänglich machen. Das deutsche Strafverfahrensrecht muss die beiden sich widersprechenden Zielsetzungen in Ausgleich bringen. Die Problematik ist nicht neu, sie erhält jedoch durch die den Datenschutz immer stärker betonende Rechtsprechung des BVerfG[10], die Fortentwicklung des europäischen Datenschutzrechts (für den hier relevanten Bereich vor allem die Richtlinie EU 2016/680[11] und deren mittlerweile erfolgten Umsetzung in der StPO sowie Teil 3 des BDSG[12]) und die fortschreitende Digitalisierung nahezu jeder Information eine ganz neue Dimension. Im Folgenden soll das beschriebene Spannungsfeld anhand von sieben zentralen Problemfeldern beleuchtet werden. Gemeinsam ist diesen, dass für keines bislang eine abschließende, befriedigende Lösung gefunden wurde.

III. Tatsächliche und normative Herausforderungen

Die thematisierten Problemfelder lassen sich grob in drei Gruppen einteilen: (1) Zunächst sollen mit der großen und zunehmenden Verfügbarkeit von Daten zu Ermittlungszwecken, der schnellen Entwicklung der Informationstechnologie, der Grenzenlosigkeit und Flüchtigkeit von Daten so-

---

9 BVerfG NJW 2013, 1058 (1060); BGHSt 1, 94 (96); 10, 116 (118); 23, 176 (187); MüKo-StPO/*Trüg/Habetha*, 1. Aufl. 2016, § 244 Rn. 47; Meyer-Goßner/*Schmitt*, StPO, 62. Aufl. 2019, § 244 Rn. 11 jeweils m.w.N.

10 Vgl. zuletzt besonders ausführlich BVerfGE 141, 220 sowie BVerfG NJW 2019, 827 jeweils m.w.N. zur Rechtsprechungsentwicklung.

11 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.DEU.

12 Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 41, S. 1724.

wie der Automatisierung der Datenverarbeitung im Strafverfahren vier Themenfelder behandelt werden, bei denen sich durch technische Entwicklungen in der Kommunikations- und Informationstechnik neue strafverfahrensrechtliche Fragestellungen ergeben. (2) Anschließend geht der Beitrag auf genuin normative Fragestellungen ein: Gibt es ein (Grund-)Recht auf Anonymität? Existiert ein „Recht zur Verschlüsselung"? Und wenn ja, wie verhalten sich diese beiden Rechte zum (verfassungsrechtlich abgesicherten) Interesse des Staates an der Aufklärung von Straftaten? (3) Abschließend wird der „menschliche Faktor" in den Blick genommen. Alle Anstrengungen zur Anpassung und Reform des Strafverfahrensrechts an die Herausforderungen der „digitalen Revolution" sind vergebens, wenn die zur Anwendung dieses Rechts berufenen Menschen nicht in der Lage sind, die sich ihnen stellenden Probleme zu durchdringen und das Strafverfahrensrecht sachgerecht anzuwenden.

1. Zunehmende Menge und Qualität an Daten für Ermittlungsverfahren

Die große und weiter zunehmende Verfügbarkeit von Daten über Personen und Ereignisse eröffnet für Strafverfolger völlig neue Ermittlungs- und Tatnachweismöglichkeiten. Auf den persönlichen Computersystemen von Verdächtigen und Zeugen, wie PCs, Laptops, Tablets und insbesondere Smartphones, sind heute Daten über sehr viele Lebensvorgänge der jeweiligen Person gespeichert. Beispiele sind Kalender, E-Mail-Postfächer, Accounts von sozialen Medien und Messenger-Diensten, Fotos und Videos, Notizen, Unterhaltungsmedien, Daten über Hobbys (z.B. sportliche Aktivitäten, elektronische Eintrittskarten), Reisedaten, Bewegungs- und Aufenthaltsdaten (GPS, Google Maps, Apps für Wanderungen und Radtouren usw). Die vollständige Auswertung solcher Geräte dürfte in vielen Fällen – gerade bei jüngeren Menschen – deutlich mehr Informationen über den Betroffenen liefern als eine akustische Wohnraumüberwachung, in einigen Fällen ist sogar die Erstellung recht präziser Persönlichkeits- und Bewegungsprofile möglich. Daneben finden sich verfahrensrelevante Daten aber auch auf anderen Geräten. Sprachgesteuerte Assistenzsysteme zeichnen Befehle und bearbeitete Vorgänge auf, Fitness-Armbänder speichern Gesundheits- und Bewegungsdaten, Kameras sichern Meta-Bilddaten (z.B. Ort und Zeit der Aufnahme), elektronische Lesegeräte enthalten Daten über die auf ihnen gelesenen Dokumente sowie über Lesemodalitäten, smarte Kühlschränke wissen, wie viele und welche Lebensmittel wann verbraucht und/oder bestellt werden, der smarte Stromzähler zeichnet nicht nur den Stromverbrauch auf, sondern auch, welche Geräte wann einge-

schaltet und verwendet wurden. Unterwegs überwachen Navigationssysteme und Smartphones wie schnell wir uns wohin bewegen und wo wir wieviel Zeit verbringen. Selbstverständlich wird auch unser Kommunikationsverhalten wie Telefonate, Messenger-Nachrichten und die Internetnutzung von großen (kostenlosen) Internetdienstanbietern aufgezeichnet. Sehr viele dieser Daten können in einzelnen Verfahren zur Begründung eines Tatverdachts oder sogar zum Tatnachweis dienen.[13]

a) Steigerung der Intensität von Ermittlungsmaßnahmen

Mit dieser Verbesserung der Ermittlungsmöglichkeiten geht eine Steigerung der Intensität von Überwachungseingriffen einher. Durch die große, möglicherweise verfahrensrelevante, Datenmenge, die bei der Überwachung von Kommunikationsvorgängen aufgezeichnet und bei der Beschlagnahme bzw. Sicherstellung von Datenträgern erhoben werden kann, steigt (zumindest oft) die Qualität der über eine Person erlangten Informationen. Dies bedingt eine Erhöhung der Intensität des Eingriffs in die betroffenen Grundrechte wie das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG, das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleitung der Integrität und Vertraulichkeit informationstechnischer Systeme nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[14] Dies müsste eigentlich Auswirkungen auf die Verhältnismäßigkeitsprüfung sowohl im Gesetzgebungsverfahren für neue Eingriffsnormen als auch bei der Anwendung vorhandener Überwachungsbefugnisse haben. Beides ist bislang jedoch nicht bzw. nur selten der Fall. Exemplarisch kann hier zunächst auf den Entwurf eines neuen § 163g StPO im (geleakten) Gesetzentwurf des „IT-Sicherheitsgesetz 2.0“ des Bundesinnenministeriums verwiesen werden.[15] Mit dieser Norm sollen Ermittlungsbehörden Zugriff auf Nutzerkonten des Verdächtigen bei Telekommunikations- und Telemediendiensten erhalten und diese „virtuelle Identität“ (auch) nutzen, um mit Dritten in Kontakt zu treten. Der Zugriff soll mit Zwangsmitteln er-

---

13 *Gless,* StV 2018, 671; vgl. auch https://www.stern.de/panorama/stern-crime/usa--fitness-armband-ueberfuehrt-90-jaehrigen-nach-axtmord-8389118.html; https://www.heise.de/newsticker/meldung/US-Gericht-Amazon-soll-Echo-Tonaufnahmen-in-Mordfall-herausgeben-4219207.html (Stand: 2.9.2019).

14 Vgl. *Rückert,* ZStW 129 (2017), 302 (320 ff.) zu intensitätssteigernden Faktoren bei Datenverarbeitungseingriffen.

15 https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (Stand: 2.9.2019).

zwungen werden dürfen. Ebenso soll eine Auswertung der Daten, auf die mittels des Accounts zugegriffen werden kann, möglich sein (die gewonnenen Informationen sollen aber nur in einem Strafverfahren gegen den Verdächtigen oder eine nach § 52 Abs. 1 StPO geschützte Person verwendet werden dürfen, wenn der Verdächtige zustimmt). Neben vielen anderen Problemen[16] des Entwurfs spiegelt dieser nicht die Intensität wider, die eine Auswertung der Daten in solchen Nutzerkonten haben kann. In E-Mail-Accounts, Nutzerkonten von sozialen Medien und Cloud-Dienstleistern (die alle von der Regelung umfasst sind) lassen sich Informationen über vergangene Kommunikation, soziale Netzwerke, verschiedenste Tätigkeiten privater und beruflicher Natur (inkl. Informationen, die Geschäftsgeheimnissen unterfallen, insbes. Mandatsbeziehungen bei Anwälten, Patienteninformationen bei Ärzten usw.) und Bewegungsdaten erlangen. Trotz dieser potentiell extremen Eingriffsintensität enthält der Gesetzentwurf keine spezifischen Beschränkungen, um dem Verhältnismäßigkeitsprinzip Rechnung zu tragen. Insbesondere sind – anders als in den §§ 97, 105 StPO für Durchsuchung und Beschlagnahme sowie §§ 100b, 100c, 100e Abs. 2 StPO für die Online-Durchsuchung – in § 163g StPO-Entwurf kein Anordnungsvorbehalt (Staatsanwaltschaft oder Gericht), kein abschließender Straftatenkatalog und (abgesehen vom Schutz der in § 52 StPO genannten Personen) keine Beschränkung der Datennutzung (z.B. Kernbereich und Schutz von nach § 53 StPO zeugnisverweigerungsberechtigten Personen) vorgesehen.

Als Beispiel aus der Anwendung bestehender Normen kann die Beschlagnahme von E-Mails bzw. ganzen E-Mail-Nutzerkonten herangezogen werden. In solchen Nutzerkonten sind oftmals zigtausende E-Mails aus mehreren Jahren gespeichert. Sie betreffen die berufliche, private und auch intime Korrespondenz. Zusätzlich sind in modernen Nutzerkonten häufig weitere Funktionen verfügbar, die private Daten speichern, wie z.B. Kalender oder Cloud-Speicher. Da eine Durchsicht und Filterung der verfahrensrelevanten E-Mails vor Ort (also z.B. beim Verdächtigen oder beim E-Mail-Provider) aus Zeitgründen und Personalmangel nicht oder nur unter großen Anstrengungen durchgeführt werden kann, spiegeln die Strafverfolgungsbehörden in der Regel den gesamten E-Mail-Bestand (zuzüglich evtl. weiterer gespeicherter Informationen) und werten die Daten bei

---

16 *Rückert*, IT-Sicherheitsgesetz – Von der Wunschliste der Strafverfolger, FAZ-Einspruch, abrufbar: https://einspruch.faz.net/einspruch-magazin/2019-05-01/von-der-wunschliste-der-strafverfolger/239845.html (hinter Bezahlschranke); *Oehmichen/Weißenberger*, KriPoz 2019, 174; *Kubiciel/Mennemann*, jurisPR-StrafR 08/2019, Anm. 1; zu § 126a StGB-Entwurf auch *Bachmann/Arslan*, NZWiSt 2019, 241.

der Polizei oder Staatsanwaltschaft (ggf. unter Nutzung von Auswertungssoftware) aus. Gleiches gilt für bei Durchsuchungen aufgefundene Datenträger, auf denen sich noch viel größere Datenbestände befinden können. Durch die größere verfügbare Datenmenge ist hier bei der Anwendung der §§ 94 ff., 102 ff. StPO eine krasse Zunahme der Intensität von Beschlagnahme- und Durchsuchungsmaßnahmen zu beobachten. Zumindest nach der Beobachtung durch den *Verfasser* fehlt es hier jedoch häufig an einer entsprechenden Sensibilisierung der Verfahrensbeteiligten für die Intensität der Maßnahme und damit einhergehende Verhältnismäßigkeitserwägungen.

b) Zufallsfunde und Legalitätsprinzip

Die große Fülle von digital verfügbaren Informationen über Straftaten, nicht nur auf Datenträgern, sondern auch in (mehr oder weniger) frei zugänglichen Bereichen des Internets, führt zu einem weiteren Problem für die Strafverfolgungsbehörden. Die bei Durchsuchungs- und Überwachungsmaßnahmen erhobenen Datenmengen und die bei Online-Recherchen und -Ermittlungen gewonnen Daten enthalten häufig auch Informationen über Straftaten, die gar nicht Anlass der Ermittlungsmaßnahmen waren (sog. Zufallsfunde). Die große Menge an digital verfügbaren Informationen, die bei Ermittlungsmaßnahmen erhoben werden, erhöht dabei die Wahrscheinlichkeit für Zufallsfunde. Kein Problem ist dabei zunächst der rechtliche Rahmen für die Verwertung von Zufallsfunden. Hier gilt im digitalen wie im analogen Bereich § 479 Abs. 2 StPO (bzw. § 100e Abs. 6 für Maßnahmen nach §§ 100b und 100c StPO, § 100i Abs. 2 S. 2 für Maßnahmen nach § 100i und § 161 Abs. 3 StPO, wenn die Daten bei einer außerstrafprozessualen Maßnahme erlangt worden sind). Probleme entstehen jedoch, wenn die Menge der Zufallsfunde so groß wird, dass die Ermittlungen zu den Zufallserkenntnissen mit den (insbes. personellen) Ressourcen der Strafverfolgungsbehörden nicht mehr oder nur teilweise durchführbar sind. Das kann zum einen durch die Ubiquität von digitalen Verstößen gegen das Urheberrecht (§ 106 UrhG) und von Äußerungsdelikten im Zusammenhang mit sozialen Medien (insbes. §§ 130 ff., 185 ff. StGB) der Fall sein. Während hier noch in einigen Fällen die Notwendigkeit eines Strafantrags oder eines besonderen öffentlichen Interesses (vgl. §§ 109 UrhG, 194 StGB) die Problematik abmildert, gilt dies nicht für den Bereich des Handels mit illegalen Waren und Dienstleistungen im Internet, insbes. im sog. Darknet. Dort sind auf vielen Plattformen sowohl die Verkaufsangebote als auch die Bewertungen der Verkäufer und Statistiken

über Transaktionen öffentlich einsehbar. Diese enthalten in der Regel hinreichende Informationen, um einen Anfangsverdacht i.S.v. § 152 Abs. 2 StPO zu begründen. Hinzu kommt, dass viele der Straftaten, die auf den Handelsplattformen der sog. Underground Economy im Darknet begangen werden (z.B. der Handel mit Betäubungsmitteln, die Verbreitung kinderpornographischer Schriften und die Geld- und Wertzeichenfälschung), unter § 6 StGB fallen und eine Zuständigkeit der deutschen Strafverfolgungsbehörden sogar für reine Auslandstaten begründen. Die Strafverfolgungsbehörden (insbes. die Schwerpunktstaatsanwaltschaften und die spezialisierten Ermittler der Landeskriminalämter und des Bundeskriminalamts) erlangen von diesen Informationen beispielsweise im Rahmen von sog. Online-Streifen auf den bekannten Plattformen Kenntnis.[17] Hier kommt das Legalitätsprinzip des § 152 Abs. 2 StPO schnell an seine Grenzen. Der Praxis bleibt vorerst nichts anderes übrig, als die (möglichen) Ermittlungsverfahren zu priorisieren und ihre Mittel auf schwere Straftaten und aussichtsreiche Fälle zu konzentrieren. Abhilfe muss die Politik schaffen – durch eine Erweiterung der Opportunitätseinstellungsmöglichkeiten und/oder eine Aufstockung der personellen und technischen Mittel.

2. *Herausforderungen durch die Geschwindigkeit der technischen Entwicklung*

Der Technik-Visionär *Raymond Kurzweil* schrieb bereits 1999 in seinem Buch „The Law of Accelerating Returns“: „An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense ‚intuitive linear‘ view. So we won’t experience 100 years of progress in the 21st century — it will be more like 20,000 years of progress (at today’s rate).“ Die letzten 20 Jahr haben ihm Recht gegeben. Die Informations- und Kommunikationstechnologie entwickelt sich mit einer derart rasenden Geschwindigkeit, dass Mensch und Gesellschaft damit kaum mehr Schritt halten können. Noch weniger kann es das (Strafverfahrens-)Recht – nicht zuletzt aufgrund der Langsamkeit demokratischer Willensbildungsprozesse.

---

17 *Safferling/Rückert*, Konrad-Adenauer-Stiftung: Analysen & Argumente 291, 9.

a) Materielles Strafrecht: Neue Kriminalitätsformen

Herausforderungen für das Strafverfahren ergeben sich sowohl auf materiell-rechtlicher als auch auf verfahrensrechtlicher Ebene. So werden die Strafverfolgungsbehörden mit neuen Kriminalitätsformen konfrontiert. Dies sind zum einen neue Begehungsarten bekannter Kriminalitätsphänomene. Beispiele sind Gewaltausübung mittels Computersysteme bzw. Internet (z.B. der Mord durch das Manipulieren eines hackbaren Herzschrittmachers oder einer Schmerzmittel- oder Insulinpumpe),[18] die Cyber-Spionage[19] oder Äußerungsdelikte in sozialen Medien und Kommentarspalten von Online-Artikeln. Zum anderen entstehen mit neuer Technik aber auch völlig neue Kriminalitätsarten. So machten erst die Tor-Technologie und die Kryptowährungssysteme die Entstehung des professionellen und groß angelegten Handels mit illegalen Waren und Dienstleistungen im Darknet möglich. Erst durch sie war die Erschließung des Internetmarktes bei gleichzeitiger (weitgehender) Wahrung von Anonymität von Käufer und Verkäufer verwirklichbar. Auch der „Diebstahl" von werthaltigen virtuellen Gütern (neben Kryptowährungseinheiten auch z.B. virtuelle Gegenstände aus Computerspielen, bekannte Nutzerkonten in sozialen Medien etc.) ist erst durch die Entstehung dieser möglich geworden. Die Digitalisierung der Kommunikation von Kindern und Jugendlichen macht diese anfällig für das sog. Cyber-Grooming und vor allem die Digitalisierung von Informationen und die Speicherung der Daten auf an das Internet angeschlossene Rechner ermöglicht es Hackern, geheime und/oder private Dokumente und Informationen zu erlangen und diese im Internet zu veröffentlichen (sog. Doxing). Hier gilt es im Einzelfall zu prüfen, ob die bestehenden Strafnormen die neuen Konstellationen oder Begehungsarten hinreichend erfassen. Erste Schritte wurden hier bereits von der Länderarbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht" der Justizministerkonferenz unternommen.

---

18 *Wittes/Blum*, The Future of Violence, 2015.

19 Vgl. hierzu den Entwurf eines IT-Sicherheitsgesetzes 2.0 durch das BMI: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (Stand: 2.9.2019).

b) Strafprozessrecht: Neue Ermittlungsmethoden

Das Strafverfahrensrecht muss sich dagegen vor allem dem Umgang mit neuen Ermittlungsmethoden und -techniken stellen, welche teils durch die Ermittler selbst, teils durch die wissenschaftliche Forschung und teils durch Privatunternehmen entwickelt werden. Beispiele aus den letzten Jahren sind der Einsatz von Spähprogrammen im Rahmen der Quellentelekommunikationsüberwachung und der Online-Durchsuchung nach §§ 100a, b StPO, der Einsatz von Web-Crawlern und automatischen Datenauswertungsprogrammen (sog. Forensischen Web Mining – bislang unreguliert) und das heimliche Erheben von IP-Adressen durch den Versand von E-Mails mit eingebettetem Bildmaterial oder der Anforderung von Lesebestätigungen (sog. IP-Tracking, nach Auffassung des Ermittlungsrichters beim BGH zulässig nach § 100g StPO[20]) und das Erheben von IP-Adressen der Besucher von bestimmten Websiten (sog. IP-Catching, bislang unreguliert[21]) sowie – bereits seit längerer Zeit im Einsatz – das Versenden sog. Stiller SMS zur Bestimmung des Aufenthaltsorts von Verdächtigen und der Erstellung von Bewegungsprofilen (nach Auffassung des BGH gestützt auf §§ 100g, 100i StPO[22]). Herausforderungen ergeben sich für das Strafverfahrensrecht in diesem Bereich vor allem daraus, dass es sich bei (fast) allen neuen Ermittlungsmaßnahmen um Grundrechtseingriffe handelt und daher der verfassungsrechtliche Vorbehalt des Gesetzes und der sog. Wesentlichkeitsvorbehalt gelten. Die Ermittlungsgeneralklauseln der §§ 161, 163 StPO können nur als Rechtsgrundlage herangezogen werden, wenn es sich lediglich um geringfügige Grundrechtseingriffe handelt.[23] Dies ist für jede neue Ermittlungsmaßnahme gesondert und *vor* ihrem Einsatz durch die anordnende Behörde/das anordnende Gericht festzustellen. Für Techniken, die mehr als nur geringfügig in Grundrechte eingreifen, hat sich in der Praxis in den letzten Jahren eine „neue Methode" der Rechtsgrundlagen(er-)findung etabliert: Das „Zusammenbasteln" verschiedener Rechtsgrundlagen zu einer neuen „Super-Rechtsgrundlage" für die neue Ermittlungstechnik. Ein (unrühmliches) Beispiel hierfür war der Versuch, die strafprozessuale Online-Durchsuchung (lange) vor Inkrafttreten des § 100b StPO mittels einer Kombination der Befugnisse aus

20 BGH wistra 2015, 395; krit.: *Krause,* NStZ 2016, 139.

21 Nach Auffassung von *Bär* zulässig nach § 100g StPO, vgl. BeckOKStPO/*Bär,* 36. Ed. 2020, § 100g Rn. 23,

22 BGH NStZ 2018, 611 m. krit. Anm. *Rückert.*

23 BGHSt 51, 211 (218); Meyer-Goßner/*Schmitt,* StPO, 62. Aufl. 2019, § 161 Rn. 1 m.w.N.

§§ 102, 100a und 100c StPO zu legitimieren.[24] In neuerer Zeit hat der BGH den Einsatz der sog. Stillen SMS auf eine Kombination aus §§ 100i, 100g StPO gestützt.[25] In der Literatur wird die Auffassung vertreten, das IP-Catching finde seine Rechtsgrundlage in der Kombination aus §§ 100g, 100j StPO[26]. Der Bundesgerichtshof hat in seiner Entscheidung zur Onlinedurchsuchung 2007 einer Kombination verschiedener Eingriffsbefugnisse eigentlich eine Absage erteilt.[27] Gestützt hat er seine ablehnende Haltung damals zu Recht auf den Gesetzesvorbehalt und die Grundsätze der Normenklarheit und -bestimmtheit.[28] Bei der Schaffung und Ausgestaltung von Rechtsgrundlagen für Grundrechtseingriffe geht es nicht nur darum, bestimmte verfassungs- oder europarechtliche Anforderungen einzuhalten. Aus der Perspektive der Normunterworfenen muss auch die Vorhersehbarkeit der möglichen Grundrechtseingriffe berücksichtigt werden. Könnten Normen in beliebiger, unvorhersehbarer Art und Weise, kombiniert werden, um neue Eingriffsbefugnisse aus der Taufe zu heben, wäre dieses Prinzip vollkommen ausgehebelt. Der Vorbehalt des Gesetzes und der Wesentlichkeitsvorbehalt erfordern es überdies, dass der Gesetzgeber nicht nur über die Ausgestaltung einzelner Befugnisse entscheidet, sondern auch darüber, ob es bestimmte Befugnisse überhaupt geben soll – unabhängig davon, ob die neue Ermittlungsmethode von ihrer Eingriffstiefe her mit bestehenden Befugnissen vergleichbar ist. Deshalb sind die Ermittlungsgeneralklauseln auch zu Recht nur bei geringfügigen Grundrechtseingriffen anzuwenden. Dass die Behäbigkeit des Gesetzgebers gerade im sich schnell entwickelnden Bereich der Informations- und Kommunikationstechnologie frustrierend sein kann, ist verständlich – ändert aber nichts an den verfassungsrechtlichen Vorgaben.

Der Gesetzgeber muss sich daher der Herausforderung stellen, rechtzeitig praxistaugliche und verfassungskonforme Rechtsgrundlagen für neue, aber absehbare, Ermittlungsmaßnahmen zu schaffen. Grundlage hierfür kann – und sollte – ein Dialog der Rechtspolitik mit Experten aus Praxis und Wissenschaft sein, in welchem die technische Entwicklung in den Blick genommen und Lösungen entwickelt werden. Auch hier ist die oben angesprochene Länderarbeitsgruppe „Digitale Agenda für das Straf- und

---

24 BGH Ermittlungsrichter wistra 2007, 28 ff.; zu Recht ablehnend BGH 51, 211 (218 f.).

25 BGH NStZ 2018, 611 m. krit. Anm. *Rückert;* ablehnend auch *Singelnstein*, NStZ 2014, 305 (308).

26 BeckOK-StPO/*Bär*, 36. Edition 2020, § 100g Rn. 23.

27 BGH 51, 211 (219).

28 BGH 51, 211 (219).

Strafprozessrecht“ sicherlich der richtige Weg. So kann auch vermieden werden, dass – wie unlängst bei der Regelung der Online-Durchsuchung geschehen – zukünftige Normen an der technischen Realität und den tatsächlichen Bedürfnissen der Strafverfolger vorbeigehen.[29]

3. *Grenzenlosigkeit des Internets und Flüchtigkeit von Datenbeständen*

Die moderne Infrastruktur des Internets und von Computersystemen stellt weitere Herausforderungen an das (nationale) Strafverfahrensrecht. Durch das Internet sind Computersysteme weltweit vernetzt und Datenbestände schwierig zu lokalisieren. Sie sind an verschiedenen Orten „gleichzeitig“ (im Sinne mehrerer Kopien „desselben“ oder eines im Informationsgehalt „ähnlichen“ Datenbestandes) vorhanden, liegen ggf. sogar „aufgeteilt“ an verschiedenen Speicherorten vor (bezogen auf den einheitlichen Informationsgehalt) und werden in kürzester Zeit „umgezogen“ (also von einem an einen anderen Ort übertragen).

a) Flüchtigkeit und Beweglichkeit von Datensätzen

Die „Flüchtigkeit“ und Beweglichkeit von Datenbeständen stellt eine Herausforderung für das Beweisrecht der StPO dar. So können Datensätze, die denselben Lebensvorgang betreffen, an verschiedenen Orten in verschiedenen Zuständen vorliegen, also einen unterschiedlichen Informationsgehalt aufweisen. Ein einfaches Beispiel ist ein Chatverlauf, der auf den Geräten der Chat-Partner in unterschiedlicher Form gespeichert ist, sei es, weil er von einem Partner auf seinem Gerät bewusst manipuliert wurde oder weil ein Synchronisationsvorgang auf einem Gerät noch nicht stattgefunden hat. Außerdem werden Datensätze häufig fortgeschrieben, verändert oder gelöscht, sodass sich der Informationsgehalt ändert oder sogar für ein Strafverfahren nicht mehr zur Verfügung steht. Ein weiteres Problem entsteht durch die mannigfaltigen Manipulationsmöglichkeiten an Datensätzen, die ohne entsprechende technische Expertise nicht oder nur schwer zu erkennen sind. Sämtliche beschriebenen Probleme betreffen den strafverfahrensrechtlichen „Wert“, den ein Datensatz in verschiedenen Verfahrensstadien hat. Zuvorderst ist hiermit die für verschiedene Stufen eines Tatverdachts notwendige Tatsachenqualität im Ermittlungsverfahren

29 Vertiefend hierzu: *Freiling/Safferling/Rückert,* JR 2018, 9; *Großmann,* GA 2018, 439.

betroffen. Grundrechtseingreifende Maßnahmen im Ermittlungsverfahren erfordern für die Begründung des für die jeweilige Maßnahme notwendigen Verdachtsgrades eine bestimmte Tatsachenqualität. Diese ergibt sich teilweise bereits aus dem Gesetz, z.B. „zureichende tatsächliche Anhaltspunkte" in § 152 Abs. 2 StPO, „bestimmte Tatsachen" in §§ 100a ff. StPO. Teilweise werden die Anforderungen jedoch auch von der Rechtsprechung aufgestellt bzw. konkretisiert. Beispielsweise ist nach der Rspr. des BVerfG für einen Tatverdacht nach § 100a StPO erforderlich, „dass auf Grund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus Zeugenaussagen, Observationen oder anderen sachlichen Beweisanzeichen" darauf geschlossen werden kann, dass der Tatverdächtige eine Katalogtat begangen hat.[30] Bislang kaum explizit thematisiert, jedoch selbstverständlich, ist, dass die Beweismittel, die zur Begründung eines Tatverdachts dienen sollen, echt und unverfälscht sein, aus einer vertrauenswürdigen Quelle stammen und diese Eigenschaften überprüfbar sein müssen. In der IT-Forensik werden zur Beschreibung dieser Eigenschaften in Bezug auf Daten häufig die Begriffe der Authentizität und Integrität verwendet.[31] Noch vielmehr gilt dies natürlich für Datensätze, die im Hauptverfahren als Beweismittel für die Schuld des Angeklagten herangezogen werden sollen. Als objektive Tatsachengrundlage[32] für die subjektive Überzeugung des Gerichts von der Schuld des Angeklagten müssen die Datensätze ein Höchstmaß an Echtheit und Vertrauenswürdigkeit aufweisen. Die Flüchtigkeit und die leichte Manipulierbarkeit von Daten bedingen, dass für das Strafverfahren standardisierte Maßnahmen zur Sicherung der Authentizität und Integrität der im Verfahren verwendeten Datensätze entwickelt und angewendet werden müssen. Alle Verfahrensbeteiligten sollen in den Stand versetzt werden, die verwendeten Daten auf diese beiden Eigenschaften hin jederzeit überprüfen zu können. Die technischen Möglichkeiten sind hier bereits weitgehend vorhanden und sogar recht einfach zu implementieren. Das Strafverfahrensrecht muss nur sicherstellen, dass diese technischen Maßnahmen in der Fläche Anwendung finden. Die derzeitige Praxis ist hier sehr unterschiedlich, in Abhängigkeit von der technischen Kompetenz der Verfahrensbeteiligten und deren Sensibilisierung für die Problematik.[33]

---

30 BVerfG NJW 2007, 2752 (2753).

31 *Maras,* Computer Forensics, Second Edition 2015, S. 46 ff.; BSI, Leitfaden IT-Forensik 2011, S. 23; S. 30; SWGDE, Digital & Multimedia Evidence Glossary, S. 5, S. 11.

32 Hierzu KK/*Ott,* 8. Aufl. 2019, § 261 Rn. 5 ff. m.w.N. zur AllgM.

33 Zum Ganzen ausführlich *Heinson,* IT-Forensik, 2015, S. 146 ff. m.w.N.

b) Lokalisierung der Datensätze im Ausland

Das moderne Cloud-Computing und das Angebot verschiedener internetbasierter Dienstleistungen führt dazu, dass verfahrensrelevante Datensätze häufig ganz oder teilweise auf Datenträgern im Ausland gespeichert sind. Wegen der Flüchtigkeit dieser Datenbestände sind die Strafverfolgungsbehörden darauf angewiesen, schnell eine exakte Kopie des jeweiligen Datensatzes zu erhalten. Der traditionelle Weg über die Rechtshilfe ist hier in vielen Fällen zu langsam oder führt gar nicht zum Erfolg.[34] Eigene Datenerhebungen durch die Strafverfolgungsbehörden würden zwar oftmals eine schnelle Sicherung der Datensätze im Ausland ermöglichen, grundsätzlich dürfen deutsche Strafverfolgungsbehörden jedoch keine Ermittlungsmaßnahmen auf fremdem Hoheitsgebiet durchführen.[35] Die bisher existierenden Instrumente grenzüberschreitender Zusammenarbeit im europäischen (z.B. die Informations- und Datenbanksysteme von Europol, die Regelungen zur Zusammenarbeit in Art. 39 ff. SDÜ, die Beschleunigung des Rechtshilfeverfahrens gem. Art. 15 EuropReHiÜbk, die Sicherstellung von Vermögensgegenständen innerhalb von 24 Stunden nach Art. 4, 5 Rahmenbeschluss 2003/577/JI des Rates, die Richtlinie über die europäische Ermittlungsanordnung in Strafsachen und die Bildung gemeinsamer Ermittlungsgruppen nach dem Rahmenbeschluss 2002/465/JI) und internationalen Kontext (für den hiesigen Zusammenhang vor allem die Cybercrime Convention 2001, die es aber lediglich ermöglicht, auf Daten im Ausland zuzugreifen, wenn diese öffentlich zugänglich sind oder der Berechtigte sein Einverständnis erklärt, vgl. Art. 32 der Cybercrime Convention) werden von den Strafverfolgungsbehörden zu Recht als nicht hinreichend empfunden.[36] Dies hat eine andauernde und intensiv geführte Diskussion über die Zulässigkeit von transnationalen Dateneingriffen und über die Konsequenzen rechtswidriger transnationaler Dateneingriffe für die Beweisverwertung verursacht.[37] Zur Lösung des Problems wurden in letzter Zeit zahlreiche Gesetzgebungsvorhaben und völkerrechtliche Abkommen auf den Weg gebracht bzw. sind teilweise schon ins Werk gesetzt.

---

34 *Goger/Stock*, ZRP 2017, 10 (11).

35 MüKoStPO/*Hauschild*, 1. Aufl. 2014, § 110 Rn. 18 m.w.N.

36 *Goger/Stock*, ZRP 2017, 10 (12 f.).

37 Vgl. aus der Diskussion jeweils m.w.N.: *Zerbes/El-Ghazi*, NStZ 2015, 425; *Brodowski/Eisenmenger*, ZD 2014, 119; *Wicker*, MMR 2013, 765; *Krause*, Kriminalistik 2014, 213 (214 f.); *Soiné*, NStZ 2018, 497 (500); BeckOK-StPO/*Hegmann*, 34. Edition 2019, § 110 Rn. 15; Meyer-Goßner/*Schmitt*, *StPO*, 62. Aufl. 2019, § 110 Rn. 7b; KK-*Bruns*, 8. Auflage 2019, § 110 Rn. 8a.

Bereits in Kraft getreten ist der US-amerikanische CLOUD-Act, der Anbieter elektronischer Kommunikationsdienste und sog. Remote-Computing-Dienste, die amerikanischem Recht unterfallen, verpflichtet, Daten über seine Kunden und deren Kommunikation auch dann an US-Strafverfolger herauszugeben, wenn die entsprechenden Daten im Ausland gespeichert sind.[38] Die Europäische Union arbeitet intensiv an der sog. E-Evidence-Verordnung, welche eine unmittelbare Datenübermittlung an Strafverfolgungsbehörden innerhalb der Europäischen Union (und teilweise auch aus Drittstaaten) ermöglichen soll. Für Details sei auf die Beiträge von *Patricia Hamel* (S. 103) und *Margarete von Galen* (S. 127) weiter hinten in diesem Tagungsband verwiesen. Im Zusammenhang mit der E-Evidence-Verordnung und dem CLOUD-Act wird auch über ein völkerrechtliches Abkommen zwischen der EU und den USA verhandelt, dass den Strafverfolgungsbehörden wechselseitigen Direktzugriff auf Daten ermöglichen soll.[39] Überdies finden sich im geleakten Entwurf des IT-Sicherheitsgesetzes 2.0 des Bundesinnenministeriums mit § 110 Abs. 1a TKG-Entwurf und § 15b Abs. 2 TMG-Entwurf Normen, welche die Anbieter von Telekommunikations- und Telemediendiensten dazu verpflichten sollen, Bestandsdaten deutscher Kunden stets auch im Inland zu speichern und damit den Direktzugriff deutscher Strafverfolgungsbehörden zu ermöglichen.[40] Ein rechtspolitisch bislang zu wenig thematisiertes und daher nicht gelöstes Problem in diesem Zusammenhang betrifft die Kollision unterschiedlicher Datenschutzstandards zwischen den einzelnen an solchen Abkommen beteiligten Ländern. Es ist unklar, wie ein hinreichender Schutz der Daten der eigenen Bürger nach den eigenen Standards gewährleistet werden kann, wenn gleichzeitig ein wechselseitiger Direktzugriff der Strafverfolgungsbehörden vereinbart wird. Hier steht derzeit zu befürchten, dass der Datenschutz der deutschen Bürger am europäischen und internationalen Verhandlungstisch starke Einschränkungen erfahren wird.[41] Nicht unberücksichtigt bleiben darf dabei, dass der Direktzugriff auf in Deutschland gespeicherte Daten durch weniger rechtsstaatliche orientierte Staaten

---

38 Für Details vgl. *Gausling,* MMR 2018, 578.

39 https://netzpolitik.org/2019/eu-startet-gespraeche-mit-den-usa-ueber-zugriff-auf-cloud-daten/ (Stand: 2.9.2019).

40 https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 (Stand: 08.05.2020).

41 Zum Ganzen *Rath/Spies,* CCZ 2018, 229; *Schaar,* MMR 2018, 705; *Burchard,* ZRP 2019, 164 jeweils m.w.N.

gleichzeitig eine Gefährdung des Raums der Sicherheit für Dissidenten und Exilanten aus diesen Staaten in Deutschland bedeutet.

c) Internationalisierung der Strafverfolgung

Die Grenzenlosigkeit des Datenverkehrs und die leichte Vernetzung krimineller Akteure über das Internet hat die Notwendigkeit herbeigeführt, strafrechtliche Ermittlungsverfahren über Grenzen hinweg zu führen. Viele Ermittlungserfolge gegen die (organisierte) Internetkriminalität der letzten Jahre sind zumindest zum Teil auf die Zusammenarbeit mit ausländischen Strafverfolgungsbehörden zurückzuführen.[42] In diesen Zusammenhängen stellt sich zunehmend das Problem, dass die unterschiedlichen, nationalen Strafverfahrensordnungen unterschiedliche Eingriffsbefugnisse und Schutzstandards aufweisen. Oftmals reichen die Befugnisse der ausländischen Ermittlungsbehörden weiter als diejenigen der deutschen Strafverfolger. In der Praxis hat dies zum Phänomen des sog. Forum Shopping geführt. Dabei werden Ermittlungsmaßnahmen bei einer gemeinsamen grenzüberschreitenden Ermittlung, die in einem oder mehreren der beteiligten Staaten nicht erlaubt wären, von denjenigen Ermittlungsbehörden durchgeführt, in deren Heimatland die Ermittlungsmaßnahme erlaubt ist. Die erlangten Daten und Informationen werden später geteilt und von allen beteiligten Behörden verwendet.[43] Ein Beispiel für die Vornahme von nach deutschem Recht rechtswidrigen Ermittlungsmaßnahmen ist das Verfahren gegen die Betreiber und Nutzer des Darknet-Markets „Hansa Market". Dort hatten niederländische Ermittler die gesamte Plattform übernommen und über mehrere Wochen aktiv weiterbetrieben. Während dieser Zeit wurden weiterhin illegale Waren und Dienstleistungen über die Plattform gehandelt. Nach deutschem Strafverfahrensrecht wäre eine solche Maßnahme nicht zulässig gewesen.[44] Dennoch wurden die von den niederländischen Behörden erlangten Informationen auch mit deutschen Strafverfolgern geteilt und von diesen in deutschen Strafverfahren verwen-

---

42 Z.B. Ermittlungen gegen die Darknet-Handelsplattform „Hansa Market", https://www.wired.com/story/hansa-dutch-police-sting-operation/; zur KiPo-Plattform „Elysium", https://www.spiegel.de/panorama/justiz/kinderpornos-was-ermittler-duerfen-und-was-nicht-a-1221593.html (Stand: jeweils 2.9.2019).

43 Vgl. *Swoboda*, HRRS 2014, 10 (17 f.).

44 Vgl. *Sieber/Brodowski* in Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 48. EL 2019, Teil 19.3 Rn. 47 f.

det.[45] Das deutsche Strafverfahrensrecht und die deutsche Rechtspolitik steht daher vor der Herausforderung, die notwendigen Instrumente internationaler Zusammenarbeit mit den Werten und Grundentscheidungen des deutschen Strafverfahrensrechts in Ausgleich zu bringen. Ohne Reibungsverluste bei den (vergleichsweise hohen) deutschen Schutzstandards wird dies wohl nicht gelingen.

d) Vereinheitlichung des europäischen Datenschutzrechts

Auch in den Bereich der Internationalisierung des deutschen Strafverfahrensrechts fällt die notwendige Anpassung der deutschen StPO (und der Datenschutzgesetze) an die Richtlinie EU 2016/680. Europarecht wird in Zukunft einen zentralen Teil des Strafverfahrens, insbesondere des strafrechtlichen Ermittlungsverfahrens, prägen. Der Gesetzgeber steht vor der nicht zu unterschätzenden Aufgabe, das bislang in der StPO nur partikular geregelte und durch die Rechtsprechung des BVerfG nur schrittweise weiterentwickelte Datenschutzrecht umfassend neu zu regeln und die Vorgaben der Europarichtlinie einzuhalten. Ein Gesetz zur Umsetzung ist mittlerweile in Kraft getreten.[46] Unklar ist jedoch bislang, ob eine richtlinienkonforme Umsetzung vollständig gelungen ist[47] und welche Folgen sich für die Praxis der Strafverfahren in Zukunft konkret ergeben werden. Auch bei der Rechtsanwendung wird es einschneidende Veränderungen geben. Im Geltungsbereich der Richtlinie – und diese gilt in sehr weiten Teilen der StPO – sind gem. Art. 51 Abs. 1 HS. 2 EU-Grundrechtecharta die Grundrechte der EU-Charta unmittelbar als höherrangiges Recht anwendbar und zu beachten.[48] Dies hat zur Folge, dass nunmehr auch die Rechtsprechung des EuGH unmittelbar Einfluss auf die Ausgestaltung und Anwendung deutscher StPO-Normen hat. Gleiches gilt auch – über

---

45 *Rückert/Wüst,* KriPoz 2018, 247 (250); https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/171122_RauschgiftDarknet.html; https://www.spiegel.de/netzwelt/netzpolitik/darknet-ermittler-zerschlagen-grosse-marktplaetze-alphabay-und-hansa-a-1158933.html (Stand: 2.9.2019).

46 https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Umsetzung_RL-EU-2016-680_und_Anpassung_datnschutzrechtlicher_Bestimmungen.pdf?__blob=publicationFile&v=3. (Stand: 2.9.2019).

47 Siehe z.B. Gola/Heckmann/*Paschke,* 13. Aufl. 2019, § 54 BDSG Rn. 9.

48 Zur Anwendbarkeit der EU-Grundrechtecharta bei Umsetzung von EU-Richtlinien in nationales Recht und Anwendung dieses nationalen Rechts: Meyer/*Borowsky,* 4. Aufl. 2014, Art. 51 Rn 28; *Esser,* in: Sieber/Satzger/v. Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2. Aufl. 2014, S. 955 jeweils m.w.N.

die Brücke des Art. 6 Abs. 3 EUV (nach dem Beitritt der EU zur EMRK über Art. 6 Abs. 2 EUV[49]) – für die EMRK und damit für die Rechtsprechung des EGMR. Die EMRK gilt somit im Anwendungsbereich der Richtlinie für die StPO als höherrangiges Recht und nicht mehr „nur" im Range eines Bundesgesetzes oder nur mittelbar über die völkerrechtsfreundliche Auslegung von deutschen Grundrechten.[50] Da der EuGH jedoch die Anwendung nationaler grundrechtlicher Schutzstandards für zulässig hält, wenn den Mitgliedstaaten durch das Unionsrecht ein Umsetzungsspielraum eingeräumt ist und sichergestellt ist, dass hierdurch „weder das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird, noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden",[51] ergeben sich hier in Zukunft spannende Abgrenzungsfragen, die von Rechtsprechung und Rechtswissenschaft zu lösen sein werden. Für diese Fragen hat das BVerfG in seinen Entscheidungen „Recht auf Vergessen I + II" kürzlich wichtige Leitlinien vorgegeben. Dort hat das Gericht entschieden, dass primär die deutschen Grundrechte Prüfungsmaßstab für nationales Recht sind, welches der Durchführung von europäischem Recht dient, wenn der europäische Normgeber dem nationalen Gesetzgeber einen Umsetzungsspielraum einräumt, solange die nationalen Grundrechte den gleichen Schutzstandard aufweisen, wie die europäischen Grundrechte.[52] Gibt es dagegen keinen Umsetzungsspielraum, sind die europäischen Grundrechte der entscheidende Maßstab. Allerdings behält sich das BVerfG auch in diesen Fällen vor, in Kooperation mit dem EuGH das nationale Recht an den europäischen Grundrechten zu messen.[53] Da das BVerfG diese Differenzierung hinsichtlich einzelner Normen vornimmt, wird es bei den einzelnen Bestimmungen der Richtlinie

---

49 Zum aktuellen (Still-)Stand des Beitrittsverfahrens: *Ambos,* Internationales Strafrecht, 5. Aufl. 2018, § 10 Rn. 7 ff.

50 Zur bisherigen h.M. der Geltung der EMRK als einfaches Bundesgesetz: BVerfGE 128, 326 (367); *Safferling,* Internationales Strafrecht, § 13 Rn. 20; *Kreicker,* in: Sieber/Satzger/v. Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2. Aufl. 2014, S. 904 jeweils m.w.N.; zur völkerrechtsfreundlichen Auslegung des GG: BVerfGE 128, 326 (367 f.); *Safferling,* Internationales Strafrecht, 2011, § 13 Rn. 22 f.; *Ambos,* Internationales Strafrecht, 5. Aufl. 2018, § 10 Rn. 4; *Kreicker,* in: Sieber/Satzger/v. Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2. Aufl. 2014, S. 904 jeweils m.w.N.; zur „intensiveren" Berücksichtigung der EMKR im Strafrecht bereits *Safferling,* Internationales Strafrecht, § 13 Rn. 24.

51 EuGH Rs. C-617/10 Rn. 29; vgl. auch *Esser,* in: Sieber/Satzger/v. Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, 2. Aufl. 2014, S. 955 mw.N.

52 BVerfG Beschl v 06.11.2019- 1 BvR 16/13 und Beschl v 06.11.2019 -1 BvR 276/17.

53 BVerfG Beschl v 06.11.2019- 1 BvR 16/13 und Beschl v 06.11.2019 -1 BvR 276/17.

darauf ankommen, ob diese einen Umsetzungsspielraum aufweisen, oder nicht.

4. Die Automatisierung der Datenverarbeitung im Strafverfahren

Die immense Menge an Daten, die in vielen Strafverfahren auszuwerten ist, kann heute in vielen Fällen nicht mehr manuell durch Ermittlungspersonen selbst erfolgen. Häufig würde eine manuelle Auswertung so viel Zeit in Anspruch nehmen, dass eine Kollision mit dem Beschleunigungsgrundsatz zu befürchten wäre. Daher muss vermehrt auf Softwarelösungen zur Datenauswertung und ggf. -verknüpfung zurückgegriffen werden, um verfahrensrelevante Informationen aus den Daten zu extrahieren und durch Verknüpfung zu generieren. Durch die Automatisierung der Auswertung großer Datenmengen und insbesondere durch die Verknüpfung verschiedener Datensätze können dabei sehr viel präzisere Persönlichkeits- und Bewegungsprofile generiert und Informationen über soziale Netzwerke und Kommunikationsstrukturen erlangt werden. Dies hat eine weitere Intensivierung der Betroffenheit der Datenschutzgrundrechte zur Folge[54], was sowohl Auswirkungen auf die Verhältnismäßigkeit bei der Anwendung bestehender Eingriffsbefugnisse (z.B. §§ 98a, 98c StPO) hat, als auch für neuartige automatisierte Ermittlungswerkzeuge (z.B. das sog. forensische Web Mining[55]) in vielen Fällen eine neue und eigene Rechtsgrundlage bedingt.[56]

a) Anforderungen an Funktionsweise und Transparenz

Bislang zu wenig beleuchtet beim Einsatz von Software zur Datenauswertung im Strafverfahren sind die strafverfahrensrechtlichen Anforderungen an Funktionsweise und Transparenz solcher Programme. Damit die Ergebnisse der Datenauswertung eine hinreichende Tatsachengrundlage für die Begründung eines Tatverdachts sind und einen Beweiswert zum Nachweis der Schuld haben können, muss die verwendete Software den wissen-

---

54 *Rückert*, ZStW 129 (2017), 302 (326 ff.).
55 *Rückert*, ZStW 129 (2017), 302 (307).
56 *Rückert*, ZStW 129 (2017), 302 (329 ff.); jetzt auch Meyer-Goßner/*Schmitt*, StPO, 62. Aufl. 2019, § 163 Rn. 28a; KMR-StPO/*Noltensmeier-von Osten*, 92. Lfg., § 163 Rn. 17.