KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Anna Bildner

Zugriff auf und Auswertung von Massendaten im Strafverfahren

Ludwig-Maximilians-Universität München
Juristische Fakultät
Prof. Dr. Mark A. Zöller
Abgabedatum: 26.10.2020

Inhaltsverzeichnis

I. Der Bedeutungszuwachs digitaler Beweismittel im Strafverfahren

Die Bedeutung digitaler Daten als Beweismittel für die Strafverfolgungsbehörden wächst stetig.[1] Ein Grund für diesen Bedeutungszuwachs ist in dem Phänomen „Big Data" zu sehen. Pausenlos werden allein durch die massenhafte Verbreitung von Smartphones vielfältige Daten über die Bevölkerung erhoben und ausgewertet. Noch nie zuvor bot eine solche Menge an Informationen in ihrer Zusammenschau einen derart detailreichen Einblick in die Persönlichkeiten der Bevölkerung.[2] Insoweit ist es mehr als naheliegend, dass auch die Strafverfolgungsbehörden ein immer größeres Interesse an digitalen Daten zeigen, um diese für wertvolle Ermittlungsansätze und schließlich als Beweismittel im Strafverfahren zu nutzen.[3] Dies geht jedoch zunächst mit rechtlichen und schließlich mit technischen Herausforderungen einher, welche im Folgenden dargestellt werden. Als Einführung in die Thematik gilt es zunächst die Besonderheiten digitaler Daten als Beweise und das Phänomen „Big Data" genauer darzustellen. Anschließend wird dargelegt, inwieweit die äußerst praxisrelevante Ermittlungsmaßnahme der Sicherstellung und Beschlagnahme gem. § 94 StPO den wachsenden Datenmengen begegnen kann, ohne dabei den Grundrechtsschutz der Betroffenen aus den Augen zu verlieren. Abschließend wird anhand der ermittlungstechnischen Methoden der IT-Forensik verdeutlicht, wie die Analyse von Massendaten effektiv gelingen kann und welcher gesetzlichen Normierungen es für eine rechtskonforme Anwendung bedarf.

II. Big Data und die allgemeinen Besonderheiten digitaler Beweise

1. Allgemeine Besonderheiten digitaler Beweise

Digitale Daten weisen als Beweismittel einige Besonderheiten auf, die es im Strafverfahren zu berücksichtigen gilt.[4] Im Kern lassen sich diese auf die fehlende Körperlichkeit zurückführen.[5] Digitale Daten sind nicht durch das menschliche Auge unmittelbar wahrnehmbar[6], sondern liegen in einer Notation aus zwei Variablen 0 und 1, genannt Bits oder Qubits vor.[7] Sie sind also Zahlenfolgen, die erst nach einem mehrstufigen Dechiffrierungsprozess als Beweismittel verwertbar sind und dann z.B. ein Foto, ein Dokument oder Standortdaten ergeben.[8] Die Verwertung digitaler Beweise erfolgt in der Hauptverhandlung üblicherweise auf dem Weg des Urkunden- oder Augenscheinbeweises.[9] Der Umwandlungsprozess in die wahrnehmbaren Formate geschieht wiederum mithilfe geeigneter Werkzeuge (Hard- oder Software).[10]

Dieser Verarbeitungsprozess bringt jedoch eine hohe Manipulationsanfälligkeit und das Risiko des Datenverlustes mit sich.[11] Zwar sind Manipulationen von Beweisen kein allein digitales Phänomen, allerdings gehen die Bearbeitungsmöglichkeiten weiter als bei analogen Beweismitteln. Benötigt werden lediglich ein Bearbeitungsprogramm und rudimentäre IT-Kenntnisse, um Texte oder Bilder zu verändern.[12] Meist haben mehrere Personen Zugriff auf die Datensätze und eine stabile Internetverbindung ermöglicht den Zugriff völlig ortsungebunden, z.B. durch die

1 *Warken,* NZWiSt 2017, 289 (289).
2 *Blechschmitt*, MMR 2018, 361 (361).
3 *Blechschmitt*, MMR 2018, 361 (363).
4 *Momsen*, in: FS Beulke, 2015, S. 871 (875).
5 *Warken,* NZWiSt 2017, 449 (449).
6 *BGH*, NJW 2012, 244 (245).
7 *Warken,* NZWiSt 2017, 289 (291).
8 *Fährmann,* MMR 2020, 228 (229).
9 *Sieber*, Gutachten C zum 69. Deutschen Juristentag, 2012, S. 67.
10 *Savić*, Die digitale Dimension des Strafprozessrechts, 2020, S. 48.
11 *Momsen*, in: FS Beulke, 2015, S. 871 (877).
12 *Knopp,* ZRP 2008, 156 (157).

Nutzung von Cloudspeicherungen.[13] Diese leichte Veränderbarkeit ist ein Unsicherheitsfaktor, der die Richtigkeit der durch das Beweismittel behaupteten Tatsache in Frage stellen kann und sich dadurch auch auf den Beweiswert digitaler Daten auswirkt.[14]
Eine weitere Herausforderung ist die eindeutige Zuordnung der Daten zu konkreten Individuen aufgrund der Möglichkeit anonymen Agierens im Internet, welche z.B. durch die Nutzung von Aliasidentiäten im Darknet entsteht.[15] Die Speicherung digitaler Daten erfolgt mittlerweile zunehmend im Ausland, was Zuständigkeitsfragen aufwirft.[16] Zudem geht die Erhebung digitaler Beweismittel, insbesondere von Massendaten, mit einer spezifischen Grundrechtsrelevanz einher.[17]

2. Das Phänomen „Big Data"

Eine weitere Besonderheit digitaler Beweismittel ist das Phänomen „Big Data". Der Begriff kennt keine allgemeingültige Definition.[18] Charakteristisch für das Phänomen ist die Komplexität der Daten, welche mit den „vier V`s"[19] umschrieben wird: Volume (Datenvolumen), Velocity (Datengeschwindigkeit), Variety (Datenvielfalt) und Veracity (Datenqualität). Big Data macht es also möglich, riesige Datenmengen aus unterschiedlichen Quellen in hoher Geschwindigkeit, teilweise sogar in Echtzeit zu sammeln, zu analysieren, auszuwerten und damit Aussagen über immer mehr Lebensbereiche zu treffen.[20] Die Masse der Daten findet ihre Ursache unter anderem in der Menge unterschiedlicher Datenquellen. Längst hat sich ein Großteil unseres Lebens von der analogen in die digitale Welt verlagert: mit elektronischen Foto- und Videoaufnahmen, kommunizierender Alltagstechnik, bargeldlosem Zahlen und der Teilnahme an Social-Media-Diensten seien nur ein paar Beispiele genannt. Auch im öffentlichen Bereich werden ständig elektronische Daten etwa in der Finanzverwaltung, bei den Krankenkassen und durch die Videoüberwachung öffentlicher Plätze erhoben.[21] Außerdem gelangen immer mehr internetfähige Geräte auf den Markt (sog. Internet of Things), welche sich untereinander vernetzen, wodurch unmittelbar große Datenmengen entstehen.[22] Die Strafverfolgung steht nun vor der Herausforderung, dieser Informationsflut zu begegnen.

III. Der Zugriff auf Massendaten im Strafverfahren

Aufgrund wachsender Datenmengen gibt es „mehr Sachverhalt"[23], den es gemäß dem rechtsstaatlichen Legalitätsprinzip (§ 152 Abs. 2 StPO) umfassend zu erforschen gilt. Gleichzeitig führt der technische Fortschritt zu besseren Auswertungsmöglichkeiten der gewonnenen Daten.[24] Im Folgenden wird die Erhebung digitaler Datenmengen auf Grundlage der Strafprozessordnung (StPO) und die Auswertung der dadurch gewonnenen Informationen beleuchtet. Im Fokus steht dabei der offene Zugriff auf gespeicherte Daten gem. §§ 94 ff. StPO. Anschließend wird beantwortet, wie mit der Hilfe von IT-Forensik die Auswertung großer Datenmengen gelingen kann.

13 *Warken,* NZWiSt 2017, 289 (295).
14 *Momsen*, in: FS Beulke, 2015, S. 871 (875).
15 *Müller,* NZWiSt 2020, 96 (100).
16 *Warken,* NZWiSt 2017, 417 (421 ff.).
17 *Warken,* NZWiSt 2017, 289 (293 f.).
18 *Dorschel*, Praxishandbuch Big Data, 2015, S. 6.
19 *Dorschel*, S. 6 ff.
20 *Savić*, S. 26.
21 *Warken,* NZWiSt 2017, 329 (332).
22 *Warken*, NZWiSt 2017, 329 (333).
23 *Schneider,* ZIS 2020, 79 (80).
24 *Singelnstein,* in: Hoffmann-Riem, Big Data – Regulative Herausforderungen (2018), S. 179 (181).

1. Bisherige gesetzgeberische Entwicklungen

Um den Herausforderungen der Digitalisierung angemessen begegnen zu können, war in den letzten Jahren gerade der Bereich der Telekommunikation (§§ 100a ff. StPO) ständigen Veränderungen ausgesetzt.[25] Mit den im Sommer 2017 eingeführten Regelungen zur Quellen-TKÜ (§ 100a StPO) und der verfassungsrechtlich umstrittenen[26] Online-Durchsuchung (§ 100b StPO) wurden die strafprozessualen Befugnisse erheblich ausgeweitet und sorgten für Diskussionen.[27]

Im Bereich der auf körperliche Gegenstände zugeschnittenen Rechtsgrundlagen der Sicherstellung und Beschlagnahme (§§ 94 ff. StPO) wird den informationstechnischen Entwicklungen hingegen seit der Entstehung der StPO im Jahr 1877 trotz ihrer praktischen Relevanz[28] nur vereinzelt Rechnung getragen.[29] Exemplarisch sind hier die Vorschriften über die Rasterfahndung in § 98c StPO und § 98a StPO zu nennen.[30] Mit der Umsetzung der Cybercrime Konvention[31] des Europarates wurde außerdem § 110 Abs. 3 StPO geschaffen, wonach die Durchsicht eines elektronischen Speichermediums „auch auf hiervon getrennte Speichermedien" erfolgen darf, „soweit auf sie von dem Speichermedium aus zugegriffen werden kann". Die Konvention enthält zudem in Art. 19 Abs. 3 Regelungen zur Sicherstellung gespeicherter Computerdaten, welche ein besonderes Augenmerk auf Sicherung der Integrität der Daten legen. [32] Dies hat sich der deutsche Gesetzgeber allerdings noch nicht zum Vorbild genommen, sondern erkennt die §§ 94 ff. StPO auch in der digitalen Welt als noch ausreichend an.[33] Daran schließt sich die Frage an, ob der Rückgriff auf für analoge Beweismittel intendierte Normen dem Phänomen Big Data mit besonderem Blick auf den Grundrechtsschutz der Betroffenen überhaupt noch gerecht werden kann.

2. Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO

Sinn und Zweck der Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO ist die Sicherung des Strafverfahrens.[34] Um den Verlust von Beweismitteln zu verhindern, müssen diese in staatlichen Gewahrsam genommen werden.[35] Im Zusammenhang mit der Erhebung von Massendaten werden die Vorschriften vor allem in umfangreichen Wirtschaftsstrafverfahren bei Sicherstellung großer EDV-Systeme relevant.[36] Doch auch in anderen Bereichen finden die §§ 94 ff. StPO ihre Anwendung, etwa bei der Sicherstellung von Smartphones, welche als Beweismittel aus modernen Strafprozessen nicht mehr wegzudenken sind.[37]

a) Allgemeine Voraussetzungen

Laut § 94 Abs. 1 StPO haben die Strafverfolgungsbehörden die Befugnis zur Sicherstellung von „Gegenständen", die z.B. bei einer Durchsuchung des Beschuldigten oder Dritten (§§ 102, 103 StPO) gefunden werden, sofern diese

25 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 52. EL April (2020), Teil 19.3, Rn. 8.
26 *Gercke*, in: HK-StPO, 6. Aufl. (2019), § 100b Rn. 7; *Roggan,* StV 2017, 821 (826 ff.).
27 BGBl. 2017 I Nr. 58; dazu *Singelnstein/Derin,* NJW 2017, 2646 ff.
28 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. (2018), § 1 Rn. 1.
29 *Schilling/Rudolph/Kuntze,* HRRS 2013, 207 (209).
30 BGBl. 1992 I S. 1302.
31 Convention on Cybercrime vom 21.11.2001, ETS Nr. 185, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a. (zuletzt abgerufen am 25.10.20).
32 *Sieber/Brodowski,* in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 9.
33 BVerfGE 124, 43 (58f.).
34 *Wohlers/Greco*, in: SK-StPO, 5. Aufl. (2016), § 94 Rn. 1.
35 *Hauschild*, in: MüKo-StPO, 2014, § 94 Rn. 1.
36 *Schneider,* ZIS 2020, 79 (79); *Basar/Hièramente,* NStZ 2018, 681 (681).
37 *Wenzel,* NZWiSt 2016, 85 (86).

für die Beweisführung von Bedeutung sein können.[38] Beweisgegenstände können im Allgemeinen alle beweglichen oder unbeweglichen Sachen sein, die die Eigenschaft eines körperlichen Gegenstandes erfüllen.[39] Erst wenn die freiwillige Herausgabe verweigert wird, kann die förmliche Beschlagnahme (§ 94 Abs. 2 StPO) durch den Richter oder bei Gefahr im Verzug, durch die Staatsanwaltschaft oder ihre Ermittlungspersonen angeordnet werden (§ 98 Abs. 1 S. 1 StPO).[40] Anordnungsvoraussetzung ist lediglich der Anfangsverdacht i.S.d. § 152 Abs. 2 StPO.[41] Die Beschlagnahme darf aber keinesfalls ins „Blaue hinein" erfolgen, vielmehr bedarf es konkreter Anhaltspunkte, weshalb eine Straftat nach aktuellem Kenntnisstand zumindest möglich erscheint.[42] Schließlich darf das Objekt der Sicherstellung keinem Beschlagnahmeverbot i.S.d. § 97 StPO unterliegen.[43]

b) Daten als „Gegenstände" i.S.d. § 94 StPO

Im Jahr 1877 konnte der historische Gesetzgeber die rasante technische Entwicklung noch nicht vorhersehen, sodass die §§ 94 ff. StPO ursprünglich für analoge Beweismittel geschaffen wurden.[44] Fraglich ist, ob auch digitale Daten unter den Anwendungsbereich des § 94 ff. StPO fallen. Einigkeit besteht darin, dass § 94 StPO die Sicherstellung und Beschlagnahme von Datenträgern zulässt.[45] Umstritten ist hingegen, ob digitale Daten selbst sichergestellt werden können. Der Wortlaut „Gegenstände" ließe vermuten, dass digitale Daten aufgrund ihrer fehlenden Körperlichkeit, aus dem Anwendungsbereich auszuschließen seien, da man sonst den Wortlaut überdehne. Der Beschlagnahme unterlägen danach ausschließlich körperliche Speichermedien nicht aber die Daten selbst, diese wären keine Gegenstände i.S.d. Vorschrift.[46]
Das *BVerfG* erkennt an, dass die §§ 94 ff. StPO „zwar ursprünglich auf körperliche Gegenstände zugeschnitten seien", der „Wortsinn" des § 94 StPO gestatte jedoch auch die Einbeziehung nichtkörperlicher Gegenstände. Außerdem werde der Wortlaut schon mit Blick auf die Unterscheidung zum engeren Begriff der körperlichen Sache nicht überschritten.[47] Digital gespeicherte Informationen lägen somit innerhalb des Anwendungsbereichs.[48] Die Auslegung für die analoge Welt geschaffener Normen im digitalen Kontext erscheint zumindest fragwürdig und bringt Unsicherheiten mit sich. Insbesondere das verfassungsmäßig geforderte Gebot der Normklarheit wird dadurch berührt.[49] Die höchstrichterliche Rechtsprechung sieht § 94 StPO allerdings als hinreichend bestimmt an, sodass über § 94 StPO auch der Zugriff auf digitale Daten selbst erfolgen kann.[50] Der Streit entfaltet grundsätzlich „eher theoretischen Charakter und weniger praktische Relevanz"[51], da in der Ermittlungspraxis ohnehin zumeist physische Trägermedien sichergestellt werden, welche problemlos unter den Gegenstandsbegriff subsumiert werden können.[52] Es gilt trotzdem festzuhalten, dass der Zugriff auf umfassende Datenbestände gem. § 94 StPO lediglich auf Grundlage eines Anfangsverdachts damit unter den „denkbar geringsten Voraussetzungen"[53] möglich ist.

38 *Sieber/Brodowski*, in Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 71.
39 *Gercke*, in: HK-StPO, § 94 Rn. 8.
40 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl. (2020), § 94 Rn. 13.
41 *Gercke*, in: HK-StPO, § 94 Rn. 31.
42 *Greven*, in: KK-StPO, 8. Aufl. (2019), § 94 Rn. 8.
43 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 20.
44 *Jahn/Brodowski*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren (2020), S. 67 (72).
45 *Gercke*, in: HK-StPO, § 94 Rn. 17.
46 *Gercke*, in: HK-StPO, § 94 Rn. 18; *Kemper*, NStZ 2005, 538 (541); *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. (2017), § 43 Rn. 4; *Bär*, Handbuch zur EDV-Beweissicherung, 2007, Rn. 407; *Roggan*, NJW 2015, 1995 (1999).
47 BVerfGE 124, 43 (63).
48 BVerfGE 113, 29 (51 f.); *BVerfG*, NJW 2006, 976 (980); *BVerfG*, NJW 2009, 2431 (2434).
49 *Ludewig,* KriPoZ 2019, 293 (296).
50 BVerfGE 113, 29 (51 f.); BVerfGE 115, 166 (191 ff.).
51 *Bär*, Rn. 407.
52 *Gercke*, in: HK-StPO, § 94 Rn. 18.
53 *Singelnstein,* NStZ 2012, 593 (597).

c) Beschlagnahme von Telekommunikationsdaten

Ein spezielles Problem ist die Frage, inwiefern auf Grundlage des § 94 StPO eine Beschlagnahme von Telekommunikationsdaten erfolgen kann. Die Problemstellung lässt sich am Kommunikationsmedium der E-Mail erläutern. Dafür muss zwischen drei Mediums-Zuständen unterschieden werden: Die E-Mail kann sich erstens noch im laufenden Übertragungsvorgang befinden, zweitens noch bei Sender oder bereits beim Empfänger befinden oder drittens beim Anbieter zwischengespeichert sein.[54] Nach der Rechtsprechung des *BVerfG*[55] gehören Daten, die sich in der zweiten Phase befinden zu den sicherstellungsfähigen Gegenständen i.S.d. § 94 StPO, wenn diese bei Sender- oder Empfänger gespeichert sind. Der Kommunikationsvorgang hat dann noch nicht begonnen oder ist bereits abgeschlossen. Die Daten befinden sich damit im Herrschaftsbereich der Kommunikationsteilnehmer, die dann selbst über eine Speicherung oder Löschung der Daten entscheiden, sodass lediglich das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG berührt ist.[56]

Befindet sich die E-Mail noch im laufenden Übertragungsvorgang ist Art. 10 Abs. 1 GG betroffen. Das Grundrecht schützt die Vertraulichkeit der Kommunikation und soll sicherstellen, dass die Grundrechtsträger ohne Vorbehalte kommunizieren können.[57] Die Datenerhebung erfolgt dann durch Ausleitung während des Kommunikationsvorgangs. Dies geschieht durch einen heimlichen und damit besonders intensiven Grundrechtseingriff, der nur auf Basis des § 100a StPO und seinen strengeren Voraussetzungen erfolgen kann.[58] Komplizierter ist der Zugriff auf beim Provider zwischengespeicherte Daten.

Das *BVerfG* sieht in dieser Phase den Schutzbereich des Art. 10 Abs. 1 GG ebenfalls als eröffnet an und nimmt damit eine Erweiterung dessen vor.[59] Jede Kenntnisnahme kommunikativer Daten stelle ohne Einwilligung des Betroffenen einen Grundrechtseingriff dar.[60] Die Auslagerung der E-Mails auf den nicht im Herrschaftsbereich des Nutzers liegenden Server des Providers habe nicht automatisch das Einverständnis des Nutzers eines Drittzugriffs zur Folge.[61] Aus diesem Mangel an Beherrschbarkeit ergebe sich vielmehr eine besondere Schutzbedürftigkeit, welche eine Verlängerung des Grundrechtsschutzes rechtfertige.[62] Trotz der Eröffnung des Schutzbereichs des Art. 10 Abs. 1 GG, betrachtet das *BVerfG* die §§ 94 ff. StPO als verfassungsmäßige Ermächtigungsgrundlage für diesbezügliche Grundrechtseingriffe.[63] Bisher war es einhellige Ansicht, dass die alleinige Rechtsgrundlage für Eingriffe in Art. 10 Abs. 1 GG in § 100a StPO zu sehen sei.[64] Die Eröffnung des Schutzbereiches von Art. 10 Abs. 1 GG schloss die Anwendung des § 94 StPO aus. Das *BVerfG* argumentiert nun, solange der Eingriff in Art. 10 Abs. 1 GG offen und punktuell erfolge, sei dieser durch § 94 StPO hinreichend gerechtfertigt.[65] Damit erfolgt die Bestimmung der Rechtsgrundlage nicht anhand des betroffenen Schutzbereichs, sondern anhand der Offen- oder Verdecktheit der geplanten Maßnahme.[66] Somit kann der offene Zugriff auf E-Mails, die beim Provider zwischengespeichert sind nach § 94 StPO erfolgen. Eine Katalogtat wie bei einem Zugriff nach § 100a StPO muss nicht vorliegen.[67] Diese Argumentation kann nicht überzeugen. Für den Nutzer ist es so letztendlich unerheblich, ob

54 *Singelnstein*, NStZ 2012, 593 (596); unabhängig davon, ob man den Prozess insgesamt in 3, 4 oder 7 Phasen unterteilt vgl. dazu *Brodowski,* JR 2009, 402.
55 *BVerfG*, NJW 2009, 2431 (2433).
56 BVerfGE 115, 166 (Ls. 1).
57 BVerfGE 85, 386 (389); BVerfGE 100, 313 (363).
58 *Singelnstein,* NStZ 2012, 593 (595).
59 BVerfGE 124, 43 (56).
60 BVerfGE 85, 386 (398).
61 *BVerfG*, MMR 2009, 673 (675).
62 BVerfGE 124, 43 (72).
63 BVerfGE 124, 43 (58 ff.).
64 *Krüger,* MMR 2009, 673 (682).
65 BVerfGE 124, 43 (58 ff.).
66 *Singelnstein,* NStZ 2012, 593 (596); *Kasiske,* StraFo 2010, 228 (230 f.); *Klein,* NJW 2009, 2996 (2998).
67 *Kasiske,* StraFo 2010, 228 (232).

seine Nachrichten durch Art. 10 Abs. 1 GG geschützt sind, wenn auf diese unter den deutlich einfacheren Voraussetzungen des § 94 StPO zugegriffen werden kann und der Schutz dadurch geschwächt wird.[68] Es ist außerdem nicht plausibel, dass für einen einheitlichen Kommunikationsvorgang je nach Phase andere Eingriffsvoraussetzungen gelten sollten. Richtigerweise müsste immer § 100a StPO einschlägig sein.[69] Die dargelegte Rechtsprechung lässt sich auch auf anderen Formen der Telekommunikation übertragen, bei denen eine Speicherung erfolgt.[70] Dazu gehören die Daten eines Nutzerkontos in sozialen Netzwerken sowie Cloud-Inhalte.[71] Folgt man der Ansicht des *BVerfG*, ist die Erhebung von umfassenden Kommunikationsdaten in der Praxis sowohl beim Beschuldigten als auch im Zwischenspeicher des Providers, nach § 94 StPO allein unter der Voraussetzung des Anfangsverdachts möglich. Die fehlende Beschränkung auf Seite der Rechtsgrundlage muss folglich durch die Begrenzung anhand verfassungsrechtlicher Grundsätze ausgeglichen werden.[72]

3. Grundrechtliche Grenzen des § 94 StPO

Die Strafverfolgung ist gem. Art. 1 Abs. 3 GG an die Grundrechte gebunden. Maßnahmen nach § 94 können also potentiell in verschiedene Grundrechte eingreifen.[73] Sofern nicht das speziellere Grundrecht der Telekommunikationsfreiheit gem. Art. 10 Abs. 1 GG eingreift[74], bildet im Bereich der Datenerhebung das allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 GG die Basis des grundrechtlichen Schutzes. Dieser Schutz wird bei der Sicherstellung umfangreicher Datenmengen durch das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. I Abs. 1 GG verstärkt[75], welches die Befugnis des Einzelnen umfasst, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[76]. Der Schutzumfang beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden, sondern umfasst auch personenbezogene Daten, die für sich genommen nur einen geringen Informationsgehalt haben.[77] Aufgrund der umfassenden technischen Möglichkeiten gäbe es kein „belangloses Datum“[78]; auch eine für sich unwichtige Information kann im Zusammenspiel mit anderen Informationen Rückschlüsse auf den Betroffenen zulassen.[79] Noch nicht abschließend geklärt ist welche Bedeutung dem subsidiären Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht)[80], welches sich ebenfalls aus Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG herleiten lässt, für § 94 StPO zukommt.[81]

a) Besondere Eingriffsintensität der Maßnahme

Eine Maßnahme nach § 94 StPO geht aufgrund der Vielzahl vorzufindender Daten und der daraus folgenden großen Streubreite des Informationsgehalts regelmäßig mit einer besonderen Eingriffsintensität einher. Von der Da-

68 *Krüger*, MMR 2009, 673 (683).
69 *Roxin/Schünemann*, § 36 Rn. 6; *Wohlers/Greco*, in: SK-StPO, § 94 Rn. 27.
70 *Singelnstein,* NStZ 2012, 593 (597).
71 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 16b; *Blechschmitt,* MMR 2018, 361 (364).
72 *Singelnstein,* NStZ 2012, 593 (597).
73 *Gercke*, in: HK-StPO, § 94 Rn. 4.
74 BVerfGE 124, 43 (Ls. 1).
75 BVerfGE 113, 29 (45).
76 BVerfGE 65, 1 (Ls. 1)
77 BVerfGE 120, 274 (312); vgl. BVerfGE 118, 168 (184 f.).
78 BVerfGE 65, 1 (45).
79 *Di Fabio,* in: Maunz/Dürig-GG, 91. EL (April 2020), Art. 2 I Rn. 174.
80 BVerfGE 120, 274 (Ls. 1).
81 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 66.

tenbeschlagnahme sind häufig nicht allein der Beschuldigte, sondern regelmäßig auch Dritte, etwa der Kommunikationspartner oder Zugangsberechtigte, wie Kommunikationsdienstleister, in ihren Grundrechten betroffen, auch wenn sie in keiner Beziehung zum Tatvorwurf stehen.[82] Auch der Umfang des erlangten Datenvolumens intensiviert die Eingriffstiefe.[83] Während eine einzelne Information zum Aufenthaltsort des Beschuldigten keine besonderen Rückschlüsse erlaubt, kann eine hinreichend große Zahl von zeitbezogenen Daten die Erstellung eines ganzen Bewegungsprofils ermöglichen. Auch die Erhebung von Daten aus dem Browserverlauf oder die Kenntnisnahme durchgeführter Downloads, kann den Betroffenen in seinen Lebensbereichen stark berühren.[84] Ein weiterer Einflussfaktor auf die Eingriffsintensität ist die Offen- oder Verdecktheit einer Maßnahme. Heimliche Eingriffe unterliegen aufgrund der fehlenden Einflussmöglichkeiten des Betroffenen einer höheren Rechtfertigung.[85] § 100e Abs. 2 S. 1 StPO normiert daher für die Onlinedurchsuchung (§ 100b StPO), dass ihre Anordnung durch die zuständige Kammer am Landgericht erfolgen muss. Bei Gefahr im Verzug kann der Vorsitzende entscheiden (§ 100e Abs. 2 S. 2 StPO), nicht aber die Staatsanwaltschaft und ihre Ermittlungspersonen, wie dies gem. § 98 Abs. 1 S. 1 StPO bei § 94 StPO der Fall ist. Für Eingriffe gem. § 100b StPO muss außerdem der Verdacht einer besonders schweren Straftat gem. § 100b Abs. 2 StPO vorliegen. Begründet wird die niedrigere Eingriffsschwelle für § 94 StPO damit, dass dieser nur offene und punktuelle Eingriffe erlaubt. Führt man sich aber die umfassenden Datenmengen, welche auf Grundlage des § 94 StPO z.B. aus einem Smartphone ausgelesen werden können vor Augen, besteht hinsichtlich des möglichen Umfangs der gewonnenen Daten zumindest eine Nähe zur Online-Durchsuchung.[86]

b) Anforderungen an den Verhältnismäßigkeitsgrundsatz

Die besondere Eingriffsintensität des § 94 StPO erfordert eine besondere Achtung des Verhältnismäßigkeitsgrundsatzes, welcher als übergeordnete Regel staatlichen Handelns auch im Strafverfahren gilt.[87] Vor allem im Beschlagnahmerecht kommt dem Grundsatz aufgrund der weiten Formulierungen im Gesetzestext erhebliche Bedeutung zu.[88] Die Sicherstellung muss daher zur Erreichung ihres Zwecks geeignet und erforderlich sein und in einem angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen.[89] Aus gleich geeigneten Maßnahmen ist stets diejenige mit der geringsten Grundrechtsbeeinträchtigung zu wählen.[90] Dabei ist vor allem die Beschränkung des zulässigen Umfangs der Datenbeschlagnahme in sachlicher, inhaltlicher und zeitlicher Hinsicht von Bedeutung.[91]

aa) Begrenzung auf verfahrensrelevante Daten

Der Grundsatz der Verhältnismäßigkeit begrenzt auch das rechtsstaatliche Legalitätsprinzip (§ 152 Abs. 2 StPO).[92] Es ist daher die verfassungsrechtliche Aufgabe der Strafverfolgungsbehörden den Zugriff auf verfahrensrelevante

82 Vgl. BVerfGE 100, 313 (380); BVerfGE 107, 299 (320f.).
83 Vgl. BVerfGE 113, 29 (55 ff.).
84 *Warken,* NZWiSt 2017, 289 (293).
85 *BVerfG*, NJW 2007, 2464 (2469f.).
86 *Ludewig,* KriPoZ 2019, 293 (297) m.V.a. *Momsen,* DRiZ 2018, 140 (143).
87 BVerfGE 20, 162 (187).
88 *Menges*, in: LR-StPO, 27. Aufl. (2019), § 94 Rn. 51.
89 BVerfGE 20, 162 (186); *Köhler,* in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 18.
90 *Grzeszick*, in: Maunz/Dürig-GG, Art. 20 VII Rn. 113.
91 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 91.
92 BVerfGE 44, 353 (373).

Gegenstände zu beschränken.[93] Im Zeitalter von Big Data fällt es jedoch immer schwerer zwischen relevanten und irrelevanten Daten zu unterscheiden, sodass die Gefahr überschießender Beweisgewinnung entsteht.[94] Um eine umfassende Sachverhaltsaufklärung zu ermöglichen und keine beweisrelevanten Daten zu übersehen, gehen Ermittler in der Praxis oft nach der „Staubsaugermethode“[95] vor. Dies wiegt besonders schwer, wenn unbeteiligte Dritte von der Maßnahme betroffen sind.[96] Die Lösung dieses Problems steht vor praktischen Schwierigkeiten: Zum einen ist eine Trennung relevanter Daten von irrelevanten Daten schon aufgrund der fehlenden körperlichen Teilbarkeit schwer möglich. Außerdem ist den Daten ihr Inhalt nicht von außen anzusehen.[97] Ist noch nicht absehbar, inwieweit die Daten strafrechtlich relevante Informationen enthalten, können sie nicht gem. § 94 StPO sichergestellt werden. Hier kommt die vorläufige Sicherstellung gem. § 110 StPO ins Spiel, welche gerade auf die Feststellung potentieller Beweismittel abzielt[98] und laut *BVerfG* eine Begrenzung auf verfahrensrelevante Daten somit erst möglich mache.[99] Die Norm erlaubt die Durchsicht von „Papieren“ auf ihre Beweisrelevanz, um zu einem späteren Zeitpunkt über eine Beschlagnahme zu entscheiden.[100] Damit geht die Anwendung der Norm ähnlich der Handhabung bei § 94 StPO über den Wortlaut hinaus.[101] Um den praktischen Bedürfnissen der Staatsanwaltschaft gerecht zu werden, werden auch Unterlagen in Form digitaler Daten vom Begriff „Papiere“ umfasst.[102] Das *BVerfG* sieht in § 110 StPO eine mildere Maßnahme gegenüber der Beschlagnahme, da sie lediglich einen vorübergehenden Eingriff zur Feststellung der Beweiserheblichkeit bezweckt. Die Beschlagnahme wirkt hingegen bis zum Verfahrensabschluss, wodurch der staatliche Zugriff intensiviert würde.[103] Aufgrund des weiten Ermessensspielraums[104] erfolgt in der Praxis regelmäßig ein umfassender Zugriff auf den gesamten Datenbestand, was zu einer „vollständigen Durchleuchtung“[105] des Betroffenen führt. Über § 110 Abs. 3 StPO kann außerdem der Zugriff auf Cloud-Daten legitimiert werden, sofern sie vom Datenspeicher aus erreichbar sind und sich im Inland befinden.[106] Sieht man den Schwerpunkt des Eingriffs in der Offenlegung der Daten und nicht in dem vorübergehenden Datenentzug ist § 110 StPO gegenüber § 94 Abs. 2 StPO keinesfalls die mildere Maßnahme.[107] Die Eingriffstiefe wird zudem verstärkt, wenn der Datenträger aufgrund von Verschlüsselungen oder aufgrund des Datenvolumens in die Diensträume der Behörden mitgenommen werden müssen.[108] Die Durchsicht muss dann zügig geschehen.[109] Auch § 110 StPO rückt damit in die Nähe der verdeckten Maßnahmen. Zwar ist die Maßnahme dem Einzelnen bekannt und damit eine richterliche Überprüfung gem. § 98 Abs. 2 StPO möglich, allerdings zeigen die fehlende sachliche und zeitliche Begrenzung der Durchsicht sowie das nur vage zugestandene Anwesenheitsrecht[110], dass ihr wesentliche Gesichtspunkte einer offenen Maßnahme fehlen.[111] Folglich kann § 110 Abs. 1 StPO zwar den Umfang der beschlagnahmten Daten reduzieren, das Ausmaß der offengelegten Informationen ist jedoch ebenfalls enorm. Die Durchsicht der Daten darf dabei nur von der Staatsanwaltschaft und ihren Ermittlungspersonen (§ 152 GVG) durchgeführt werden, § 110 Abs. 1 StPO. In der Praxis sind dies meist eigens ausgebildete und

93 BVerfGE 113, 29 (Ls. 2).
94 Vgl. *BVerfG,* NJW, 2005, 1917, (1920 ff.).
95 *Basar/Hièramente,* NStZ 2018, 681 (681).
96 *Warken,* NZWiSt 2017, 289 (293).
97 *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt (2017), S. 265 (271).
98 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 2.
99 *BVerfG*, NJW 2005, 1917 (1921).
100 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 2.
101 *Ludewig,* KriPoZ 2019, 293 (298).
102 Vgl. BVerfGE 113, 29 (51).
103 *BVerfG*, NJW 2005, 1917 (1921).
104 Vgl. *BGH*, NJW 1995, 3397 (3397).
105 *Peters,* NZWiSt 2017, 465 (473).
106 *Gercke,* in: HK-StPO, § 110 Rn. 16.
107 *Peters,* NZWiSt 2017, 465 (468).
108 *Ludewig,* KriPoZ 2019, 293 (298).
109 *BGH*, NStZ 2003, 670 (671).
110 Für eine gesetzliche Festschreibung *Peters*, NZWiSt 2017, 465 (469 ff.).
111 Vgl. *Peters,* NZWiSt 2017, 465 (469).

erfahrene Ermittlungspersonen im Bereich der IT-Forensik.[112] Bei fehlender Expertise ist allgemein anerkannt, dass die Staatsanwaltschaft im Stadium der Durchsicht, im Falle besonders spezieller und unbekannter Sachverhalte auf externe EDV-Sachverständige zurückgreifen darf (§§ 161 Abs.1, S. 1, 72 ff. StPO).[113] Eine eigenverantwortliche Durchsicht der Daten durch den externen Sachverständigen ist jedoch unzulässig.[114]

bb) Kopieren von Daten als eingriffsschwächere Methode?

Die Beschlagnahme kann entweder durch die Mitnahme des physischen Datenträgers oder durch die Erstellung einer Kopie erfolgen.[115] Dabei stehen sich zwei Prinzipien gegenüber. Zum einen fordert das Unmittelbarkeitsprinzip als Prozessmaxime, dass bei sachlichen Beweisen – zu denen auch Datenträger und Daten zählen – die Tatsachen aus der Quelle selbst geschöpft werden müssen und grundsätzlich keine Beweissurrogate genügen.[116] Das Beweismittel ist daher stets im Original zu sichten.[117] Bei Kopien schwinge ein gewisses Verfälschungsrisiko mit, was den Beweiswert der Daten schwächen könne.[118] Dies spräche dafür Datenträger stets selbst zu beschlagnahmen. Mit der körperlichen Sicherstellung und dem damit verbundenen Nutzungsentzug geht jedoch ein zusätzlicher Grundrechtseingriff in Art. 14 Abs. 1 GG einher.[119] Können IT-Systeme eines Unternehmens für einen längeren Zeitraum nicht genutzt werden, kann dadurch enormer wirtschaftlicher Schaden entstehen. Dem Verhältnismäßigkeitsgrundsatz ist deshalb auch mit Blick auf den Nutzungsentzug Rechnung zu tragen, was für die Erstellung einer Sicherungskopie spricht. Allerdings gilt es zunächst zu klären, inwieweit es rechtmäßig ist, Sicherungskopien zu erstellen.[120] Dazu müsste § 94 Abs. 1 StPO neben dem Zugriff auf die Originaldaten auch das Anfertigen von Kopien dieser Daten erlauben.[121]

Der Wortlaut „in Verwahrung nehmen“ umfasst nur die tatsächliche Mitnahme der Datenträger. *Bär*[122] sieht in der Anfertigung einer Sicherungskopie eine Sicherstellung „in anderer Weise“ gem. § 94 Abs. 1 StPO. Der Zweck der Maßnahme, die Herstellung staatlicher Sachherrschaft über den Beweisgegenstand zur Verfahrenssicherung, könne auch ohne Mitnahme des IT-Systems selbst gelingen. Dies ist überzeugend. Auch bei analogen Beweismitteln ist das Erstellen von Abbildern nicht konkret im Wortlaut des § 94 StPO geregelt, trotzdem ist es üblich Fotokopien von Beweisgegenständen anzufertigen.[123] Nicht jedes Minus zu einer Eingriffshandlung bedarf auch der Erwähnung im Gesetz, dies wäre nicht praktikabel, wollte man alle möglichen Ermittlungsmaßnahmen erfassen.[124] Zudem ist es mittlerweile technisch möglich, ein identisches Duplikat von Daten anzufertigen, wodurch das Verfälschungsrisiko deutlich gesenkt wird.[125] Auch das *BVerfG* sieht das Erstellen von Kopien als gleich effektive Maßnahme an und bezeichnet dieses Vorgehen mit Blick auf den Verhältnismäßigkeitsgrundsatz als vorzugswürdiges milderes Mittel.[126] Sicherungskopien anzufertigen ist damit als „Minus-Maßnahme“[127] grundsätzlich zulässig und verfassungsmäßig geboten.[128]

112 *Wenzel*, NZWiSt 2016, 85 (87).
113 *Bruns*, in: KK-StPO, § 110 Rn. 4; *Wenzel,* NZWiSt 2016, 85 (87).
114 *Bruns*, in: KK-StPO, § 110 Rn. 4; *Wenzel*, NZWiSt 2016, 85 (87).
115 *Basar*, in: FS Wessing, 2015, S. 634 (640).
116 *Fischer,* in: KK-StPO, Einleitung, Rn. 20.
117 *Warken,* NZWiSt 2017, 449 (450).
118 *Basar*, in: FS Wessing, 2015, S. 634 (641).
119 *Axer*, in: BeckOK-GG, 44. Ed. (Stand: 15.08.2020), Art. 14 Rn. 64.
120 *Heinson*, IT-Forensik, 2015, S. 215.
121 *Kemper,* NStZ 2005, 538 (541 f.).
122 *Bär*, Rn. 416.
123 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 16.
124 *Menges*, in: LR-StPO, § 94 Rn. 63.
125 *Bär,* Rn. 416.
126 *BVerfG,* NJW 2005, 1917 (1921).
127 *Gercke*, in: HK-StPO, § 94 Rn. 22.
128 *Menges*, in: LR-StPO § 94 Rn. 4; *Möhrenschlager,* wistra 1991, 321 (329); *Roxin/Schünemann*, § 34 Rn. 4; *Sieber*, S. 66.

c) Kernbereich privater Lebensgestaltung

Neben dem Verhältnismäßigkeitsgrundsatz ist der Schutz des Kernbereichs privater Lebensgestaltung als zweite Grenze staatlicher Eingriffe von wesentlicher Bedeutung. Definiert wird dieser als letzter unantastbarer Bereich menschlicher Freiheit, welcher der Einwirkung staatlicher Gewalt, auch in Abwägung mit dem Informationsbedürfnis der Strafverfolgungsbehörden, nicht zugänglich ist.[129] Sein Schutz ist Ausdruck der in Art. 1 Abs. 1 GG verankerten Menschenwürdegarantie[130] und unterliegt keiner Verhältnismäßigkeitsprüfung, sodass kein Eingriff in den Kernbereich gerechtfertigt werden kann. Lediglich der inhaltliche Umfang des Schutzes ist der Auslegung zugänglich.[131] Mit Blick auf den Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst der Kernbereich Angaben über Personen, die dem Staat zur Kenntnis gelangen können.[132] Damit werden die Möglichkeit innere Vorgänge wie Empfindungen und Gefühle sowie Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen sowie die vertrauliche Kommunikation mit anderen geschützt.[133] Die zunehmend starke Verflechtung von Informationstechnik mit dem Lebensalltag hat zur Folge, dass sich höchstpersönliche Erlebnisse auch digital abbilden lassen. Insoweit wird es sich bei der Auswertung von großen Datenmengen kaum vermeiden lassen, auch kernbereichsrelevante Daten, wie z.B. Informationen zur Sexualität[134], zu erfassen.[135] Es bedarf daher Vorkehrrungen, die eine staatliche Kenntnisnahme sensibler Daten vermeiden.[136] Das praktische Problem liegt jedoch darin, dass erst eine Kenntnisnahme des Aussagegehalts der Daten, also eine Verletzung des Kernbereichs, die Beurteilung der Kernbereichsrelevanz ermöglicht.[137] Um dem zu begegnen wird im Vorhinein versucht aus dem Kontext von Daten Schlüsse auf deren Inhalt zu ziehen. Betreffzeilen von E-Mails oder Namen von Ordnern können dafür Hinweise liefern. [138] Eine staatliche Kenntnisnahme kann so jedoch leicht durch entsprechende Bezeichnung der Daten vermieden werden. Die Erhebung von Kernbereichsdaten lässt sich folglich, besonders im Zeitalter von Big Data, nicht vollständig vermeiden ohne staatliche Ermittlungen dadurch teilweise unmöglich zu machen.[139] Aufgrund der Unvorhersehbarkeit des Inhalts der Daten lässt das *BVerfG* eine umfangreiche Erhebung grundsätzlich zu.[140] Diesem Umstand begegnete der Gesetzgeber bei der Online-Durchsuchung (§ 100b StPO) mit der Einführung des § 100d Abs. 3 StPO. Danach ist technisch soweit wie möglich sicherzustellen, die Erhebung kernbereichsrelevanter Daten zu vermeiden bzw. unverzüglich zu löschen. Trotz ähnlicher Eingriffstiefe, was Umfang und Informationsgehalt betrifft, fehlt eine solche Regelung für die §§ 94 ff. StPO.

d) Zwischenergebnis

Die Beschlagnahme digitaler Daten gem. § 94 StPO stellt trotz der Offenheit und einem nur punktuellen Zugriff einen intensiven Grundrechtseingriff dar. Die Norm erlaubt trotz ihres Wortlauts den Zugriff auf körperliche Datenträger sowie auf digitale Daten selbst, wovon auch jegliche Form von gespeicherten Kommunikationsdaten umfasst ist. Der Anfangsverdacht als materielle Voraussetzung für die Anwendung des § 94 StPO bildet für einen

129 BVerfGE 109, 279 (313).
130 BVerfGE 109, 279 (Ls. 2).
131 *Desoi/Knierim,* DÖV 2011, 398 (402, 404).
132 *Heinson*, S. 189.
133 BVerfGE 109, 279 (313).
134 BVerfGE 109, 279 (314).
135 BVerfGE 120, 274 (336).
136 *Heinson*, S. 189.
137 BVerfGE 109, 279 (313).
138 *Heinson*, S. 189.
139 Vgl. *Czerner*, in: Labudde/Spranger, S. 265 (274).
140 BVerfGE 113, 348 (392).

solch weitgehenden Eingriff die denkbar niedrigste Schwelle. Um die grundrechtlichen Vorgaben zu erfüllen besteht die Notwendigkeit verfahrensmäßiger Vorschriften, wie konkrete Regelungen zur Beschränkung der Erhebung verfahrensunerheblicher Daten sowie Daten aus dem Kernbereich privater Lebensgestaltung.

IV. Die Auswertung von Massendaten im Strafverfahren – Der Einsatz von IT-Forensik

Konnten digitale Daten gem. § 94 StPO rechtmäßig sichergestellt werden, folgt die genaue Untersuchung der beweisrelevanten Daten. Dafür werden in der Praxis die Methoden der IT-Forensik eingesetzt.[141]

1. Begriffsbestimmung

Aufgabe der Forensik ist es, mit modernster Technik und der Unterstützung von Experten, Spuren zu analysieren und so den Tathergang möglichst genau zu rekonstruieren.[142] Zur Behandlung digitaler Spuren hat sich die IT-Forensik als ein Teilgebiet der allgemeinen Forensik, welches auf IT-Systeme spezialisiert ist, herausgebildet.[143] Da die Forensik keine eigene Wissenschaft darstellt, sondern sich je nach Untersuchungsauftrag der Methoden unterschiedlicher wissenschaftlicher Disziplinen bedient, soll eine allgemeine Definition benutzt werden: IT-Forensik ist die Sicherung und Analyse von Daten aus IT-Systemen mit wissenschaftlichen Methoden zur Beweisführung vor Gericht.[144]

2. IT-Forensik im Ermittlungsverfahren

Die Vorgehensweise der IT-Forensik lässt sich grob in drei Schritte einteilen: ordnungsgemäße Sicherung, Analyse und verständliche Präsentation der Daten vor Gericht (secure, analyse, present; kurz: S-A-P).[145]

a) Beweiswertwahrung als Ziel der IT-Forensik

Zweck der Sicherstellung gem. § 94 StPO ist wie bereits erwähnt die Verfahrenssicherung. Gelingt dieser Schritt, erfolgt in der Hauptverhandlung die Bewertung der digitalen Beweismittel aufgrund einer freien richterlichen Beweiswürdigung (§ 261 StPO). Das Gericht ist dabei an keine Beweisregeln gebunden, die vorschreiben, wann eine Tatsache als erwiesen gilt oder welchen individuellen Wert ein Beweis hat.[146] Im Hinblick auf die Manipulationsanfälligkeit ist die Bestimmung des Beweiswerts von Daten jedoch schwierig.[147] Es ist daher das Ziel der IT-Forensik den Beweiswert der Daten während der Sicherung und Auswertung zu erhalten und sie vor Integritätsverletzungen zu schützen.[148] Um dies zu erreichen arbeitet die IT-Forensik mit Methoden der gerichtsfesten Sicherung und Analyse digitaler Spuren, wobei sachgerechte Kopie und Auswertung der Daten von großer Bedeutung sind.[149]

---

141 Grundlegend zur IT-Forensik *Heinson* (Fn. 119).
142 *Savić*, S. 291 m.w.N.
143 *Heinson*, S. 16.
144 *Heinson,* S. 17.
145 *Heinson,* S. 25.
146 *Eisenberg*, Beweisrecht der StPO, 10. Aufl. (2017), III. Rn. 88.
147 *Sieber*, S. 68.
148 *Heinson*, S. 4.
149 *Sieber*, S. 68.

b) Übliche Methoden der Sicherung

Während in der analogen Welt Untersuchungen überwiegend am Original stattfinden, wird in der digitalen Welt üblicherweise eine Sicherungskopie angefertigt.[150] In der Praxis erfolgt dies regelmäßig durch die sog. Spiegelung, bei der eine bitweise 1:1 Kopie erfolgt. Der Datenträger wird dabei ausgelesen und auf einem Zweiten abgespeichert.[151] Dabei entsteht ein identisches Duplikat, an welchem sodann verschiedene Untersuchungsschritte ausgeführt werden können, ohne die Originaldaten zu verändern.[152] Außerdem können mehrere Personen denselben Datenträger nach unterschiedlichen Gesichtspunkten und Methoden durchsuchen.[153] So kann ein Ergebnis jederzeit überprüft und das Risiko von Veränderungen der Datenbasis vermieden werden.[154] In der Praxis stößt diese Technik im Umgang mit Massendaten an Grenzen.[155] Aufgrund des zunehmenden Datenvolumens muss zum einen ausreichend Kapazität für forensische Duplikate zur Verfügung stehen, zum anderen kann die Auslesung einen enormen zeitlichen Mehraufwand bedeuten.[156] Außerdem muss in rechtlicher Hinsicht stets die Verhältnismäßigkeit der Datensicherung bedacht werden. Wie bereits dargestellt, darf es aufgrund der Zweckgebundenheit strafprozessualer Ermittlungsmaßnahmen nicht zu einem Komplettzugriff kommen.
Sind Daten nicht auf einem lokalen Speicher gesichert, sondern auf Servern von Drittanbietern, ist eine Spiegelung nicht möglich. Stattdessen wird mit einer Live-Sicherung ein direkter, nicht nur lesender Zugriff durch Softwareanwendung auf die Daten vorgenommen.[157] Die Live-Sicherung hat jedoch die große Schwäche, dass sie stets Veränderungen im System nach sich zieht und damit die Integrität der Daten verletzt.[158] So können z.B. die sog. Metadaten[159] verwischt werden. Auch bei der Live-Sicherung ist eine Selektion der Daten aufgrund zeitlicher und ressourcentechnischer Grenzen nur schwer möglich.[160]

c) IT-forensische Massendatenanalyse

Um der zunehmenden Komplexität und dem Umfang digitaler Daten angemessen zu begegnen werden spezielle forensische Massendatenanalysemethoden entwickelt. Dabei werden Daten auf kriminelle Handlungen hin untersucht, um diese aufzudecken, nachzuweisen oder bestimmte Muster zu erkennen.[161] Dafür stehen unterschiedliche Analysemethoden zur Verfügung. Bei regelbasierten Analysen werden bestimmte Muster als Grundlage genommen, diese Muster müssen erfüllt sein, um relevante Daten zu identifizieren. Nach der inhaltlichen Erarbeitung werden die Daten in einen Algorithmus überführt und abschließend näher untersucht.[162] Eine weitere Möglichkeit ist der Einsatz lernender Systeme („Machine Learning“). Der Begriff meint die Fähigkeit Künstlicher Intelligenz[163] (KI), basierend auf der Grundlage großer Datenmengen, die zugrundeliegenden Algorithmen zu entwickeln und

150 *Freiling/Sack,* DUD 2014, 112 (112).
151 *Schilling/Rudolph/Kuntze,* HRRS 2013, 207 (211).
152 *Heinson*, S. 31.
153 Leitfaden IT-Forensik des Bundesamts für Sicherheit in der Informationstechnik, 2011, S. 26, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 25.10.2020).
154 BVerfGE 120, 274 (325); *Bär*, Rn. 417.
155 *Freiling/Sack*, DuD 2014, 112 (113).
156 Leitfaden IT-Forensik, 2011, S. 28.
157 *Basar/Hieramente,* NStZ 2018, 681 (682).
158 *Heinson*, S. 43.
159 Metadaten beschreiben die Eigenschaften der eigentlichen Daten und sind selbst spurlos veränderbar, *Heinson*, S. 4.
160 *Basar/Hièramente* NStZ 2018, 681 (683).
161 *Sauermann,* StraFo 2018, 449 (503).
162 *Sauermann*, StraFo 2018, 449 (503).
163 Eine gute Orientierung über den Begriff der Künstlichen Intelligenz und den Anwendungsmöglichkeiten für die Strafrechtspflege bieten *Staffler/Jany*, ZIS 2020, 164 ff.

diese zu trainieren, um anhand bereits vorhandener Datenauswertungen Aussagen für die Zukunft zu treffen.[164] Sie generieren ihr Wissen also aus historischen Datensätzen.[165] Durch entsprechende Softwareanwendungen lassen sich digitale Datenmengen elektronisch vorselektieren wodurch die Masse der zu sichtenden Daten reduziert wird.[166] Allerdings muss berücksichtigt werden, dass bei einer maschinellen Vorselektierung aufgrund der großen Datenmengen auch Unbeteiligte betroffen sein können. Schließlich besteht die Gefahr, dass umfassende Persönlichkeitsprofile von Bürgern erstellt werden.[167] Die grundrechtliche Schutzwirkung der informationellen Selbstbestimmung gilt auch für den Datenverarbeitungsprozess, sodass es gerade für die maschinelle Auswertung von Beweismitteln einer Ermächtigungsgrundlage bedarf.[168] Bei der Entwicklung von forensischen Methoden zur Vorselektierung muss es darüber hinaus das Ziel sein, so viele Daten wie nötig zu sichern, um dem Legalitätsprinzip gerecht zu werden und gleichzeitig so wenige Daten wie möglich zu erheben, um das Verhältnismäßigkeitsprinzip und das Verbot überschießender Beweisgewinnung zu wahren. Für die zu selektierende Datenmenge ergibt sich daher, dass diese relevant und erlaubt sein muss.[169] Trotz dieser verfassungsrechtlichen Bedenken ist die aktuelle Situation unbefriedigend. Mit der Hilfe von Selektierungsmethoden wäre eine Prüfung der vorhandenen Daten viel effektiver möglich. Gerade bei großen Datenmengen besteht die Gefahr, dass wichtige Beweise übersehen werden.[170] Dieses Risiko könnte erheblich minimiert werden. Rechtlich ist ein solches System jedoch nur umsetzbar, wenn der Gesetzgeber klare Grenzen für eine verhältnismäßige Verwendung der Systeme definiert und dies nicht der Praxis überlässt.[171]

An dieser Stelle soll außerdem nicht unerwähnt bleiben, dass die Staatsanwaltschaften im Rahmen ihrer Ermittlungstätigkeit vermehrt dazu tendieren, zur Auswertung digitaler Daten die Hilfe privater IT-Forensik Dienstleister in Anspruch zu nehmen, indem diese förmlich als Sachverständige bestellt werden (§§ 72 ff. StPO).[172] Die Aufträge beziehen sich häufig auf die Auswertung sensibler Kommunikationsdaten, die zuvor im Zuge umfangreicher Beschlagnahmemaßnahmen sichergestellt wurden.[173] In diesem Zusammenhang stellt sich zum einen die Frage, ob die Staatsanwaltschaft überhaupt im Wege der Sachverständigenbeauftragung auf die Dienste privater IT-Forensiker zurückgreifen darf oder ob es sich bei derartigen Tätigkeiten nicht vielmehr um genuine Ermittlungsarbeit handelt, die ausschließlich der Staatsanwaltschaft und ihren Ermittlungspersonen obliegt.[174] Daran schließt sich außerdem die Frage an, ob originär hoheitliche Ermittlungsaufgaben überhaupt auf Private übertragen werden können.[175] Dies kann an dieser Stelle jedoch nicht vertieft werden.

d) Ein Blick in die Praxis: Forschungsprojekt ZAC NRW

Wie durch eine Ermittlungssoftware Datenreduktion gelingen kann zeigt ein Beispiel aus der Praxis: Seit August

164 *Staffler/Jany,* ZIS 2020 164 (166).
165 *Sauermann,* StraFo 2018, 449 (503).
166 *Fährmann,* MMR 2020, 228 (232).
167 *Singelnstein,* NStZ 2012, 593 (606).
168 *Fährmann,* MMR 2020, 228 (232).
169 *Freiling/Sack,* DuD 2014, 112 (117).
170 *Fährmann,* MMR 2020, 228 (232).
171 *Fährmann*, MMR 2020, 228 (232f.); *Schneider* ZIS 2020, 79 (82).
172 Dieses Vorgehen war erstmals in Zusammenhang mit Ermittlungen wegen Verbreitung, Erwerb und Besitz kinderpornografischer Schriften (§ 184b StGB) zu beobachten, siehe https://www.spiegel.de/netzwelt/web/outsourcing-privatermittler-sichten-beweise-bei-kinderporno-anklagen-a-533078.html (zuletzt abgerufen am 10.3.21), dazu auch die Antwort der Bundesregierung auf eine Kleine Anfrage von Abgeordneten der FDP-Bundestagsfraktion, BT Drs. 16/8335, S. 1; vgl. dazu *Braun/Roggenkamp*, NK 2012, 141 (141 ff.); diese Methoden finden aber zunehmend auch in komplexen Wirtschaftsstrafverfahren Anwendung, ausführlich zu dieser aktuellen Problematik *Wackernagel/Graßie*, NStZ 2021, 12 (12 ff.).
173 *Wackernagel/Graßie*, NStZ 2021, 12 (12).
174 Im Ergebnis für den Großteil aller Fälle ablehnend *Wackernagel/Graßie*, NStZ 2021, 12 (13 ff.).
175 Für unzulässig haltend *Wackernagel/Graßie*, NStZ 2021, 12 (16 ff.); insbesondere kann nicht auf die Ermittlungsgeneralklausel (§ 161 Abs. 1 StPO) als gesetzliche Grundlage zurückgegriffen werden *Wenzel*, NZWiSt 2016, 85 (86).

2019 forscht das Justizministerium Nordrhein-Westfalen gemeinsam mit der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) [176] in Zusammenarbeit mit der Microsoft GmbH Deutschland und verschiedenen Experten zur Bekämpfung von Kinderpornografie im Internet anhand Analysemethoden Künstlicher Intelligenz.[177] Die unüberschaubare Menge des vorhandenen Untersuchungsmaterials wird derzeit noch manuell durch die Ermittler gesichtet. Immer besteht die Gefahr, dass dabei strafrechtlich relevante Bilder leicht in der Masse harmloser Dateien untergehen. Zudem sind die Ermittler bei der Sichtung enormen psychischen Belastungen ausgesetzt.[178] Die manuelle Ermittlung ist daher sowohl in zeitlicher als auch personeller Hinsicht wenig zweckmäßig.[179] Durch automatische Bilderkennung mit Hilfe eines Algorithmus soll kinderpornografisches Material erkannt und von sonstigen Dateninhalten getrennt werden.[180] Durch diese Datenselektion soll zum einen eine Beschleunigung der Datenauswertung, zum anderen eine Reduktion auf die verfahrensrelevanten Bilddateien erreicht werden. Der reduzierte Datensatz wird schließlich von den Ermittlern analysiert. Eine Herausforderung des Projekts liegt darin, durch die Weiterleitung der Daten zur Analyse an Dritte nicht selbst den Tatbestand der Verbreitung und des Besitzes kinderpornografischer Schriften gem. §§ 184b ff. StGB zu verwirklichen.[181] Diese Sorge wurde durch eine Komprimierung der Daten gelöst. Die Bilder sind zwar für die Software verwertbar, für Menschen hingegen nicht sichtbar.[182] Das Forschungsprojekt zeigte bereits Wirkung: Im September 2020 wurden bei Durchsuchungen von Tatverdächtigen in ganz Deutschland wegen des Verdachts auf Besitz und Verbreitung von Kinderpornografie (§ 184b StGB) Beweismittel sichergestellt, welche auf den bisherigen Auswertungen der ZAC gründen.[183] Das Potential solcher Systeme kann allerdings nur ausgeschöpft werden, wenn die Maßnahme auf einem festem Rechtssystem mit klaren Regeln für die Verwendung baut.[184]

An dieser Stelle lohnt sich außerdem ein Blick über die innerdeutschen Grenzen hinaus: innerhalb der Europäischen Union ist die Verbesserung der Ermittlungstätigkeiten der Strafverfolgungsbehörden durch den Einsatz von KI bereits seit Jahren ein Forschungsschwerpunkt.[185] Im Rahmen der Forschungsförderung *Horizon 2020*[186] werden zahlreiche Projekte gefördert, die speziell die Unterstützung der Strafverfolgungsbehörden durch innovative Technologien, wie Blockchain Analyse, Big-Data Analyse oder den Einsatz von KI und Machine Learning betreffen.[187] Diese Entwicklung ist nur zu begrüßen.

e) Problem: Fehlende rechtliche Vorgaben

Trotz weitreichender technischer Möglichkeiten finden diese bislang noch kaum Wiederhall in den Vorgaben der Strafprozessordnung.[188] Zu den wenigen Regelungen gehört § 100a Abs. 5 StPO, der sich allerdings nur auf die Quellen-TKÜ und gem. § 100b Abs. 4 StPO auf die Onlinedurchsuchung bezieht. Auch § 496 Abs. 2 StPO enthält

176 https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html(zuletzt abgerufen am 25.10.20).
177 https://www.land.nrw/de/pressemitteilung/kuenstliche-intelligenz-im-kampf-gegen-kinderpornographie (zuletzt abgerufen am 25.10.2020).
178 https://www.tagesspiegel.de/politik/depressionen-oder-psychosen-drohen-auswertung-von-kinderpornos-fuer-ermittler-eine-zumutung/25898696.html (zuletzt abgerufen am 25.10.20).
179 *Staffler/Jany,* ZIS 2020, 164 (169).
180 https://news.microsoft.com/de-at/features/automatische-bilderkennung-hilft-im-einsatz-gegen-kinderpornografie/ (zuletzt abgerufen am 25.10.20).
181 Zu dieser Problematik *Rückert/Goger,* MMR 2020, 373 ff.
182 https://www.handelsblatt.com/technik/forschung-innovation/cyberkriminalitaet-mit-kuenstlicher-intelligenz-will-die-justiz-kinderpornografie-bekaempfen/24871714.html?ticket=ST-806263-B7mZL7HfFVMTyPz9ffWq-ap3 (zuletzt abgerufen am 25.10.20).
183 https://www.presseportal.de/blaulicht/pm/12415/4694676 (zuletzt abgerufen am 25.10.20).
184 *Staffler/Jany,* ZIS 2020, 164 (169).
185 Siehe dazu EU Research for a Secure Society, Fighting crime and terrorism, including cybercrime, migration and home affairs, European Union, 2019, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/fba6e440-1f89-11e9-8d04-01aa75ed71a1/language-en (zuletzt abgerufen am 10.3.21); *Gercke*, ZUM 2019, 789 (803).
186 https://ec.europa.eu/programmes/horizon2020/en/h2020-sections-projects (zuletzt abgerufen am 10.3.21).
187 Mit der Nennung einiger Projektbeispiele *Gercke*, ZUM 2019, 789 (803).
188 *Basar*, in: FS Wessing, 2015, S. 634 (639); vgl. *Blechschmitt,* MMR 2018, 361 (364).

Vorgaben, die wiederum sehr allgemein gehalten sind und nur von den „erforderlichen organisatorischen und technischen Maßnahmen“ (§ 496 Absatz 2 Nr. 1 StPO) und „Grundsätzen einer ordnungsgemäßen Datenverarbeitung“ (§ 496 Absatz 2 Nr. 2 StPO) sprechen. Auch aus den §§ 483 ff. StPO folgen keine Regelungen zur Authentizitätsicherung der Daten.[189] Anhaltspunkte für konkrete Regelungen lassen sich dem Leitfaden IT-Forensik[190] des Bundesamts für Sicherheit und Informationstechnik (BSI) entnehmen.[191] Auch wenn die Vorgaben nicht rechtsverbindlich sind, können sie den Behörden als Orientierung dienen. Die Legislative ist daher aufgerufen, in dem höchst grundrechtsrelevanten Bereich der strafrechtlichen Ermittlungsbefugnisse klare gesetzliche Rahmenbedingungen für die technische Auswertung digitaler Daten zu schaffen, um so der Verhältnismäßigkeit Rechnung zu tragen und eine effektive Strafverfolgung zu ermöglichen.[192] Die Maßstäbe des „Leitfadens IT-Forensik“ bieten hierfür eine gute Grundlage.[193]

3. Zwischenergebnis

Der IT-Forensik ist es gelungen, technische Verfahren und Methoden für einen gekonnten Umgang mit digitalen Daten zu etablieren. In der Praxis erfolgt eine Orientierung an Leitfäden. Die wachsenden Kompetenzen werden in den Fachabteilungen (ZAC) im BKA und den LKA gebündelt.[194] Um die technischen Möglichkeiten, besonders im Bereich der Massendatenanalyse voll im Strafverfahren nutzen zu können, braucht es jedoch konkrete gesetzliche Vorschriften für die Auswertung digitaler Beweise und den Einsatz derartiger Software.

V. Reformbedarf

1. Beschränkende Eingriffsgrundlagen

Die vorangegangenen Ausführungen zeigen, dass § 94 StPO nur bedingt dazu geeignet ist, die intensiven Grundrechtseingriffe, die sich bei der Erhebung großer Datenmengen ergeben zu rechtfertigen.
Die tiefgreifenden Eingriffe stützen sich auf eine Ermächtigungsgrundlage, die seit 1877 beinahe unverändert besteht, was einen Anpassungsbedarf offenbart.[195] Die schlichte Übertragung einer Befugnis aus der analogen in die digitale Welt kann gesetzgeberisches Handeln nur vorübergehend ersetzen[196] und wird mit der Weiterentwicklung technischer Möglichkeiten nur zu mehr Unsicherheiten für die Rechtsanwender führen.[197] Die Forderung nach Normenklarheit ist keine Prinzipienreiterei, sondern für einen Rechtsstaat unerlässlich.[198] Vertraut man allein auf die verfassungskonforme Anwendung des § 94 StPO, wird dem Risiko von Grundrechtsverletzungen nur unzureichend begegnet. Gerade allgemeine Prinzipien wie der Verhältnismäßigkeitsgrundsatz erzielen im Verhältnis zu konkreten Regelungen im Tatbestand nur eine geringe Wirkung.[199] Daher wäre es mehr als sinnvoll, die An-

189 *Fährmann,* MMR 2020, 228 (231).
190 Leitfaden IT Forensik des Bundesamts für Sicherheit in der Informationstechnik, 2011, (Fn. 152).
191 *Schneider,* ZIS 2020, 79 (82).
192 Vgl. *Fährmann,* MMR 2020, 228 (231).
193 *Basar,* in: FS Wessing, 2015, S. 634 (647); *Sieber*, S. 127; *Fährmann,* MMR 2020, 228 (231); *Schneider,* ZIS 2020, 79 (82).
194 https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html (zuletzt abgerufen am 25.10.20).
195 *Ludewig,* KriPoZ 2019, 293 (297).
196 *Roggan,* NJW 2015, 1995 (1999).
197 Vgl. auch *Sieber*, S.14.
198 *Peters,* NZWiSt 2017, 465 (472).
199 *Singelnstein,* NStZ 2012, 593 (606).

forderungen, die sich aus dem Grundgesetz, speziell aus dem Verhältnismäßigkeitsgrundsatz, ergeben im Gesetzestext klarzustellen.[200] Schon das *BVerfG* setzte fest, dass der Gesetzgeber den Grundrechtsschutz bei staatlichen Ermittlungshandlungen durch Anpassung bestehender oder Schaffung ergänzender Regelungen effektiv sichern muss.[201] Während das *BVerfG* die Anforderungen an die Verhältnismäßigkeit im Bereich des Gefahrenabwehrrechts bereits stärker konturiert hat[202], steht dies im Strafverfahrensrecht noch aus.[203]

Die Beschlagnahme gem. § 94 Abs. 2 StPO erlaubt den Zugriff auf einen umfassenden Datenbestand, was bis zur Zusammensetzung eines Persönlichkeitsprofils führen kann. Damit geht die Maßnahme, welche als Grundlage nur den Anfangsverdacht erfordert, weit über ihren ursprünglichen Zweck hinaus. Dies lässt § 94 StPO zu einer „Super-Ermächtigungsgrundlage[204]“ für die Beweisgewinnung werden. Dem muss im Hinblick auf die Grundsätze der Zweckbindung und der Datensparsamkeit, welche mit dem Phänomen Big Data immer größere Relevanz entfalten, unbedingt entgegengewirkt werden. Außerdem erscheint eine ausdrückliche einfach gesetzliche Regelung zum Schutz des Kernbereichs persönlicher Lebensgestaltung aufgrund der Nähe zur Online-Durchsuchung notwendig. Als Vorbild kann § 100d StPO herangezogen werden. [205]

2. Regelungen zur Auswertung digitaler Daten

Darüber hinaus benötigt die StPO dringend konkrete Vorgaben zur Sicherung der Authentizität digitaler Daten, um diese nicht in ihrem Beweiswert zu schwächen.

Dafür werden verschiedene Maßnahmen vorgeschlagen, die sich auch im Leitfaden IT-Forensik wiederfinden: Um Verfälschungen auszuschließen, sollte der Datenverarbeitungsprozess chronologisch in Protokollen dokumentiert werden. So kann nachvollzogen werden, woher die Daten stammen und wie sie aus dem IT-System gewonnen wurden.[206] Die Integrität kann weiterhin mit einer frühzeitigen Erstellung von sogenannten Hashwerten gesichert werden. [207] Jede Datei hat einen individuellen Hashwert, der sich bei einer Manipulation verändert.[208]

Wurde ein Hashwert genommen, kann dieser mit dem Hashwert des Datensatzes im Strafverfahren jederzeit verglichen werden. Stimmen die Werte überein, kann eine Veränderung mit großer Sicherheit ausgeschlossen werden.[209] Durch ein Zugangssystem für die gespeicherten Daten sollte zudem garantiert werden, dass nur berechtigten Personen Zugriff auf die Daten erhalten. Dies trüge dem Grundrechtsschutz Rechnung und ließe erkennen, wer Zugang zu den Daten hatte.[210] Jeder Verarbeitungsschritt sollte reproduzierbar sein, weshalb Kopien für die Auswertung der Daten erstellt werden sollten, um stets einen unveränderten Datensatz zur Verfügung zu haben.[211] Da es sich bei im Strafverfahren relevanten Daten meist um sehr sensible Daten handelt, sind diese zudem durch ein besonderes Speicherungssystem vor dem Zugriff Unberechtigter zu sichern.[212] Es ist besorgniserregend, wenn sensible Daten auf privaten Servern, etwa bei Amazon, gespeichert werden.[213] Mit Blick auf die wachsenden Datenmengen sollte außerdem geprüft werden, wie forensische Massendatenanalyseverfahren die Ermittlungsarbeit

200 *Heinson*, S. 404.
201 *BVerfG*, NJW 2005, 1338 (Ls. 3).
202 BVerfGE 141, 220 (263 ff.).
203 *Singelnstein,* in: Hoffmann-Riem, S. 179 (181).
204 *Roggan,* NJW 2015, 1995 (1997).
205 *Ludewig,* KriPoZ 2019, 293 (299).
206 *Heinson*, S. 144 f.
207 *Müller,* NZWiSt 2020, 96 (100).
208 Hinsichtlich der technischen Grundprinzipien: *Erbguth,* MMR 2019, 654 (655).
209 *Heinson*, S. 149 f.
210 *Fährmann,* MMR 2020, 228 (230) m.V.a. Leitfaden IT-Forensik, 2011, S. 23.
211 *Heinson*, S. 147.
212 *Sieber*, S. 67 f.
213 https://netzpolitik.org/2019/bundespolizei-speichert-bodycam-aufnahmen-weiter-bei-amazon/ (zuletzt abgerufen am 25.10.20).

durch Datenreduktion und Datenselektion effektiver gestalten können, ohne eine unverhältnismäßige Beeinträchtigung von Grundrechten zu verursachen. Das Projekt der ZAC NRW liefert dafür erste Anhaltspunkte.

VI. Fazit

Im Laufe der letzten Jahre wurde die StPO immer mehr an die Herausforderungen der digitalen Welt angepasst. Dabei wurden jedoch die für körperliche Gegenstände zugeschnittenen Eingriffsgrundlagen der §§ 94 ff. StPO vom Gesetzgeber nicht ausreichend berücksichtigt. Das Resultat: Aufkommende Probleme mussten in der Praxis anhand möglichst verfassungskonformer Anwendung der Vorschriften und auf Grundlage teils widersprüchlicher Rechtsprechung gelöst werden. Eine solche Vorgehensweise wird jedoch der vielen Besonderheiten, die mit digitalen Daten im Strafverfahren verbunden sind, nicht gerecht.[214] Wie der Mathematiker *Norbert Wiener (1894-1964)* passend formulierte: „Information is information, not matter or energy. No materialism which does not admit this can survive at the present day".[215] Für die Rechtswissenschaften bedeutet dies, die noch anerkannte Praxis, für körperliche Gegenstände intendierte Ermittlungsbefugnisse auf digitale Daten anzuwenden, mit Blick auf technische Weiterentwicklungen kritisch zu hinterfragen. Für den Gesetzgeber ergibt sich daraus der dargestellte Handlungsbedarf.

Hierbei sollten zudem die Möglichkeiten der IT-Forensik berücksichtigt werden. Der Auswertung von Massendaten kommt dabei mit Blick auf Datenselektion und Datenreduktion eine besondere Bedeutung zu. Das Potential digitaler Ermittlungsmethoden mit zunehmenden Datenmengen ist evident und die Auseinandersetzung damit letztendlich unumgänglich.[216] Der Staat muss mit den technischen Entwicklungen Schritt halten und sich die daraus resultierenden Ermittlungsmethoden zu Nutze machen, damit auch in Zukunft eine effektive Strafverfolgung gelingen kann. Der digitale Fortschritt ist derart rasant, dass für staatlichen Organe im Zeitalter des Phänomens Big Data eine qualitative sowie quantitative Überforderung droht.[217] Vor den Konsequenzen einer solchen Überlastung ist der einzelne Grundrechtsträger unter allen Umständen zu schützen.

214 Vgl. *Sieber*, S. 14.
215 Zitiert nach *Sieber*, S. 14.
216 *Staffler/Jany* ZIS 2020, 164 (169).
217 *Eschelbach*, Big Data im Strafprozess, Vortrag 2016, letzte Seite.