Auswirkungen der Digitalisierung auf das Ermittlungsverfahren

Impulse aus der Strafverteidigungspraxis

Von Dr. **Frédéric Schneider**, Hamburg*

I. Einleitung

„Alles was digitalisiert werden kann, wird digitalisiert". Ganz diesem Zitat der ehemaligen CEO des Hewlett-Packard-Konzerns, Cara Fiorina, entsprechend, machen technische Fortschritte selbstverständlich auch vor dem Strafrecht nicht halt. Und anstatt digitale Neuerungen pauschal zu verteufeln, tun Strafrechtler angesichts der rapiden technischen Entwicklungen unserer Zeit gut daran, deren Auswirkungen und Vereinbarkeiten mit dem Strafrecht zu untersuchen.

Um ein Gefühl dafür zu bekommen, wie weit gefächert die Implikationen der Digitalisierung auch für das Strafrecht sind, reicht bereits ein Blick auf die vielen in dieser Sonderausgabe der ZIS behandelten Themen. Darüber hinaus drücken neue Formen der Kriminalität und damit einhergehend neue Straftatbestände auch der Strafverteidigung ihren Stempel auf.[1] So ergibt sich bereits aus dem Entstehungsdatum des StGB, dass die mit Hilfe etwa des Computerbetrugs gemäß § 263a StGB oder der Datenhehlerei gemäß § 202d StGB erfassten Phänomene digitaler Wirklichkeit strafrechtlich erst im Nachhinein erfasst werden konnten.[2]

Daneben lassen sich in der Praxis aber angesichts der digitalen Entwicklung auch Veränderungen hinsichtlich grundlegender Säulen des Ermittlungsverfahrens beobachten. Da die Arbeit des Strafverteidigers im Wirtschaftsstrafrecht aber ganz maßgeblich in diesem Verfahrensstadium erfolgt und sich Änderungen hier zugleich auf das gesamte materielle Strafrecht auswirken, erscheint die diesbezügliche Diskussion besonders dringlich.

Aus dem Bereich des Ermittlungsverfahrens näher betrachtet werden hier im Folgenden daher die Auswirkungen der Digitalisierung auf den strafprozessualen Anfangsverdacht und die Durchsuchung von EDV-Systemen. Dabei sollen nach einer sehr kursorischen Skizze des Ermittlungsverfahrens tatsächliche Auswirkungen der Digitalisierung sowie deren aktuelle Auswirkungen in der Praxis benannt und Vorschläge für eine Anpassung der Strafprozessordnung bzw. den Umgang mit dieser dargestellt werden.

II. Rahmen und Prinzipen des Ermittlungsverfahrens

Zur Betrachtung dieser Auswirkungen der Digitalisierung auf das Ermittlungsverfahren ist es zunächst notwendig, kurz dessen Rahmen und Prinzipien in Erinnerung zu rufen.

Ausgangspunkt ist der Anfangsverdacht, d.h. es müssen konkrete Anhaltspunkte vorliegen, die es nach den kriminalistischen Erfahrungen als möglich erscheinen lassen, dass eine verfolgbare Straftat begangen wurde.[3]

Die generelle Vorgabe ist gemäß § 152 Abs. 2 StPO sodann das Legalitätsprinzip, wonach Ermittlungen erfolgen müssen. Auch wenn dieses Legalitätsprinzip auf dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG beruht, ist es nicht grundgesetzlich festgeschrieben und eröffnet dem Gesetzgeber bei der konkreten Ausgestaltung einen Spielraum.[4] Im Kern geht es darum, einen möglichst objektivierten Maßstab zu schaffen, um sicherzustellen, dass strafrechtliche Ermittlungen nicht von den subjektiven Erwägungen des Ermittelnden im Hinblick auf Tat und Täter abhängen. Gerade weil Zweckmäßigkeits- und Effektivitätserwägungen sich – trotz begrenzter Ressourcen – nicht gut mit dem Legalitätsprinzip vertragen, ist es für die Funktionsfähigkeit der Strafrechtspflege und zur Vermeidung überbordender Sozialkontrolle von großer Bedeutung, ein Dunkelfeld zwar zu erforschen, aber zugleich zu akzeptieren.[5] Dessen vollständige Erhellung ist weder geschuldet noch einlösbar.[6] Sie ist anerkanntermaßen auch nicht gewollt. Entscheidend ist vielmehr, im Hinblick auf dieses Dunkelfeld Kapazitäten dergestalt einzusetzen, dass dem Legalitätsprinzip zu größtmöglicher Verwirklichung verholfen werden kann.[7]

Mit Hilfe einzelner Ermittlungen wird im Laufe des folgenden Ermittlungsverfahrens geprüft, ob sich der Anfangsverdacht zu einem hinreichenden Tatverdacht konkretisieren lässt.[8] Besonders einschneidende der stets grundrechtsrelevanten Ermittlungsmaßnahmen sind vom Gesetzgeber dabei in spezifischen Ermächtigungsgrundlagen der StPO ausgestaltet. Andere fußen auf den Generalklauseln in den §§ 161, 163 StPO.[9] Von besonderer praktischer Bedeutung ist dabei im Wirtschaftsstrafrecht die Durchsuchung gemäß §§ 102 ff. StPO und die – sich daran anschließende – Sicherstellung und Beschlagnahme von Daten und Unterlagen gemäß der §§ 94 ff. StPO.

---

* Der *Autor* ist Partner in einer auf das Strafrecht spezialisierten Kanzlei in Hamburg.

[1] Siehe etwa *Popp*, JuS 2011, 385; vgl. auch *Gercke*, ZUM 2017, 915 (917 ff.).

[2] Näher zur Entstehungsgeschichte dieser Regelungen etwa *Mühlbauer*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 3. Aufl. 2019, § 263a Rn. 11; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 5. Aufl. 2017, § 202d Rn. 1 ff., jeweils m.w.N.

[3] Vgl. BVerfG, Beschl. v. 23.7.1982 – 2 BvR 8/82 = NStZ 1982, 430.

[4] Ausführlich zum dogmatischen Hintergrund des Legalitätsprinzips *Peters*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 152 Rn. 1 ff. m.w.N.

[5] Instruktiv zur Dunkelfeldforschung etwa *Kreuzer*, NStZ 1994, 10; *ders*., NStZ 1994, 164.

[6] Vgl. *Kölbel*, in: Knauer/Kudlich/Schneider (Fn. 4), § 160 Rn. 71 m.w.N.

[7] Vgl. *Peters* (Fn. 4), § 152 Rn. 7.

[8] *Gorf*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand 1.10.2019, § 170 Rn. 2.

[9] Zum Ganzen *Griesbaum*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 163 Rn. 1 m.w.N.

Konkretisiert sich der Anfangsverdacht durch die Ermittlungen zu einem hinreichenden Tatverdacht, ist die Staatsanwaltschaft gemäß § 170 Abs. 1 StPO grundsätzlich gehalten, Anklage zu erheben. Lässt sich der Verdacht indes nicht erhärten, stellt sie das Verfahren gemäß § 170 Abs. 2 StPO ein.

III. Was bedeutet Digitalisierung für das Ermittlungsverfahren?

Die digitale Entwicklung wirkt sich in der Praxis auf das vorstehend kursorisch skizzierte Ermittlungsverfahren in tatsächlicher Hinsicht in zweifacher Weise aus. Erstens gibt es mehr Daten und damit mehr Informationen und zweitens haben sich die technischen Möglichkeiten im Vergleich zu früher vervielfacht.

Mehr Daten bedeuten dabei „mehr Sachverhalt", wobei dies gerade nicht nur qualitativ, sondern vor allen Dingen auch quantitativ „mehr Sachverhalt" bedeutet. Der Zuwachs technischer Möglichkeiten führt wiederum zu mehr Auswertungsmöglichkeiten.

Diese Veränderungen sind faktische Gegebenheiten, mit denen man umgehen muss, und zwar unabhängig davon, ob man dem digitalen Wandel kritisch gegenübersteht oder nicht. Wer die Augen vor der technischen Entwicklung verschließt und es schließlich verpasst, erforderliche Änderungen in Bereichen des materiellen und prozessualen Strafrechts vorzunehmen, riskiert substantielle Unstimmigkeiten. Die Kohärenz des Systems Strafrecht ist aber auch aus Sicht eines Strafverteidigers ein hohes Gut, trägt sie doch ganz erheblich zu Akzeptanz und Vorhersehbarkeit bei. Stete Anpassungen des Systems an die Lebenswirklichkeit erscheinen mithin für alle Beteiligten sinnvoll.

Statt einer Diskussion über gegebenenfalls erforderliche Anpassungen und einer darauf aufbauenden einheitlichen, strukturierten Vorgehensweise der Ermittlungsbehörden erleben wir in der Verteidigungspraxis hingegen häufig das Gegenteil. Scheinbar aus Überforderung, mit der schieren Masse an Daten und Auswertungsmöglichkeiten umzugehen, werden Ermittlungen nicht mehr konsistent geführt. Zwar ergibt sich auch hieraus häufig beträchtliches Verteidigungspotential, doch kann dies – auch aus Verteidigerperspektive – letztlich nicht die sinnvolle Antwort auf eine sich digitalisierende Gesellschaft sein.

Als Beitrag für die mithin erforderliche Suche nach dieser Antwort werden im Folgenden einige Impulse für erforderliche Anpassungen gegeben.

IV. Auswirkungen der digitalen Entwicklung auf den Anfangsverdacht

Dass aufgrund der digitalen Entwicklung immer mehr Daten existieren und jene angesichts der technischen Entwicklung immer schneller analysiert werden können, führt zu einer immer häufigeren Annahme eines Anfangsverdachts.

Wie dargelegt hat jener eine sehr geringe Annahmeschwelle und liegt bereits vor, wenn tatsächliche Umstände es nach kriminalistischer Erfahrung für möglich erscheinen lassen, dass eine verfolgbare Straftat begangen wurde.[10] Gerade im Bereich des Wirtschaftsstrafrechts liegt eine Vielzahl an Daten aber bereits ohne Durchführung irgendwelcher Ermittlungsmaßnahmen vor. Die derzeit in aller Munde befindlichen Cum-Ex-Transaktionen etwa waren nicht geheim, sondern vielmehr vorab der BaFin angezeigt und über Börsen abgewickelt worden. Den Sozialversicherungsträgern liegt eine Vielzahl an Daten hinsichtlich der Versicherten vor, die etwa im Hinblick auf eine mutmaßliche Bestechlichkeit im Gesundheitswesen gemäß § 299a StGB oder ein Vorenthalten und Veruntreuen von Sozialversicherungsbeiträgen gemäß § 266a StGB geeignet sein können, einen Anfangsverdacht zu begründen. Im Bereich des Steuerstrafrechts haben Betriebsprüfer einen umfassenden Zugriff auf Unternehmensdaten. Aus den zunehmenden technischen Möglichkeiten wiederum folgt ein immer schnellerer Erstzugriff auf diese Daten.

Nun könnte man in einem ersten Zugriff davon ausgehen, diese immer neuen Möglichkeiten seien für die Ermittlungsbehörden ausschließlich eine willkommene Hilfe bei der Verbrechensbekämpfung. Wie eingangs geschildert, greift aber mit Feststellung eines Anfangsverdachts das Legalitätsprinzip, wonach Ermittlungen erfolgen müssen. Reine Zweckmäßigkeitserwägungen, etwa unzureichende Kapazitäten, vermögen hieran nichts zu ändern. Gerade in den besonders datenintensiven Bereichen des Wirtschaftsstrafrechts, in denen sich aus den vorstehenden Gründen häufig ein Anfangsverdacht ergibt, sind diese Ermittlungen aber erfahrungsgemäß besonders personal- und zeitintensiv. Eine Überforderung der Ermittlungsbehörden und unangemessen lange Bearbeitungszeiten sind die Folge.[11] Gerade für den Beschuldigten, über dem mit Anfangsverdacht das Damoklesschwert des Strafverfahrens schwebt, ist diese Situation nur schwer erträglich.

Eine im Gesamtsystem unangemessene Kriminalisierung datenintensiver Bereiche sowie eine fehlende Steuerungsmöglichkeit der Allokation von Kapazitäten ist darüber hinaus geeignet, die Idee eines erforderlichen Dunkelfeldes auszuhöhlen.

In einigen Bereichen reagieren die Ermittlungsbehörden auf diese Entwicklung bereits seit vielen Jahren faktisch mit Augenmaß. Nur so lässt sich etwa erklären, dass es in der Praxis verhältnismäßig selten zu Verurteilungen wegen Insolvenzverschleppungen kommt, wenn diese nicht zu sehr großen Schäden der Gläubiger geführt haben oder gar mit Betrugstaten einhergingen.[12] Viel häufiger sind trotz der genannten Schwierigkeiten in der Praxis aber gegenläufige Tendenzen zu beobachten. Neben der Ausweitung des sog. Vorermittlungsverfahrens und dem gezielten Einsatz von Software auch zur Ermittlung eines Anfangsverdachts finden

[10] Siehe Fn. 3.

[11] Vgl. zur besonderen Dauer und zum Umfang von datenintensiven Ermittlungsverfahren im Wirtschaftsstrafrecht ebenfalls *Peters*, NZWiSt 2017, 465.

[12] Vgl. zum kaum bestehenden Dunkelfeld im Rahmen der Insolvenzverschleppung *Hohmann*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 7, 3. Aufl. 2019, InsO § 15a Rn. 6 m.w.N.

sich in der Praxis etwa immer mehr Beamte, die sich durch eine Weitergabe von Informationen an Ermittlungsbehörden vor dem Risiko einer Strafvereitelung im Amt gemäß § 258a StGB schützen wollen.[13] Diese Sorge ist dabei so präsent, dass im Hinblick auf die Betriebsprüfer beispielsweise ein Anwendungserlass zu § 10 BpO existiert, der den Umgang mit Verdachtsmomenten zur Vermeidung strafrechtlicher Risiken für die Prüfer konkretisiert.[14]

Ausgehend von der eingangs geschilderten Bedeutung des Dunkelfeldes und der Notwendigkeit einer sinnvollen Allokation von Ressourcen der Kriminalitätsbekämpfung zur wirksamen Erfüllung unserer Strafzwecke brauchen wir eine Diskussion über den Inhalt und die Bedeutung des Anfangsverdachts in digitaler Zeit. Während ein solcher bislang anzunehmen war, wenn irgendwelche Anfangspunkte nach kriminalistischer Erfahrung eine verfolgbare Tat möglich erschienen ließen, existieren heute Bereiche, in denen aus vorliegenden Daten und der besonderen Weite von Straftatbeständen, etwa im Bereich der Korruption, immer entsprechende Anhaltspunkte folgen werden. Die hieraus folgende These ist, dass es einer strengeren Interpretation des Anfangsverdachtes bedarf. Nur auf diese Weise können eine Fehlallokation von Ressourcen vermieden und die Verfolgung der Strafzwecke aufrechterhalten werden. Erforderlich ist zur genauen Ausgestaltung eine intensive Diskussion in Strafrechtswissenschaft und -praxis. Möglich wäre etwa, für den Anfangsverdacht in betroffenen Bereichen nicht bereits die Möglichkeit, sondern die Wahrscheinlichkeit einer verfolgbaren Straftat zu fordern.

Eine Lösung des Problems mittels Einzelfallaugenmaß der Behörden oder über den § 153 StPO, wie sie heute häufig zu beobachten ist, ist demgegenüber rechtsstaatlich bedenklich.[15]

V. Durchsuchungen von EDV-Systemen

Erhebliche Probleme begründen für Ermittlungsbehörden erfahrungsgemäß die Durchsuchung und Auswertung von EDV-Systemen. Dabei soll es an dieser Stelle nicht um die sog. Online-Durchsuchung[16], sondern vielmehr um den praktisch besonders relevanten Fall gehen, in dem im Rahmen von Durchsuchungsmaßnahmen Datenträger sichergestellt worden sind. Der Durchsuchung von Privat- und Geschäftsräumen kommt gerade im Wirtschaftsstrafrecht eine große praktische Bedeutung zu und der Fokus liegt dabei immer mehr auf der EDV.[17] Letztere offenbart den Ermittlungsbehörden neben einer Vielzahl von Unternehmenszahlen und Dokumenten insbesondere auch Korrespondenz zwischen Beteiligten und gewinnt damit nicht nur hinsichtlich einer Konkretisierung der subjektiven Tatseite an besonderem Wert für die Ermittlungen.

Während der Gesetzgeber zwischenzeitlich immer wieder Regelungen getroffen hat, die sich mit dem Zugriff auf entsprechende Daten befassen – etwa den § 110 Abs. 3 StPO für den Umgang mit Daten, die außerhalb des Durchsuchungsortes gespeichert sind oder die Cyber-Crime-Konvention für im Ausland befindliche Daten[18] –, fehlt es an Vorgaben zur Auswertung dieser Daten. In der Praxis werden jene von den Ermittlungsbehörden regelmäßig zunächst zur Durchsicht gemäß § 110 StPO in Gänze kopiert, während die Durchsicht dann in den Räumen der Ermittlungsbehörden erfolgen soll. Diese Praxis wirft zunächst Fragen auf, inwieweit hier die richterlich kontrollierte Beschlagnahme gemäß §§ 94 ff. StPO zu Gunsten der Durchsicht gemäß § 110 StPO an Bedeutung verliert. Lange und umfassende Durchsichtsmaßnahmen beinhalten die Gefahr, sich immer wieder vom ursprünglichen Anfangsverdacht zu lösen und die Einhaltung eines verhältnismäßigen Vorgehens wird hier nicht richterlich überprüft. Verstöße hiergegen ziehen für die Ermittlungsbehörden keine Konsequenzen nach sich und können von der Verteidigung im Nachhinein nicht wirksam gerügt werden.[19] Große Bedeutung gewinnt aus Sicht der Verteidigung daher zunächst die Frage, ob für den Verteidiger bzw. den Rechtsbeistand des von der Durchsuchung betroffenen ein Anwesenheitsrecht bei dieser Durchsicht besteht.[20] Insbesondere aber ist auch an dieser Stelle noch nicht abschließend geklärt, wie mit dem aus der Digitalisierung folgenden Zustand „mehr Technik und mehr Daten“ umzugehen ist.

Mehr Technik bedeutet in diesem Zusammenhang nicht nur, dass immer mehr Speichermedien vorhanden sind, die diverse Daten sammeln (etwa Smartphones, Smartwatches, Lautsprecher mit Sprachsteuerung[21]), sondern vor allen Dingen auch, dass immer mehr Software zur Auswertung der Daten existiert und zum Einsatz gelangt. Seit das BKA mit der Rasterfahndung zur Bekämpfung der RAF die Grundlagen für technische Ermittlungsmaßnahmen gelegt hat, ist viel passiert. Mittlerweile haben sogar große Softwareanbieter die Ermittlungsbehörden und deren Erfordernis der Auswertung großer Datenmengen als relevanten Markt entdeckt und bieten speziell hierfür konzipierte Software an.[22] Deren Auswer-

[13] Kritisch zum Vorermittlungsverfahren bereits *Wölfl*, JuS 2001, 478; instruktiv hierzu *Peters* (Fn. 4), § 152 Rn. 62 ff.

[14] Gleichlautende Erlasse der obersten Finanzbehörden der Länder v. 31.8.2009 BStBl. I 2009, S. 829.

[15] Kritisch zum zunehmenden Rückgriff auf diese Regelung aus Komplexitätserwägungen ebenfalls *Peters* (Fn. 4), § 153 Rn. 3 ff.

[16] Ausführlich hierzu etwa *Soiné*, NStZ 2018, 497.

[17] Siehe zu Praxisproblemen bei der IT-Durchsuchung *Graßie/Hiéramente*, CB 2019, 191.

[18] Ausführlich zur Umsetzung der Cyber-Crime-Konvention *Gercke*, MMR 2004, 728; *ders.*, MMR 2004, 801.

[19] Eindrücklich und überzeugend zu diesen verschiedenen Kritikpunkten an der praktischen Vorgehensweise *Peters*, NZWiSt 2017, 465; vgl. ebenfalls *Basar/Hiéramente*, NStZ 2018, 681.

[20] Hierzu ebenfalls *Peters*, NZWiSt 2017, 465 (472); *Klose*, NZWiSt 2019, 93 (98).

[21] Siehe hierzu etwa die jüngste Diskussion auf der Innenministerkonferenz tagesschau.de v. 9.6.2019, abrufbar unter https://www.tagesschau.de/inland/innenminister-smart-home-geraete-101.html (4.2.2020).

[22] Ausführlich hierzu *Singelnstein*, NStZ 2018, 1; zum Einsatz der Software i2 Analyst‘s Notebook etwa *Borchers*, heise online v. 28.11.2012, abrufbar unter

tungs- und auch Vorhersagemöglichkeiten gehen dabei weit über das hinaus, was Ermittlungsbeamte auch unter Nutzung gängiger Software zu leisten vermögen. Besonders aktuell sind in dieser Hinsicht derzeit etwa Programme zur Vorhersage von Verhalten (sogenanntes „predictive policing") und solche, die lernen, selbständig Muster zu erkennen, die das Programm dann in großen Datensätzen wiedererkennen kann (sog. „machine learning").[23] Da eine derart intensive Datenverarbeitung indes besonders schwer in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 GG eingreifen kann,[24] ist es fragwürdig, wenn jene allein auf den Ermittlungsgeneralklauseln der StPO fußt. Eine Erkenntnis der zunehmenden Digitalisierung muss daher sein, dass wir eine stete Diskussion über das Erfordernis neuer, einschränkender Ermächtigungsgrundlagen in der StPO benötigen. Dabei liegt es angesichts der besonderen Grundrechtsrelevanz des Umgangs mit Daten nahe, zu fordern, dass jeder Grundrechtseingriff mit Hilfe digitaler Werkzeuge einer speziellen Ermächtigungsgrundlage bedarf. Dies muss nicht zwingend eine neue (siehe etwa §§ 94 ff. StPO für den Eingriff in Art. 10 GG bei der E-Mail-Beschlagnahme), darf aber nicht die allgemeine Ermittlungsgenehmigung aus §§ 160, 163 StPO sein.

Besonders zweischneidig ist in der Praxis der richtige Umgang mit dem Umstand, dass den Ermittlungsbehörden angesichts der Digitalisierung immer mehr Daten zur Verfügung stehen. Hier stehen sich das Legalitätsprinzip und der Verhältnismäßigkeitsgrundsatz gegenüber. Während Ersterer eine möglichst umfassende Auswertung verlangt, streitet Letzterer zumeist für einen möglichst schonenden Eingriff. Bereits im Jahr 2005 hat das Bundesverfassungsgericht diesbezüglich ausgeführt: „Bei Durchsuchung, Sicherstellung und Beschlagnahme von Datenträgern und darauf vorhandener Daten muss der Zugriff auf für das Verfahren bedeutungslose Informationen im Rahmen des Vertretbaren vermieden werden."[25]

Neben den Schwierigkeiten, die sich angesichts der – in Wirtschaftsstrafverfahren teils unvorstellbaren – Datenmengen für die Ermittlungsbehörden daraus ergeben, dass es an personeller und sachlicher Ausstattung fehlt, gewinnt man als Verteidiger häufig das Gefühl, dass die Behörden keine einheitliche Idee haben, wie die beiden vorgenannten Prinzipien im Rahmen der Auswertung in Einklang gebracht werden können. Um die Schwierigkeit und Berührungsängste zu verdeutlichen, kann man sich etwa vor Augen führen, dass der absolute Standard in deutschen Ermittlungsbehörden auch heute noch die Ermittlungsakte in Papierform ist.

Die StPO bietet an dieser Stelle jedenfalls keine Lösung und die häufig latente Sorge der Ermittler vor Datenverlust erschwert die Herangehensweise.[26] In der Folge werden die Daten immer häufiger zur Auswertung an private Dritte gegeben und damit eine besonders grundrechtsrelevante Aufgabe „outgesourct" oder die Auswertung erfolgt unzureichend, etwa sehr punktuell und nicht mehr kontextual. Nicht selten retten sich die Ermittlungsbehörden in Opportunitätserwägungen und stellen Verfahren ein. Für Strafverteidiger eröffnet eine große Datenmenge vor diesem Hintergrund häufig ein weiteres Verteidigungsfeld, zumal die Auswertung jedenfalls meist lange Zeit in Anspruch nimmt, was sich zumindest strafmildernd auswirkt. Gleichwohl ist es auch aus Sicht der Verteidigung unangenehm, dass es an einem verbindlichen und damit für alle Beteiligten vorhersehbaren Maßstab fehlt, wie mit großen Datenmengen umzugehen ist.

Vor diesem Hintergrund benötigen wir dringend verbindliche Regelungen zum Umgang mit großen Datenmengen im Ermittlungsverfahren. Dabei können die Ermittlungsbehörden insbesondere auch von den diversen Privaten lernen, die interne Ermittlungen für Unternehmen anbieten und dabei immer weiter daran arbeiten, einen Standard zu entwickeln, wie eine entsprechende Aufarbeitung legitimerweise aussehen kann.[27] Positiv hervorzuheben sind in diesem Zusammenhang etwa Ausführungen des Bundesamts für Sicherheit in der Informationstechnik im „Leitfaden IT-Forensik",[28] wohingegen enttäuschend zur Kenntnis genommen werden muss, dass auch der aktuelle Entwurf eines Verbandssanktionengesetzes keine Standards für die grundrechtskonforme Auswertung großer Datenmengen benennt.

VI. Schluss

Abschließend bleibt nur festzuhalten, dass die zunehmende Digitalisierung der Gesellschaft selbstverständlich auch vor dem Strafrecht nicht Halt macht. Besonders bedeutend und grundrechtsrelevant sind dabei die Fragen, die sich angesichts der tatsächlichen Veränderungen im Rahmen des Ermittlungsverfahrens ergeben. Eine stete und intensive Diskussion über eine grundrechtskonforme Ausgestaltung des Ermittlungsverfahrens ist hier von großer Wichtigkeit. Mit den Auswirkungen auf den Anfangsverdacht und die Durchsicht

https://www.heise.de/newsticker/meldung/Streit-um-Data-Mining-bei-deutschen-Polizeibehoerden-1758346.html; https://netzpolitik.org/2013/bundeskriminalamt-zum-schnupperkurs-fur-polizeiliche-vorhersagesoftware-bei-ibm-in-freiburg/ (4.2.2020).

[23] Siehe hierzu etwa die Meldung unter becklink 2009574; ZD-Aktuell 2017, 05455; *Singelnstein*, NStZ 2018, 1; *Meinicke*, K&R 2015, 377; *Gercke*, ZUM 2019, 798 (803).

[24] Vgl. *Hermann/Soiné*, NJW 2011, 2922; *Singelnstein*, NStZ 2018, 1.

[25] BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02.

[26] Ausführlich zu Löschungspflichten in diesem Zusammenhang *Basar/Hiéramente*, NStZ 2018, 681.

[27] Ausführlich zur Grundlage und Ausgestaltung solcher Internal Investigations diverse Monographien, etwa Knierim/Rübenstahl/Tsambikakis (Hrsg.), Internal Investigations, 2. Aufl. 2016; Spehl/Grützner (Hrsg.), Corporate Internal Investigations, 2013; Bay (Hrsg.), Handbuch Internal Investigations, 2013; Moosmayer/Hartwig (Hrsg.), Interne Untersuchungen, 2. Aufl. 2018; *Rieder/Menne*, CCZ 2018, 203; *Bittmann/Brockhaus/v. Coelln/Heuking*, NZWiSt 2019, 1.

[28] Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (4.2.2020).

von großen Datenmengen in EDV-Systemen konnten in diesem Beitrag nur zwei von vielen Bereichen dargestellt werden, in denen Anpassungen erforderlich sind. Es bleibt zu hoffen, dass die diesbezügliche Diskussion an Bedeutung und Intensität zunimmt, damit allen Beteiligten im Strafprozess auch weiterhin ein schlüssiges, legitimes und vorhersehbares Regelwerk zur Verfügung steht.