Strafprozessualer Zugriff auf E-Mail-Kommunikation

– zugleich Besprechung zu BVerfG, Beschl. v. 16. 6. 2009 – 2 BvR 902/06* sowie zu BGH, Beschl. vom 31. 3. 2009 – 1 StR 76/09** –

Von Dominik Brodowski, LL.M. (UPenn)***

E-Mail-Kommunikation ist mannigfaltig neu- und andersartig: so erfolgt sie regelmäßig über international tätige, ausländische und private Dienstleister und überwindet in Sekunden die Beschränkungen von Raum und Zeit. Von einem ebenso schnellen, aber vergänglichen Telefongespräch unterscheidet sie sich durch ihre dauerhafte digitale Speicherung, im Zuge derer eine Archivierung sämtlicher E-Mail-Kommunikation über Jahre hinweg phänomenologisch nicht unüblich und äußerst kostengünstig ist.

Angesichts vielfältiger Zugriffsmöglichkeiten (I.) auf Inhalte und Umstände von E-Mail-Kommunikation in strafprozuessualen Ermittlungsverfahren und nahezu vollständig fehlender *lex specialis*[1] sind diese nach wie vor ein rechtliches Minenfeld. Zwei aktuelle höchstrichterliche Entscheidungen zum Zugriff auf Nachrichten, die im Postfach bei einem E-Mail-Provider lagern, nähern sich dieser Rechtsfrage von gegenläufigen Blickwinkeln: Auf der einen Seite diskutierte der *2. Senat des BVerfG* im Beschluss vom 16. 6. 2009 – 2 BvR 902/06 –, der angesichts gegenläufiger, über knapp 3 Jahre wiederholt erlassener einstweiliger Anordnungen[2] umso überraschender war, die betroffenen Grundrechte (II.) und die sich hieraus ergebenden, spezifisch verfassungsrechtlichen Mindeststandards (III.) und hat dabei einen offenen, punktuellen Zugriff im Kontext einer Hausdurchsuchung vor Augen. Auf der anderen Seite setzte sich der *1. Strafsenat des BGH* im zeitlich früheren Beschluss vom 31. 3. 2009 – 1 StR 76/09 – mit der im Ausgangspunkt strafprozessrechtlichen Frage nach der einschlägigen Ermächtigungsgrundlage auseinander (IV.) und bezieht sich dabei auch auf dem E-Mail-Benutzer verdeckte, längerfristige Überwachungen.

I. Technische Zugriffsmöglichkeiten auf E-Mail-Kommunikation

1. Ein einzelner E-Mail-Kommunikationsvorgang durchläuft bis zu sieben verschiedene Phasen:[3] Das *Entwerfen* (1. Phase) einer E-Mail erfolgt entweder »clientbasiert«, d. h. auf dem Rechner des Absenders, oder »serverbasiert«, d. h. die Rohdaten – einzelne Zeichen – werden in Echtzeit oder gelegentlich als Sicherungskopie auf einen Mailserver eines E-Mail-Providers übertragen und dort gespeichert.[4] E-Mail-Provider ist jeder Dritte, der technische Infrastruktur für E-Mail-Kommunikation zur Verfügung stellt, mithin auch Universitäten und (IT-Abteilungen von) Unternehmen.[5] Durch das *Absenden* (2. Phase) einer E-Mail wird die Nachricht um Meta-Informationen[6] vervollständigt und an eine spezielle Software – Mail Transport Agent (MTA, »Mailserver«) – übergeben. Diese überprüft zunächst die Legitimität des Nachrichtenversands, filtert dann etwa mit Schadsoftware versehene Nachrichten aus, ermittelt sodann den für die weitere Zustellung zuständigen Mailserver und versucht die Nachricht diesem (nach Möglichkeit verschlüsselt, Transport Layer Security) zu übermitteln (3. Phase). Typischerweise erfolgt während dieser Schritte eine Zwischenspeicherung der Nachricht auch im Festspeicher der jeweiligen Server.[7] Gelangt die Nachricht nach Weiterleitung durch unter Umständen mehrere andere Mailserver auf denjenigen Rechner, auf dem sich das E-Mail-Postfach des Empfängers befindet, unterwirft dort ein Mail Delivery Agent (MDA) die Nachricht ggf. weiteren Kontrollen und *speichert* sie in dessen *Postfach ab* (4. Phase). Der Empfänger kann die eingehenden Nachrichten ein- oder mehrmalig, vollständig oder teilweise aus dem Postfach *abrufen* und sich auf einer Website anzeigen (»Webmail«), als Kopie auf einem anderen Rechner abspeichern (»herunterladen«) oder an eine andere E-Mail-Adresse weiterleiten lassen (5. Phase). Bis zu einer Löschung der Nachricht aus dem Postfach – sei es manuell, sei es automatisch nach Ablauf einer Lagerfrist – ist die Nachricht noch im Postfach verfügbar. Allerdings führt selbst ein solches Löschen durch den Empfänger nicht notwendigerweise zu einer sofortigen, vollständigen, irreversiblen Vernichtung der Daten, einschließlich aller vom E-Mail-Provider automatisch erstellter Sicherungskopien (6. Phase).[8] Nach Abruf der Nachricht auf eigene Rechner des Empfängers steht es diesem frei, eine eingegangene E-Mail oder Teile hiervon lokal oder auf weiteren internetbasierten Diensten zu speichern (7. Phase).

Rechtlich vergleichbar zu behandeln sind andere neue Formen elektronischer (Individual-)Kommunikation, etwa in so genannten »sozialen Netzwerken« oder als Annex zu Diskussionsforen.[9] Diese sind zumeist serverbasiert, verwenden eigenständige technische Protokolle und bündeln die verschiedenen Phasen oft auf einem Server. Auch das als »Bürgerportal« bezeichnete Konzept einer so genannten »De-Mail« ergänzt lediglich die E-Mail-Kommunikation, etwa um zusätzliche Metadaten, welche der Bezahlung (»e-Porto«), Authentifizierung und Identifikation dienen, oder um langfristige, integritätsgeschützte Sicherungskopien (»De-Safe«).[10]

2. In strafprozessualen Ermittlungen können einerseits die bloßen Umstände der Telekommunikation – namentlich die

* In diesem Heft, S. 429 = NJW 2009, 2431 = EuGRZ 2009, 404.

** In diesem Heft, S. 428 = NJW 2009, 1828 = NStZ 2009, 397 m. zust. Anm. Bär NStZ 2009, 398; abl. Szebrowski MMR 2009 Heft 7, V.

*** Verf. ist Wiss. Ang. am Lehrstuhl für Europäisches Straf- und Strafprozessrecht an der Eberhard Karls Universität Tübingen, Prof. Dr. Joachim *Vogel*, RiOLG.

1 Nennenswerte Ausnahme ist die in § 100 g StPO i. V. m. § 113 a Abs. 3 TKG normierte Zugriffsmöglichkeit auf Verbindungsdaten (»Vorratsdatenspeicherung«). Vgl. hierzu die einstweilige Anordnung des 1. Senats des BVerfG vom 11. 3. 2008 – 1 BvR 256/08 = BVerfGE 121, 1; erweitert am 28. 10. 2008 = EuGRZ 2008, 663; zuletzt verlängert am 22. 4. 2009.

2 Durch dessen 3. Kammer zuerst am 29. 6. 2006 erlassen; BVerfG StraFo 2006, 365 m. Anm. Sankol MMR 2007, 169; Schlegel HRRS 2007, 44.

3 In der Bestimmung der Phasen anders Graf in: BeckOK-StPO (Stand 15. 6. 2009) § 100 a Rdn. 27; zu wenig differenzierend Nack in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 100 a Rdn. 19 (drei Phasen); Bär in: KMR Kommentar zur Strafprozessordnung (Stand 54. Lfg. Mai 2009) § 100 a Rdn. 27 (vier Phasen).

4 Insoweit zu eng BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 27.

5 S. Lenckner in: Schönke/Schröder, StGB, 27. Aufl. 2006, § 206 Rdn. 8 m. w. N. sowie OLG Karlsruhe CR 2005, 288.

6 Hierbei handelt es sich etwa um Datum, Uhrzeit und Absender.

7 Dies dient der Gewährleistung der weiteren Zustellung, selbst wenn durch einen Stromausfall der flüchtige Speicher (RAM) nicht länger nutzbar ist.

8 Vgl. hierzu Bleich c't kompakt 2/2009, 76, 77 f. sowie http://mail.google.com/mail/help/intl/de/privacy.html (Stand 3. 8. 2009): »Verbleibende Kopien von gelöschten Nachrichten ... können bis zu 60 Tage auf unseren aktiven Servern verbleiben, bis sie gelöscht werden, und bleiben eventuell auf unseren Offline-Backup-Systemen erhalten.« Darüber hinausgehend stehen forensische Möglichkeiten zur Verfügung, auch auf Dateisystem- bzw. Datenbankebene gelöschte Daten wiederherzustellen.

9 Ebenso KK-StPO/Nack (Fn. 3) § 100 a Rdn. 28.

10 Vgl. hierzu den Gesetzentwurf zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften, BT-Drs. 16/12598.

Empfänger- und Absenderadressen, der Zeitpunkt und die beteiligten IP-Adressen (§ 113 a Abs. 3 TKG) – (Verkehrsdaten), andererseits aber auch die jeweils übermittelten Daten (Inhaltsdaten) interessieren.[11]

a) *Verkehrsdaten* werden im Rahmen typischer Programmverwendungen für einen überschaubaren Zeitraum von MTA-Software für Zwecke der Fehlersuche gespeichert (sog. »Logfiles«). Angesichts einer diesbezüglichen sechsmonatigen Speicher*verpflichtung* des Diensteanbieters gem. § 113 a TKG sind weitere Zugriffsmöglichkeiten zwar denkbar, praktisch aber höchstens dann von Relevanz, wenn die E-Mail-Kommunikation nicht über einen Speicherungsverpflichteten durchgeführt wird.[12]

b) Bei computergestütztem Zugriff[13] auf *Inhaltsdaten* ist zu differenzieren:

(i) Eine *Überwachung,* d. h. ein Abgreifen von Inhaltsdaten über einen längeren Zeitraum, kann bereits beim Eintippen einer Nachricht ansetzen, also die Dateneingabe mit Hilfe einer heimlich installierten »Key Logging«-Software auslesen und den Ermittlungsbehörden übermitteln.

Die wohl typischste Überwachung setzt aber an einzelnen beteiligten Mailservern an und leitet die in den Phasen des Absendens, der Übermittlung, der Einlagerung oder auch des Abrufs erfolgenden Datentransfers in Kopie oder an Stelle des Empfängers an die Ermittlungsbehörden weiter. Spezielle Vorgaben für einen solchen verdeckt-kollusiven Zugriff sind § 110 TKG sowie der TKÜV zu entnehmen, welche Diensteanbieter zur Mitwirkung verpflichten. Daher sind theoretisch denkbare, heimliche Manipulationen der Server oder auch ein Abgreifen der Kommunikation zwischen zwei Servern regelmäßig nicht erforderlich.

(ii) Hingegen setzt eine *Durchsicht*, d. h. ein punktueller Zugriff auf vorangegangene E-Mail-Kommunikation, grundsätzlich an den Phasen der Lagerung an und kann sich auf noch ungelesene (Phase 4) wie auf gelesene (Phasen 6, 7) Nachrichten und auf Ausgangskopien beziehen. Es können dabei entweder alle vorhandenen Nachrichten, oder aber auch nur diejenigen, die nach einer automatischen Vorsortierung für ermittlungsrelevant erachtet wurden – etwa nach Absender, Empfänger, Datum oder Wörtern, die im Nachrichtentext enthalten sind – als Kopie an die Ermittlungsbehörden übertragen werden.

Je nach Speicherort der Nachrichten hat der Zugriff auf einen lokalen Arbeitsplatzrechner zu erfolgen – sei es offen nach Beschlagnahme des Rechners, sei es verdeckt durch den Einsatz einer Remote Forensic Software (RFS) – oder aber durch Zugriff auf die bei einem E-Mail-Provider gespeicherten Daten. Letzterer erfolgt typischerweise gegenüber dem Diensteanbieter *offen,* ein verdeckter Zugriff ist aber ebenfalls denkbar, etwa wenn den Ermittlungsbehörden Benutzername und Passwort des Postfachs bekannt sind.

(iii) Ebenfalls zu berücksichtigen sind die Möglichkeiten, offen oder verdeckt auf Sicherungskopien oder temporäre Kopien von Nachrichten zuzugreifen, wie sie etwa von Diensteanbietern automatisch erstellt werden.[14] So könnten Ermittlungsbehörden noch auf Nachrichten zugreifen, welche der Benutzer zwar in seinem Postfach »gelöscht« hat, die aber dem Benutzer lediglich nicht mehr angezeigt werden und noch an anderer Stelle, zum Teil auch langfristig, gespeichert sind.

3. Die *Beweisqualität* ist bei einem verdeckten, aber auch bei einem kollusiven Zugriff (Mitwirken des Diensteanbieters ohne Wissen des Betroffenen) allein wegen eines Manipulationsrisikos und einer nur nachgeschalteten Konfrontationsmöglichkeit am geringsten.[15] Insbesondere zu Lasten Dritter ist die Beweisqualität aber auch bei lagernden Nachrichten reduziert, denn diese können nicht nur vom Benutzer gelöscht, sondern auch modifiziert und sogar hinzugefügt werden.

4. Die Beschlüsse des *BVerfG* und des *BGH* bezogen sich jeweils auf beim E-Mail-Provider gespeicherte, ungelesene und gelesene Nachrichten (Phasen 4 und 6). Im dem der *BVerfG*-Entscheidung zugrunde liegenden Verfahren geschah der Zugriff mit Wissen des Betroffenen nach einer Hausdurchsuchung; der Beschluss des *BGH* betrachtet einen kollusiven Zugriff.

II. Grundrechtliche Schutzstandards

1. Verschiedene Denkansätze lassen sich in den Diskussionen über die Eröffnung verfassungsrechtlicher Schutzbereiche, aber auch bei der Bestimmung des Anwendungsbereichs von Eingriffsbefugnissen differenzieren, sofern die Verwendung von Informationstechnologie gegenständlich ist[16]:

a) Eine *technisch-funktionale Theorie* verweist darauf, dass technische Neuerungen der Informations- und Kommunikationstechnologie teils als Ersatz, teils als Ergänzung zu herkömmlichen Kommunikations- und Arbeitsformen herangezogen werden. Virtuelle Räume treten dabei an die Stelle von physikalischen Räumen. Soweit keine wesentlichen funktionalen Auswirkungen und Unterschiede gegeben seien – wie etwa bei einem E-Mail-Versand anstelle eines Briefs –, sei auch deren rechtliche Handhabung äquivalent zu beurteilen.[17]

b) Eine *technikvergleichende Theorie* betrachtet die einzelnen technisch-realen Verfahrensschritte isoliert und orientiert sich dabei jeweils an Entsprechungen altbekannter Kommunikationsvorgänge. Eine – auch nur wenige Sekunden andauernde – Zwischenspeicherung einer E-Mail wird hierbei als Verkörperung angesehen, welche einen Telekommunikationsvorgang unterbreche.[18]

c) Eine *schutzfunktionale Theorie* stellt darauf ab, ob der durch eine Norm spezifizierte Schutz eine geeignete Barriere gegen fremde Zugriffe auf Informations- und Kommunikationstechnologie darstellt. Sei eine E-Mail bei dem Empfänger angekommen, entfalte Art. 10 GG mit seinem Fokus auf den Übertragungsweg keinen Schutz mehr; vermögen die physikalischen Grenzen einer Wohnung keinen Schutz zu liefern, sei Art. 13 GG nicht einschlägig.[19]

d) Bei der folgenden Diskussion ist darauf zu achten, dass

11 Bestandsdaten hingegen betreffen die »Begründung, inhaltliche Ausgestaltung oder Änderung« von Vertragsbeziehungen zwischen Diensteanbietern und Nutzern, mithin etwa die Anschrift des Nutzers. Vgl. § 3 Nr. 3 TKG.

12 So betraf BVerfGE 115, 166 auch eine Konstellation vor Einführung der Vorratsdatenspeicherung von Verbindungsdaten.

13 Alternativ sind auch sozial-interaktive Zugriffe denkbar, etwa bei Einsatz verdeckter Ermittler, oder auch eine optische Videoüberwachung (auch) des Bildschirms, an dem eine vormals verschlüsselte Nachricht angezeigt wird.

14 Vgl. hierzu bereits oben bei und mit Fn. 7 und 8 sowie auch VGH Kassel NJW 2009, 2470, 2470.

15 So auch BVerfGE 120, 274, 320 f. (»Online-Durchsuchung«) m. Anm. Böckenförde JZ 2008, 925; Kutscha NJW 2008, 1042; Rossnagel/Schnabel NJW 2008, 3534; Sachs/Krings JuS 2008, 481.

16 Zur grundsätzlicheren Diskussion, ob das Internet fernab nationaler Rechtsordnungen eigenständiger Inhalts- und Verhaltensregeln (und nicht nur technischer Standards) bedarf, vgl. nur Darnstädt u.a., Der Spiegel 33/2009, S. 68 ff.

17 So LG Braunschweig, Beschl. v. 12. 4. 2006 – 6 Qs 88/06, bestätigt durch BVerfG – 2 BvR 902/06. Vgl. ferner Rux JZ 2007, 285, 292 ff.; ders. JZ 2007, 831, 832 entgegen Hornung JZ 2007, 828, 829 f. sowie auch § 110 Abs. 3 StPO: Zugriff auf räumlich getrennte Speichermedien, als ob sich diese im Durchsuchungsobjekt befinden.

18 Vgl. etwa BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 28. Eine entsprechende Auffassung bei der »Online-Durchsuchung« sah den Schutzbereich des Art. 13 GG dann und nur dann eröffnet, wenn sich ein Rechner – auch zufälligerweise – gerade in einer Wohnung befinde. Vgl. hierzu exemplarisch Bär MMR 2007, 239, 240; Buermeyer HRRS 2007, 329, 332; Harendorf StraFo 2007, 149, 151; Valerius JR 2007, 275, 279 f.

19 Vgl. etwa BVerfGE 120, 274, 310 f.; BVerfG – 2 BvR 902/06 – Rz. 47; Beulke/Meininghaus StV 2007, 63, 64; Schlegel GA 2007, 648, 654 ff.

erstens ein als Korrektiv wirkender *rechtlicher* Schutz neuer Technologien gerade bei geringem *technischem* Schutz notwendig ist. Zweitens ist zu vermeiden, durch eine zu isolierte und fokussierte Betrachtungsweise Schutzlücken entstehen zu lassen, welche der rechtlichen Notwendigkeit und dem sozialen Nutzen einer Beschränkung staatlichen Handelns schaden. Drittens aber darf die virtuelle Welt nicht idealisiert werden und ihr über die Maßen Freiheitsräume zugestanden werden, wie sie aus den guten Gründen eines legitimen Strafverfolgungsinteresses in anderen Bereichen auch nicht existieren.

2. Der verfassungsrechtliche Schutz von Kommunikation über räumliche Distanzen hinweg ist Leitgedanke des Art. 10 GG. Allerdings ist sein Wortlaut und die hierauf gestützte Auslegung auf drei Kommunikationsformen begrenzt: den Brief- und Postversand sowie die Nutzung von Telekommunikation bzw. Fernmeldetechnik. Diese Fokussierung stößt zu Recht auf grundsätzliche Kritik, denn sie führt gerade in Randbereichen zu Schutzlücken. So kann etwa auf technischer Ebene[20] nicht länger zwischen von Art. 10 Abs. 1 GG geschützter Individual- und von Art. 5 Abs. 1 GG geschützter Massenkommunikation differenziert werden,[21] und so unterliegen Daten vor und nach Abschluss von Kommunikationsvorgängen – etwa ein E-Mail-Entwurf oder eine auf einem Privatrechner abgespeicherte E-Mail – nach Auffassung des *BVerfG* nicht dem Schutzbereich des Art. 10 Abs. 1 GG.[22] Zwar behilft sich das *BVerfG* zum Schutz der Privatsphäre mit dem Rückgriff auf das Allgemeine Persönlichkeitsrecht (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) und auf dessen spezielle – und auch mit speziellen Schutzstandards versehene – Ausprägungen wie den Grundrechten auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme;[23] dieser Zersplitterung vorzugswürdig erscheint allerdings ein holistischer Ansatz, wie er etwa auf europäischer Ebene gewählt wird.[24]

a) Auswirkungen hatte diese Fragmentierung bei der in beiden Verfahren gegenständlichen Frage, ob bei E-Mail-Providern gespeicherte Nachrichten noch Gegenstand von Telekommunikation sind und damit dem Schutzbereich des Art. 10 Abs. 1 GG unterliegen. Dies betrifft einerseits die Speicherung durch den E-Mail-Provider des Empfängers bis zum ersten Abruf der Nachricht durch den Empfänger, und andererseits die etwaige weitere Lagerung im E-Mail-Postfach bei dem E-Mail-Provider, nachdem der Empfänger erstmalig von der Nachricht Kenntnis genommen und daher die Möglichkeit hatte, die Nachricht zu löschen.

b) Der *2. Senat des BVerfG* wendet als entscheidendes Kriterium für die Eröffnung des Schutzbereiches aus Art. 10 Abs. 1 GG an, ob sich Nachrichten noch außerhalb des *Herrschaftsbereich* des Kommunikationsempfängers befinden (schutzfunktionale Theorie).[25] Für eine Zuordnung von beim E-Mail-Provider lagernden Nachrichten zum Herrschaftsbereich des Empfängers spricht zwar, dass es ihm freisteht, wann er die Nachricht abruft, liest, ggf. anderen zur Kenntnis gibt[26] und lokal wie im Postfach des E-Mail-Providers löscht. Doch seine Möglichkeiten zur Ausübung dieser Herrschaft sind im Regelfall begrenzt, gleich ob die Nachricht schon abgerufen wurde:[27] so ist der E-Mail-Provider sowohl technisch dazu in der Lage wie auch rechtlich dazu befugt, den Empfänger vom Zugriff auf die Nachrichten auszuschließen, etwa, wenn mehrfach das Passwort fehlerhaft eingegeben wurde. Zudem ist, wie bereits erwähnt, ein Löschen durch den Empfänger nur unvollkommen und regelmäßig reversibel. Man mag zwar argumentieren, dass dies lediglich vertragliche Einschränkungen darstellen, auf die sich Kunden von E-Mail-Providern freiwillig eingelassen haben.[28] Damit ließe man aber den Schutz für technisch weniger versierte Internet-Nutzer verkümmern;[29] aber gerade diese sind aus grundrechtlicher Sicht besonders schutzwürdig.[30]

c) Ein anderer, auf die technisch-funktionale Theorie rekurrierender Begründungsansatz, der sich auch auf die Rechtsprechung des *BVerfG* beruft,[31] verweist auf eine einheitliche Betrachtung des gesamten Kommunikationsvorgangs.[32] Sie sieht diesen jedenfalls solange als noch andauernd an, bis die Nachricht den Empfänger erreicht hat, er diese also zum ersten Mal aus dem Postfach des E-Mail-Providers geladen hat – vergleichbar einem Brief, der aus dem Briefkasten genommen werde. Anschließend noch beim E-Mail-Provider lagernde E-Mails hingegen seien bloß Manifestierungen abgeschlossener Kommunikation und daher nicht von Art. 10 Abs. 1 GG erfasst.[33] Dass diese zufälligerweise auch bei einem E-Mail-Provider und nicht auf einer Internetfestplatte gespeichert werden, ist insoweit folgerichtig technisch-funktional unerheblich und verlangt daher auch nicht nach einem höheren Schutz aus Art. 10 Abs. 1 GG. Dem widerspricht der *2. Senat des BVerfG* nun unter Bezugnahme auf die durch den E-Mail-Provider als Kommunikationsmittler existierende spezifische Gefährdungslage, der nach wie vor Zugriff auf die Nachricht habe.[34]

d) Die Vertreter einer technikvergleichenden Theorie argumentieren hingegen, dass neben der technisch bedingten, oftmals

20 Früher konnte insbesondere zwischen Rundfunk als Massen- und Telefon als Individualkommunikation unterschieden werden; heutzutage werden dieselben Techniken insbesondere des Internets für beide Zwecke genutzt: eine passwortgeschützte Internetseite ist, solange das Passwort lediglich zwei Personen bekannt ist, Individualkommunikation; wird das Passwort einem nicht länger abgrenzbaren Personenkreis zur Verfügung gestellt, liegt Massenkommunikation vor.

21 Vgl. hierzu nur Hermes in: Dreier (Hrsg.) GG, 2. Aufl. 2004, Art. 10 Rdn. 43.

22 BVerfG – 2 BvR 902/06 – Rz. 45 m. w. N.; BVerfGE 115, 166, 183 ff.; s. ferner BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 27.

23 BVerfGE 120, 274, 307 f.; krit. etwa Pagenkopf in: Sachs (Hrsg.) GG, 5. Aufl. 2009, Art. 10 Rdn. 10; Sachs/Krings JuS 2008, 481, 82.

24 Näher hierzu Dreier-GG/Hermes (Fn. 21) Art. 10 Rdn. 11, 39 unter Bezugnahme auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), AblEG L 201 vom 31. 7. 2002, S. 37. Vgl. ferner EGMR EuGRZ 1993, 65, 66 (Rz. 32). (Inaugenscheinnahme von Briefen im Rahmen einer Hausdurchsuchung als Eingriff in die Korrespondenzfreiheit).

25 BVerfGE 120, 274, 307 f. auch unter Verweis auf BVerfGE 113, 166, 183 ff.; ferner VGH Kassel NJW 2009, 2470, 2471.

26 Man beachte aber, dass die Telekommunikationsdienstleister betreffende Strafvorschrift § 206 Abs. 1 StGB akzessorisch zum Schutzbereich des Art. 10 Abs. 1 GG ist und daher verdeutlicht, dass dieser nicht zu eng ausgelegt werden darf.

27 So auch LG Hamburg StV 2009, 70, 71, das aber zu sehr auf die Möglichkeit des – rechtlich im Regelfall unzulässigen – Lesezugriffs durch den E-Mail-Provider abstellt.

28 So die Argumentation mit einem Empfangsboten i. S. d. § 130 BGB durch KK-StPO/Nack (Fn. 3) § 100 a Rdn. 22.

29 Experten hingegen ist es möglich, selbst einen so genannten »Root-Server« zu betreiben und dabei unter anderem als E-Mail-Provider zu agieren. Als Administrator eines »Root-Servers« stehen einem sodann eine Vielzahl von Möglichkeiten offen, insbesondere auch über die Sicherungskopien und die definitive Löschung von Daten zu herrschen.

30 So auch BVerfG – 2 BvR 902/06 – Rz. 46, 53. Insofern überzeugt es auch nicht, dass BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 28 auf den geringen technischen Schutz einer E-Mail-Kommunikation verweist: gerade weil die technischen Schranken so niedrig sind, müssen die rechtlichen Barrieren – sei es für illegitimen Zugriff (§ 206 Abs. 1 StGB), sei es für legitimen staatlichen Zugriff im Rahmen eines Ermittlungsverfahrens – umso höher sein, um ein adäquates Schutzniveau zu schaffen.

31 BVerfGE 106, 28, 38; BVerfGE 115, 166, 185.

32 LG Hanau StV 2000, 354; LG Mannheim StV 2002, 242; LG Hamburg StV 2009, 70, 71; Dübbers StV 2000, 355; Gaede StV 2009, 96, 97; Jäger StV 2002, 243, 24; Jahn NStZ 2007, 255, 264; Marberth-Kubicki StraFo 2002, 271, 281; Meyer-Gossner StPO, 52. Aufl. 2009, § 100 a Rdn. 6; Michalke StraFo 2005, 91, 92.

33 So interpretiert jedenfalls Sankol MMR 07, 170 die Argumentationslinie des BVerfG in der einstweiligen Anordnung (Fn. 2); a. A. jedoch LG Hamburg StV 2009, 70, 71; Gaede StV 2009, 96, 97 f.

34 BVerfG – 2 BvR 902/06 – Rz. 48.

mehrmaligen Zwischenspeicherung während der Übertragung[35] jedenfalls aufgrund der zuweilen lang andauernden Speicherung der Nachricht beim E-Mail-Provider ein Kommunikationsvorgang bereits mit Eingang beim E-Mail-Provider des Empfängers abgeschlossen sei. Die Daten[36] seien daher ab diesem Zeitpunkt nicht länger Gegenstand eines Kommunikationsvorgangs und infolgedessen nicht von Art. 10 Abs. 1 GG geschützt.[37] Auch diese Ansicht, so der *2. Senat des BVerfG*, verkenne allerdings die spezifische Gefährdungslage der fortdauernden Speicherung der Nachrichten bei einem E-Mail-Provider.[38]

e) Dem ist zuzustimmen, und es überzeugt, dass das *BVerfG* hierauf aufbauend explizit und auch der *BGH* implizit eine Differenzierung zwischen gelesenen und ungelesenen Nachrichten ablehnt: Art. 10 Abs. 1 GG bezieht sich dem Wortlaut nach nicht nur auf den Kommunikationsvorgang, sondern auch auf dessen Inhalte.[39] Insofern erscheint eine künstliche Aufspaltung eines Kommunikationsvorgangs verfehlt, gerade wenn man dabei den eigentlichen, umfassenden Schutzzweck der Norm aus den Augen verliert, denn diese dient dem Schutz der Privatsphäre und der umfassenden Ermöglichung privater Kommunikation – unter Verwendung vielfältiger technischer Möglichkeiten –[40] als Eckpfeiler einer freiheitlichen Grundordnung.

f) Infolgedessen sind richtigerweise die Phasen des Absendens, der Übermittlung, der Einlagerung im Eingangs-Postfach einschließlich eines Abrufs und auch die fortdauernde benutzerfremde Speicherung (Phasen 2–6) durch das spezielle Grundrecht aus Art. 10 Abs. 1 GG geschützt. Aus Sicht der Kommunikationspartner erübrigt sich daher eine Anwendung der Auffanggarantien der informationellen Selbstbestimmung und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Auch können sich diese weder auf Art. 13 GG berufen, soweit Räumlichkeiten des E-Mail-Providers betroffen sind, noch auf Art. 14 GG, soweit Besitz des E-Mail-Providers (etwa durch Sicherstellung eines Servers) beeinträchtigt wird, da insoweit nicht ihre eigenen, sondern nur fremde Grundrechtspositionen betroffen sind.[41] Eigenständige Bedeutung gewinnen diese Grundrechte nur in Sonderfällen eines auch gegenüber E-Mail-Providern verdeckten Vorgehens, sei es durch eine Manipulation dort installierter Software, sei es durch Zugriff mittels den Ermittlungsbehörden bekannter Benutzernamen und Passwörter oder deren Erraten durch »Brute-Force-Attacken«.

3. a) Beim Nutzer gespeicherte E-Mail-Nachrichten (Phase 7) unterliegen dem *BVerfG* nach nicht dem Schutz des Art. 10 Abs. 1 GG, da der Kommunikationsvorgang endgültig abgeschlossen sei[42] und sich die Nachricht im Herrschaftsbereich des Benutzers befinde. Zum Zugriff auf beim Nutzer gespeicherte E-Mail-Nachrichten wird aber regelmäßig ein Eingriff in Art. 13 Abs. 1 GG vonnöten sein, um an einen in der Wohnung des Nutzers gelegenen Datenträger zu gelangen. Nach Rechtsprechung des *BVerfG* ist jedoch weder Art. 13 Abs. 1 GG noch Art. 10 Abs. 1 GG, sondern das sich auf Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gründende Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme heranzuziehen, wenn ein verdeckter Zugriff auf den Datenträger – etwa im Wege einer Online-Durchsicht – erfolgen soll.[43] Bei alledem muss berücksichtigt werden, dass es sich um Daten handelt, die bei benutzerfremder Speicherung dem besonderen Schutz aus Art. 10 GG unterliegen.[44]

b) Bei lokaler Erstellung einer Nachricht (Phase 1) ordnet der Benutzer erst mit dem Befehl zum Versenden einer Nachricht die Daten einem Kommunikationsvorgang zu. Sie werden mit dieser Aktion zu Kommunikationsinhalten und unterliegen ab dann dem speziellen Regime des Art. 10 Abs. 1 GG. Zuvor unterliegen sämtliche Entwürfe und Nachrichtenteile (etwa Anhänge) demselben Schutz wie sonstige auf dem Rechner gespeicherte Daten, freilich unter Beachtung der besonderen sich aus dem Kommunikationskontext ergebenden Abwägungskriterien.

c) Erfolgt allerdings bereits im Entwurfsstadium eine Datenübertragung in Echtzeit oder phasenweise auf den Server, so lassen sich folgende rechtliche Sichtweisen differenzieren: nach der technisch-funktionalen Theorie liegt ein Äquivalent zur Nutzung eines lokalen Rechners vor, so dass dieselben Schutzstandards aus Art. 13 GG, Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG Anwendung finden. Nach der technikvergleichenden Theorie ist zwischen dem Art. 10 Abs. 1 GG unterfallenden Übertragungsvorgang auf den Server und der nicht speziell geschützten, dortigen Speicherung zu unterscheiden. Dieser Ansatz verkennt aber schutzfunktional die besondere Bedrohungslage durch das Anvertrauen potentieller Kommunikationsinhalte, welches den speziellen Schutz aus Art. 10 Abs. 1 GG verlangt. Daher muss ein kollusiver Zugriff auf serverseitig gespeicherte Nachrichtenentwürfe dessen besonderen Anforderungen genügen.

4. Bei aller Diskussion über die einschlägigen Grundrechte darf jedoch nicht übersehen werden, dass entscheidend nicht die Eröffnung derer *Schutzbereiche* ist, sondern die aus einer abstrakten Bewertung und Typisierung der Verhältnismäßigkeit folgenden *Schutzstandards*. Aufgrund der besonderen Bedeutung, Schutzbedürftigkeit und -würdigkeit von Kommunikation wird daher – notfalls unter Heranziehung eines »Auffanggrundrechts« wie dem der Vertraulichkeit und Integrität informationstechnischer Systeme – ein alle Konstellationen umfassender, adäquater Schutz zu gewährleisten sein.

5. Wegen der internationalen Dimension von E-Mail-Kommunikation und vor allem aufgrund des europastrafrechtlichen Grundsatzes der gegenseitigen Anerkennung ginge man nicht weit genug, alleine die deutsch-verfassungsrechtlichen Schutzstandards aufzuzeigen. Wenn auch eine Beschränkung staatlicher Möglichkeiten zur gegenseitigen Rechtshilfe in Strafsachen – und damit zur transnationalen Ausführung von Ermittlungsmaßnahmen – in der Begrenzung der Rechtshilfe*pflichten*[45] einiger europastrafrechtlicher Instrumente nicht zu sehen ist, so wächst auf Ebene der Europäischen Union das Bewusstsein für eine adäquate Berücksichtigung des auf Art. 6 EU gestützten Verhältnismäßigkeitsprinzips[46] bereits bei der Anordnung von Maßnahmen in Ermittlungsverfahren.[47] Bedeutsamer dürfte jedoch

35 So BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 28, der auch nur wenige Sekunden andauernde Speicherungen genügen lässt.

36 Dies schließt auch Verkehrsdaten mit ein, auf die Schlegel HRRS 2007, 44, 49 besonderen Wert legt. Allerdings stehen diese auch bei einer Beschlagnahme einer auf einem PC gespeicherten E-Mail zur Verfügung, gleich einem Briefumschlag, der bei einer Durchsuchung aufgefunden wird.

37 KMR/Bär (Fn. 3) § 100 a Rdn. 29; BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 28 f; Löffelmann in: Krekeler/Löffelmann (Hrsg.) Anwaltskommentar StPO, 2007, § 100 a Rdn. 9.

38 BVerfG – 2 BvR 902/06 – Rz. 48.

39 So auch BVerfG – 2 BvR 902/06 – Rz. 44 m. w. N.

40 Vgl. nur BVerfGE 107, 299, 313 sowie Gaede StV 2009, 96, 97 m. w. N.

41 BVerfG – 2 BvR 902/06 – Rz. 49 ff. Im Regelfall dürfte allerdings nur ein kooperatives/kollusives Vorgehen mit dem Provider verhältnismäßig sein, also etwa ihn zu verpflichten, eine identische Kopie der in einem E-Mail-Postfach gespeicherten Daten auf einen Datenträger zu speichern – anstelle den Datenträger, auf dem das E-Mail-Postfach gespeichert ist, auszubauen und auszuhändigen.

42 BVerfG – 2 BvR 902/06 – Rz. 45.

43 BVerfGE 120, 274, 306 ff. Vgl. Fn. 15.

44 Vgl. BVerfGE 115, 166 (LS 3).

45 So ist etwa der Verzicht auf die Prüfung beiderseitiger Strafbarkeit in Art. 2 Abs. 2 Rahmenbeschluss des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (AblEG L 190 vom 18. 7. 2002, S. 1) auf bestimmte Listendelikte beschränkt. Dies schließt allerdings nicht per se einen einseitigen, weitergehenden Verzicht auf eine solche Prüfung aus.

46 Callies in: Callies/Ruffert (Hrsg.) Das Verfassungsrecht der Europäischen Union, 3. Aufl. 2007, Art. 6 EUV Rdn. 21, 25.

47 Vgl. hierzu den Abschlussbericht über die vierte Runde der gegenseitigen Begutachtungen – »Praktische Anwendung des Europäischen Haftbefehls

für alle Mitgliedstaaten des Europarats – und mittelbar auch für die EU – die Judikatur des EGMR sein. Auch wenn sich diese, soweit ersichtlich, bislang lediglich auf Telefonüberwachung bezieht, so zeigen die aus Art. 8 EMRK folgenden zeitlichen und inhaltlichen Begrenzungen[48] erstens, welche hohe Relevanz der EGMR dem Schutz ungehinderter Kommunikation zugesteht, und zweitens, dass sich der EGMR zur Verwirklichung des Schutzes einer Typisierung und abstrakten Spezifizierung der Verhältnismäßigkeit bedient.

III. Verfassungsrechtliches Erfordernis einer speziellen Ermächtigungsgrundlage?

1. Der Beschluss des *2. Senats des BVerfG* tendiert zu einer bloßen *Einzelfallbetrachtung* der Verhältnismäßigkeit und weist damit in eine der Rechtsprechung des EGMR entgegengesetzte Richtung. Unstrittig ist zwar, dass eine solche Einzelfallprüfung unabdingbar ist,[49] um auch im Einzelfall aus dem Raster fallende, unverhältnismäßige Maßnahmen zu verhindern und damit den Verfassungsgrundsatz der Verhältnismäßigkeit weitestgehend zu verwirklichen. Ob darüber hinausgehend bei einem Zugriff auf bei einem Provider lagernde E-Mails (Phasen 4 und 6) eine speziellere Ermächtigungsgrundlage als §§ 94 ff. StPO erforderlich ist, richtet sich *verfassungsrechtlich* insbesondere nach den Geboten der Normenklarheit und -bestimmtheit.

2. Nach Auffassung des *2. Senats* erfüllen §§ 94 ff. StPO im Hinblick auf diese Gebote die Anforderungen an eine verfassungsrechtlich taugliche Eingriffsgrundlage in Art. 10 GG und genügen auch dessen speziellem Gesetzesvorbehalt. So enthielten erstens §§ 99, 100 a, 100 g StPO keine abschließende Regelung zu strafprozessualen Eingriffen in Art. 10 Abs. 1 GG, so dass Raum für §§ 94 ff. StPO verbleibe, zweitens sei die Erstreckung des § 94 StPO auch auf Daten und Datenträger trotz des sich auf Gegenstände beziehenden Wortlauts »hinreichend erkennbar«, und drittens sei die Zweckbindung der Maßnahme auf strafprozessuale Ermittlungen »präzise vorgegeben«. Zwar ist gegen die beiden letztgenannten Aspekte als solches nichts einzuwenden, doch überrascht die Argumentation des *BVerfG* insbesondere im Lichte der bisherigen Rechtsprechung zur Normenklarheit und -bestimmtheit.[50]

Nach dem Gebot der Normenbestimmtheit sind nicht nur der Anlass und Zweck, sondern gerade auch die Grenzen eines »Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen«.[51] Angesichts der fachgerichtlichen Rechtsprechung, die wegen der spezifischen Gefährdungslage §§ 94 ff. StPO nicht ausreichen ließ[52] und daher über die Frage des Wie[53] diskutierte, ist es nach der verfassungsrechtlichen Legitimierung auch für §§ 94 ff. StPO dem Bürger nicht länger vorhersehbar, ob ein Zugriff auf beim Provider lagernde E-Mails nach den Voraussetzungen der §§ 94 ff. StPO oder lediglich nach den strengeren Grenzen der §§ 99, 100, 100 a, 100 b StPO möglich ist. Angesichts der Existenz von solchen Spezialnormen für Eingriffe in Art. 10 GG dürfte es auch verständige Bürger überraschen, dass weitere, vergleichbare Eingriffe mit dem Schwerpunkt auf demselben Grundrecht auf eine generelle, nicht mit spezifischen Schutzstandards versehene Norm gestützt werden können. All das wiegt umso schwerer, da Bürger E-Mail als Ersatz für Briefpost sehen und sich daher – der technisch-funktionalen Theorie folgend – auf den erhöhten Schutz der §§ 99, 100 StPO verlassen. Zusätzlich leidet die vom *BVerfG* als Korrektiv vorgesehene Einzelfallprüfung der Verhältnismäßigkeit unter deren Unvorhersehbarkeit – auch angesichts derer diffuser Kriterien[54] – so dass die hinreichende Bestimmtheit und auch Klarheit der Normen der §§ 94 ff. StPO für Eingriffe dieser Intensität angezweifelt werden muss.

3. Der *2. Senat* hält §§ 94 ff. StPO für *generell* verhältnismäßig, auch soweit diese die Sicherstellung und Beschlagnahme von benutzerfremd gelagerten Nachrichten tragen. An der Verfolgung eines legitimen Ziels, der generellen Eignung und Erforderlichkeit strafprozessualer Zugriffsmöglichkeiten bestehen zutreffenderweise keine Zweifel. Bei der Verhältnismäßigkeit im engeren Sinne gilt es jedoch, mit dem legitimen staatlichen Strafverfolgungsinteresse aufzuwiegen:

a) Hierzu merkt der *2. Senat* zunächst an, dass Inhaltsdaten *per se* schutzwürdiger als bloße Verbindungsdaten seien, dass die potentielle Mitbetroffenheit von unbeteiligten Dritten erschwerend wirke und dass ein besonderes »Vertrauensverhältnis« – hier zu Kommunikationsmittlern – eine »besondere Schutzbedürftigkeit« mit sich bringe.[55] Dem ist nichts hinzuzufügen.

b) Der *2. Senat* grenzt die Reichweite seiner Prüfung dahingehend ein, als dass er lediglich von einer »einmalige[n] und punktuelle[n] Datenerhebung«[56] spricht (Durchsicht), mithin aber nicht von einem Abgreifen auch (neu) in das Postfach eingehender Nachrichten (Überwachung). Das Postulat, dass ein solcher einmaliger Zugriff weniger schwer wiege, vermag so nicht zu überzeugen:

Bei einer Datenerhebung ist nach der Rechtsprechung des *BVerfG* restriktiv zu berücksichtigen, ob sich aus den gewonnenen Informationen ein Persönlichkeitsprofil erstellen ließe.[57] Nun ist eine weit verbreitete Praxis einer Archivierung nahezu aller in irgendeiner Weise relevanter E-Mails festzustellen, die auch gesellschaftlich anerkannt ist. Diese dient nämlich einer langfristigen Sicherung der sich aus den Kommunikationsinhalten ergebenden sozialen, privaten wie gesellschaftlichen Vorteile, insbesondere in Zeiten einer Informationsflut, die nur digital zu bewältigen erscheint. Aus einem solchen umfangreichen Nachrichtenbestand ließe sich aber weitaus eher ein Persönlichkeitsprofil erstellen als aus einer nur wenige Stunden oder Tage andauernden Überwachung, so dass eine Durchsicht eher geeignet erscheint, gegen dieses verfassungsrechtliche Gebot zu verstoßen.

Zudem wird vorgebracht, gespeicherte E-Mails könne man löschen und damit deren Erhebung im Rahmen einer Durchsicht verhindern. Daher sei eine Durchsicht milder als eine Überwachung.[58] Diese Sichtweise geht fehl, denn schließlich kann und darf es kein Anliegen des Staates sein, die Vernichtung von Beweismitteln auch nur implizit zu fördern. Zudem ist eine solche Löschung oftmals reversibel, sei es aufgrund von Sicherungskopien, sei es mit Hilfe forensischer Analysen.

Statt dessen ist es die Zukunftsbezogenheit einer laufenden Überwachung, welche deren besondere Eingriffsintensität be-

und der entsprechenden Übergabeverfahren zwischen den Mitgliedstaaten«, Ratsdok. 8302/09, S. 12 f.

48 S. hierzu Grabenwarter EMRK, 3. Aufl. 2008, § 22 Rdn. 34 m. umfangr. Nachw.

49 Dies gilt auch dann, wenn für eine Ermittlungsmaßnahme ein typisierter Schutz aus Verfassungs- (etwa Art. 13 Abs. 3 GG) oder Strafprozessrecht (etwa §§ 100 a, 100 b StPO) existiert. Statt vieler Schäfer in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, vor § 94 Rdn. 117 ff. m. w. N.; Rudolphi in: Systematischer Kommentar zur StPO und zum GVG (Stand 61. Lfg. April 2009), § 94 Rdn. 68 ff.

50 BVerfGE 110, 33, 52 ff.; BVerfGE 120, 274, 315 ff.

51 BVerfGE 110, 33, 53; BVerfGE 120, 274, 316 m. w. N.

52 So i.E. auch BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 29.

53 Einerseits §§ 99, 100 mit verfahrensrechtlichem Schwerpunkt, andererseits §§ 100 a, 100 b mit materiellrechtlichem Schwerpunkt (erhöhte Verdachtsschwelle, Katalogtat). Vgl. hierzu unten IV. 2. Zur Notwendigkeit einer eindeutigen Ermächtigungsgrundlage vgl. Th. Böckenförde Die Ermittlung im Netz, 2003, 133 f.

54 S. unten III. 3. sowie V.

55 BVerfG – 2 BvR 902/06 – Rz. 65 ff.

56 BVerfG – 2 BvR 902/06 – Rz. 68.

57 BVerfGE 65, 1, 42; BVerfGE 115, 166, 193; BVerfGE 115, 320, 349 ff.

58 So LG Braunschweig, Beschl. v. 12. 4. 2006 – 6 Qs 88/06 (Ausgangsverfahren zu 2 BvR 902/06). Vgl. zu diesem Aspekt aber auch BVerfGE 115, 166, 185 f.

gründet. Bei einer Durchsicht umfangreicher Archive von E-Mails ergibt sich aber, wie aufgezeigt, eine zumindest vergleichbare Eingriffsintensität.

c) Der *2. Senat des BVerfG* legt bei seiner Prüfung der *generellen* Verhältnismäßigkeit lediglich Zugriffe mit Kenntnis des Betroffenen zugrunde,[59] wenn etwa – wie im verfahrensgegenständlichen Fall – eine solche Sicherstellung einer Durchsuchung folgt.

(i) In dieser Konstellation einer einmaligen, offenen Durchsicht wird der Unterschied zur Vorratsdatenspeicherung von Verbindungsdaten deutlich, bei der die strafprozessualen Zugriffsmöglichkeiten im Wege einer einstweiligen Anordnung des *1. Senats des BVerfG* eingeschränkt wurden.[60] Diese Vorratsdatenspeicherung und der Zugriff hierauf seien im Grundsatz heimlich angedacht, erfolgten unter Umständen für vielfältige Zwecke und über einen längeren Zeitraum. Infolgedessen betreffe die dort nötige Einschränkung strafprozessualer Zugriffsrechte eine gänzlich andere Konstellation.

(ii) Das *BVerfG* wechselt bei seiner Argumentation sodann von einer schutzfunktionalen[61] hin zu einer technisch-funktionalen Sichtweise und vergleicht die Speicherung einer »abgerufenen« E-Mail bei einem E-Mail-Provider mit der technisch äquivalenten Speicherung auf einem lokalen Rechner, welche ohnehin lediglich den Schutz aus §§ 94 ff. StPO genieße. Insofern sei keine über den Anfangsverdacht einer »einfachen« Straftat hinausgehende Verdachtsschwelle anzusetzen.

Das vermag nur teilweise zu überzeugen. Richtig ist zwar, dass im Rahmen einer Durchsuchung auch ein Zugriff auf räumlich getrennte Datenträger grundsätzlich ohne weitere Voraussetzungen zulässig ist (so nun auch § 110 Abs. 3 StPO[62]) und sich insoweit eine Speicherung gelesener E-Mail-Nachrichten bei einem E-Mail-Provider technisch-funktional nicht von einer Speicherung auf einer Internetfestplatte unterscheidet. Was aber soll die durch den *2. Senat* mühsam begründete Eröffnung des Schutzbereichs aus Art. 10 GG nützen, wenn sie keinen erhöhten – typisierten – Schutz mit sich bringt? Ebenso wenig beantwortet der *Senat* die Frage, warum gleiches auch für ungelesene E-Mails gelte.

(iii) Zudem ist zu beachten, dass Eingriffe aus §§ 94 ff. StPO dem in Art. 10 GG Betroffenen gegenüber nicht offen erfolgen müssen. Da die Herausgabe gespeicherter E-Mails durch den E-Mail-Provider erfolgen soll und dieser Gewahrsam an diesen Daten(trägern) hat, trifft diesen das Äquivalent zur Herausgabepflicht (§ 95 Abs. 1 StPO), namentlich die Pflicht zur Herstellung einer elektronischen Kopie. Diesem Betroffenen – also dem E-Mail-Provider – steht aber aufgrund des Gewahrsamsbezugs das Antragsrecht aus § 98 Abs. 2 Satz 1 StPO und wohl auch das Informationsrecht aus § 98 Abs. 2 Satz 6 StPO zu. Eine entsprechende Anwendung auf den Kunden ist zwar denkbar, jedenfalls aber nicht so weitreichend wie die detaillierte Regelung des § 101 Abs. 4, Abs. 5 StPO für den verdeckten Zugriff auf Post- (§ 99 StPO) oder laufende Telekommunikation (§ 100 a StPO).[63] Eine solche heimlich-kollusive Maßnahme ist zudem mit deutlich erhöhten Risiken verbunden, etwa den Rechtsschutz oder die Missbrauchsmöglichkeiten betreffend.

(iv) Umso mehr befremdet es, dass der *2. Senat des BVerfG* erst im weiteren Verlauf des Beschlusses solch heimlich-kollusive Zugriffe erstmals erwähnt, diese aus ermittlungstaktischen Gründen auch aus §§ 94 ff. StPO verfassungsrechtlich *obiter dictum* legitimiert und lediglich von einer Unterrichtung des Kunden »im Regelfall«[64] vor Durchführung der Maßnahme spricht, freilich mit dem Korrektiv einer nachträglichen Benachrichtigungspflicht. Diese Ausdehnung einer offenen hin zu einer auch heimlich durchführbaren Ermittlungsmaßnahme wäre auch im Rahmen der generellen Verhältnismäßigkeit zu berücksichtigen gewesen.

Der *2. Senat* setzt sich dabei lediglich mit einem offenen Zugriff mit Kenntnis des in Art. 10 GG Betroffenen auseinander und verlangt für diese Konstellation keine gesonderten Schutzstandards. Zumindest aber die den weiteren Passagen des Beschlusses zu entnehmende, partiell legitimierende Ausdehnung auch auf heimlich-kollusive Zugriffe widerspricht den Grundsätzen der Normenklarheit und -bestimmtheit und der Verhältnismäßigkeit im engeren Sinne, so dass zumindest für diese verfassungsrechtlich eine spezielle Ermächtigungsgrundlage zu verlangen ist.

4. Bei alledem ist aber der begrenzte Prüfungsgegenstand der verfassungsgerichtlichen Entscheidung zu berücksichtigen. Dieser ist auf die spezifische Verletzung von Verfassungsrecht begrenzt und beinhaltet eben nicht eine umfassende revisionsrechtliche Überprüfung der Anwendung einfachen Rechts (keine »Superrevisionsinstanz«).[65] Im verfassungsgerichtlichen Verfahren war lediglich gegenständlich, ob die Anwendung der §§ 94 ff. StPO den Vorgaben des GG entspricht – was das *BVerfG* bejahte. Hiervon zu differenzieren ist die *genuin strafprozessrechtliche* Frage, ob die Anwendung der §§ 94 ff. StPO auch einfach-gesetzlich stimmig ist, oder ob strafprozessrechtlich ein anderer – freilich auch den verfassungsrechtlichen Anforderungen entsprechender – Lösungsweg vorzugswürdig ist. Zur Klärung dieser Frage sind allein die Fachgerichte und damit zuvörderst der *BGH* berufen.[66]

IV. Zur genuin strafprozessualen Frage nach der relevanten Ermächtigungsgrundlage

1. Allein die Eröffnung des Schutzbereichs des Art. 10 Abs. 1 GG hilft jedoch bei der Bestimmung der richtigen Ermächtigungsgrundlage nicht weiter, da entgegen einer weit verbreiteten Auffassung §§ 100 a, 100 g, 100 h StPO für Eingriffe in die Telekommunikation keine abschließende Normen darstellen.[67] Denn jedenfalls auch § 99 StPO gestattet betreffend Telegramme Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG einschließlich des *Fernmeldegeheimnisses*[68], nach Auffassung des *BVerfG* auch § 94 StPO. Daher sind andere Abgrenzungskriterien heranzuziehen.

2. Der die *benutzerfremde Lagerung* (Phasen 4 und 6) von E-Mails thematisierende Beschluss des *1. Strafsenats des BGH* nähert sich diesem Aspekt aus dem Blickwinkel eines aufgrund seiner Heimlichkeit gefährlicheren, kollusiven Zugriffs ohne Wissen des E-Mail-Postfach-Inhabers, wie an dem Verweis auf die Benachrichtigungspflicht des § 101 Abs. 4, Abs. 5 StPO zu erkennen ist. Der Beschluss verdient jedenfalls dahingehend Zustimmung, dass der *1. Strafsenat* angesichts der auch von ihm gesehenen Eingriffstiefe keine künstliche Differenzierung zwischen bereits gelesenen und noch ungelesenen E-Mails vor-

59 BVerfG – 2 BvR 902/06 – Rz. 69; s. hierzu aber noch bei und mit Fn. 64.
60 S. oben Fn. 1.
61 Vgl. oben II. 2. b).
62 Neu gefasst durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. 12. 2007, BGBl. I 2008, S. 3198. Vgl. noch unten IV. 2. a).
63 Zudem ist der E-Mail-Provider zur Information des Kunden weder verpflichtet noch grenzenlos berechtigt.
64 Zunächst vorbehaltlos Rz. 69: »offene[r]« … Zugriff »mit Kenntnis des Betroffenen«. Anders dann erstmalig in Rz. 75 »in der Regel nicht heimlich, sondern offen«, noch deutlicher dann Rz. 94.
65 BVerfGE 1, 418, 420; BVerfGE 34, 269, 280; Dreier-GG/Wieland (Fn. 21) Art. 93 Rd. 34 m. w. N.; Bethge in: Maunz/Schmidt-Bleibtreu/Klein/Bethge (Hrsg.) BVerfGG, 29. Aufl. 2009, Vorbem. Rdn. 184 ff.
66 Ebenso ist es eine genuin ordnungsrechtliche und von der Verwaltungsgerichtsbarkeit zu klärende Frage, ob etwa § 4 Abs. 3 Satz 1 WpHG eine ausreichende Rechtsgrundlage für einen wertpapierordnungsrechtlichen Zugriff darstellt – für Phase 7 (zweifelhaft) bejahend VGH Kassel NJW 2009, 2470, 2471.
67 LG Hanau StV 2000, 354; LG Mannheim StV 2002, 242; KK-StPO/Nack (Fn. 3) § 100 a Rdn. 1.
68 Betreffend § 99 StPO vgl. nur KK-StPO/Nack (Fn. 3) § 99 Rdn. 1.

nimmt und zudem anerkennt, dass die Beschlagnahmevorschriften der §§ 94 ff. StPO alleine nicht ausreichen, sondern ein zusätzlicher Schutz – nach Auffassung des *Senats* durch §§ 99, 100 StPO – gewährleistet werden muss.[69]

a) Vom *1. Strafsenat* nicht näher diskutiert wird § 110 Abs. 3 StPO, dessen Anwendungsbereich begrenzt ist: Dieser setzt erstens eine rechtmäßige, offene Durchsuchung voraus, welche zweitens ein informationstechnisches System (»Speichermedium«) vorfinden muss. Drittens erlaubt er nur einen punktuellen Zugriff (Durchsicht), keine längerfristige Überwachung auch neu erstellter bzw. gespeicherter Daten. Ihrer Ratio nach verkörpert diese Norm die *technisch-funktionale* Theorie: Die lediglich räumliche Auslagerung sei technisch äquivalent zu einer lokalen Speicherung, infolgedessen müsse eine Durchsicht im Rahmen einer Durchsuchung gleichermaßen möglich sein. Daraus folgt aber auch, dass es sich um ein faktisch-funktional zur Auslagerung einer lokalen Speicherung genutztes, »räumlich getrennte[s] Speichermedium« handeln muss, auf das auch zuvor von dem aufgefundenen informationstechnischen System zugegriffen wurde.

Bei einem E-Mail-Postfach hingegen wird die Speicherung neuer Nachrichten durch den E-Mail-Provider bewirkt und stellt sich daher nicht als eine ausgelagerte Speicherung durch den von der Durchsuchung Betroffenen dar. Zudem enthält § 110 StPO in seiner jetzigen Fassung keine prozeduralen Sicherungen mehr,[70] welche dem spezifischen Gefährdungspotential und dem von Art. 10 GG geschützten, besonderen Vertrauensverhältnis zu Nachrichtenmittlern gerecht werden könnte. Daher ist § 110 Abs. 3 StPO – entgegen dem *BVerfG* und einer Auffassung in der Literatur[71] – auch als Rechtsgrundlage für offene Zugriffe auf E-Mail-Postfächer abzulehnen.

Jedenfalls aber ist § 110 Abs. 3 StPO nicht auf verdeckte oder kollusive Zugriffe anwendbar:[72] So muss jede Durchsuchung und damit regelmäßig ein intensiver Eingriff in durch Art. 13 GG geschützte Bereiche verhältnismäßig sein. Dieser vorgelagerte, typisierte Schutz würde umgangen, verzichtete man auf eine offene Durchsuchung zur Eröffnung des Anwendungsbereichs des § 110 StPO. Zudem verdeutlicht die Zwangswirkung einer Durchsuchung dem Betroffenen den Ernst der Lage, in der er sich befindet – und legt ihm daher implizit nahe, Rechtsschutzmöglichkeiten in Betracht zu ziehen. Darüber hinausgehend wird – eine dem Betroffenen zumeist höchst unerwünschte – Öffentlichkeitswirkung hergestellt, welche eine ausufernde Nutzung dieser Ermittlungsmaßnahme publik machen könnte. Gerade diesen Schutz durch das *Demos* können bloße Benachrichtigungspflichten und auch parlamentarische Aufsichtspflichten (vgl. etwa § 100 e StPO) nicht vollständig ersetzen.

b) (i) Der enge *Wortlaut* des § 99 StPO – der allerdings im Strafprozessrecht mit Ausnahme des Gebots der Normenklarheit bei Eingriffsnormen keine zwingende Grenze darstellt[73] – verweist lediglich auf Postsendungen und Telegramme. Auch die *Systematik* liefert kein schlüssiges Bild, denn selbst wenn der klassische Anwendungsbereich des § 100 a StPO die *laufende* Telekommunikation ist, so wird zumindest bei einer fortlaufenden Überwachung des Postverkehrs gem. § 99 StPO gleichermaßen in einen *laufenden* Kommunikationsprozess eingegriffen, wenn Briefe vor ihrer Lagerung in Postfächern oder vor ihrer Auslieferung ausgesondert werden. Nach Auffassung des *1. Strafsenats* scheitert die Anwendbarkeit des § 100 a StPO unter maßgeblichem Verweis auf die Kommentierung dieser Norm durch zwei seiner Richter[74] an dem Fehlen eines von dieser Norm implizit vorausgesetzten Telekommunikationsvorganges.[75]

(ii) Der *1. Strafsenat* behilft sich nun – ohne das Kind beim Namen zu nennen – mit einer *Analogie,*[76] um die Ermittlungstätigkeiten andernfalls behindernde Regelungslücke (insbesondere für kollusive Zugriffen) zu füllen: Entgegen seiner Auffassung ist die Interessenlage nicht mit § 99 StPO, sondern eher mit § 100 a StPO vergleichbar. Denn auch wenn die elektronische Post inzwischen in weiten Teilen Ersatz für Postsendungen geworden sein mag, so ist sie der herkömmlichen Post wesensmäßig verschieden – ob ihrer Verbreitung, ob ihrer Geschwindigkeit, ob ihrer Einsatzmöglichkeiten, aber auch ob der Angriffsvektoren.[77] Die anderen vom *Senat* genannten Kriterien – grundsätzliche Pflicht zur richterlichen Anordnung, Benachrichtigungspflicht (§ 101 Abs. 4 StPO) und nachträglicher Rechtsschutz (§ 101 Abs. 7 StPO) – gelten gleichermaßen für § 100 a StPO, so dass sie nicht die Vorzugswürdigkeit des § 99 StPO belegen können.

(iii) Bei aller Argumentation für die Anwendung des § 100 a StPO zum offenen wie kollusiven Zugriff auf ungelesene und gelesene E-Mails:[78] regelungstheoretisch handelt es sich sowohl bei §§ 100 a, 100 b StPO als auch bei §§ 99, 100 StPO um die materiell-rechtliche, konkretisierende und typisierende Absicherung der Verhältnismäßigkeit massiver Grundrechtseingriffe. Bei der Ausgestaltung dieser Typisierungen von Grundrechtseingriffen und deren Eingriffsschwellen besteht aber ein gewisser Gestaltungsspielraum; so war ein Verzicht auf das Erfordernis einer Katalogtat bei § 100 a StPO bei gleichzeitiger Stärkung anderer Voraussetzungen zur Telekommunikationsüberwachung in der rechtspolitischen Diskussion.[79] Diese Gestaltung der Schutzvorschriften hat bei §§ 99, 100 StPO in den Verfahrensvorschriften ihren Schwerpunkt, die insbesondere eine Durchsicht durch den Richter verlangen – und damit einen dem »Richterband« bei Telefon- und akustischer Wohnraumüberwachung vergleichbaren Kernbereichsschutz gewährleisten und auch sonst die Eingriffsintensität abmildern können.[80] Zudem hat auch bei § 99 StPO eine Verhältnismäßigkeitsprüfung zu erfolgen, die angesichts der erheblich betroffenen Grundrechtspositionen bei nicht schweren Straftaten die Anordnung einer verdeckt-kollusiven Durchsicht und erst recht einer Überwachung verwehren dürfte.[81]

Soweit man daher dem Rechtsanwender vertrauen kann, auch im Einzelfall die betroffenen Grundrechtspositionen und die Verhältnismäßigkeit bei einer Prüfung des § 99 StPO gleichermaßen streng zu berücksichtigen und sich infolgedessen *in praxi* ein vergleichbarer Schutzstandard zu §§ 100 a, 100 b StPO ergibt, ist *de lege ferenda* an sich nichts gegen eine Ausweitung des § 99 StPO auf elektronische Post einzuwenden. Allerdings spricht ob der Zerbrechlichkeit rechtsstaatlichen Strafrechts und auch aus Effektivitätsgesichtspunkten – schließlich könnte sich die richterliche Prüfung an dem gesetzlich vorgegebenen Maßstab orientieren – viel für eine weitergehende Typisierung der Verhält-

69 So i.E. auch BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 29 entgegen KK-StPO/Nack (Fn. 3) § 100 a Rdn. 22.

70 Vgl. zu dieser Aufweichung des § 110 StPO nur SK-StPO/Wohlers (Fn. 49) § 110 StPO Rdn. 3 ff.

71 Gercke in: Heidelberger Kommentar StPO, 4. Aufl. 2009, § 110 Rdn. 23; Meyer-Gossner (Fn. 32) § 100 a Rdn. 6; § 110 Rdn. 6; SK-StPO/Wohlers (Fn. 49) § 110 Rdn. 10; kritisch Schlegel HRRS 2008, 23, 28 f.

72 Bär MMR 2008, 221; Meyer-Gossner (Fn. 32) § 110 Rdn. 6, 8.

73 Aus diesem Grunde aber eine Analogie zu § 99 StPO ablehnend Gaede StV 2009, 96, 99 m. w. N.

74 KK-StPO/Nack (Fn. 3) § 100 a Rdn. 22 f.; BeckOK-StPO/Graf (Fn. 3) § 100 a Rdn. 28 ff. Vgl. ferner Th. Böckenförde (Fn. 53) 407 f.

75 Der freilich nicht mit § 3 Nr. 22 TKG gleichzusetzen ist, vgl. Gaede StV 2009, 96, 100 m. w. N.

76 Explizit jedoch in dieser Hinsicht LG Ravensburg NStZ 2003, 325.

77 So auch Gaede StV 2009, 96, 99.

78 BGH [ER] NJW 1997, 1934 sowie die in Fn. 32 Genannten.

79 BT-Drs. 16/3827 sah als limitierende Schranke vor, dass die vermuteten Umstände der Tat eine Freiheitsstrafe von mindestens einem Jahr erwarten ließ.

80 Vgl. zur früheren Rechtslage auch bei Durchsuchungen, § 110 Abs. 3 StPO a. F. SK-StPO/Wohlers (Fn. 49) § 110 StPO Rdn. 4 f.

81 Vgl. auch BeckOK-StPO/Graf (Fn. 3) § 99 Rdn. 5 f.; Meyer-Gossner (Fn. 32) § 99 Rdn. 12; KK-StPO/Nack (Fn. 3) § 99 Rdn. 10.

nismäßigkeitsprüfung, wie sie die zusätzlichen Voraussetzungen des § 100 a StPO enthalten.

c) Im gegenständlichen Verfahren, in dem zudem die Sicherstellung nicht explizit auf § 99 StPO gestützt war, wurden, soweit ersichtlich, die strengen verfahrensrechtlichen Korrektive des § 100 StPO zum weiteren Anwendungsbereich des § 99 StPO nicht eingehalten: diesbezüglich wendet der *1. Strafsenat* eine Widerspruchslösung an, die auch an anderer Stelle erheblicher Kritik ausgesetzt ist.[82] Insbesondere bei noch nicht höchstrichterlich geklärten Sachverhalten erscheint eine Pflicht des Verteidigers zum vorsorglichen Widerspruch bedenklich.

Gerade die Verfahrensvorschriften des § 100 StPO sind aber der Grund, weswegen der *1. Strafsenat* mit diesem Beschluss den Ermittlungsbehörden einen Bärendienst erwiesen hat: die Durchsicht der beschlagnahmten E-Mails – sprich: jegliche Betrachtung von Betreffzeile und Inhalt – hat grundsätzlich durch den (Ermittlungs-)Richter zu erfolgen, § 100 Abs. 3 Satz 1 StPO. Eine Übertragung ist nur auf die Staatsanwaltschaft – nicht auf deren Ermittlungspersonen[83] – und nur dann zulässig, wenn andernfalls der Untersuchungserfolg durch Verzögerung gefährdet wäre (§ 100 Abs. 3 Satz 2 StPO). Als eng auszulegende, gesetzliche Ausnahme von der Regelzuständigkeit darf eine solche Übertragung zudem nicht zum Regelfall werden. Die zusätzliche Belastung der Justiz durch den Einsatz dieses Ermittlungsinstruments darf daher nicht unterschätzt werden, was zudem als Nebeneffekt zu einer Zurückhaltung führen mag, dieses durchaus nützliche Ermittlungsinstrument einzusetzen. Auch aus ermittlungstaktischer Sicht erscheint daher das Regelungsmodell der §§ 100 a, 100 b StPO als vorzugswürdig, das zwar bei der Anordnung höhere Hürden vorsieht, aber eine effektivere Handhabung ermöglicht.

d) Eine Pflicht zur Bereitstellung von Kopien auch *gelesener* Nachrichten, die sich noch im E-Mail-Postfach befinden, wird vom *1. Strafsenat* bejaht. Dem ist zuzustimmen, weil es sich hierbei um Nachrichten handelt, die nach wie vor einem E-Mail-Provider anvertraut, in dessen Gewahrsam und weiterhin an den Empfänger gerichtet sind, und deren besondere Schutzbedürftigkeit durch spezielle verfahrensrechtliche Bestimmungen – dem *Strafsenat* nach gem. §§ 99, 100 StPO – gewährleistet wird. Allerdings haben E-Mail-Provider oftmals auch Zugriffsmöglichkeiten auf Nachrichten, die vom Empfänger bereits gelöscht wurden.[84] Stellt man mit dem *LG Hamburg* auf den Gewahrsam des E-Mail-Providers an einer Nachricht (bzw. hier an deren identische Kopie) als entscheidendes, auch zeitlich limitierendes Kriterium ab,[85] so wäre zwar ein Auskunftsverlangen gerichtet auf Recherche und Herausgabe von solchen vermeintlich oder reversibel gelöschten Nachrichten denkbar. Doch dies ginge zu weit: das Auskunftsverlangen ist konzipiert als milderes Mittel, durch welches regelmäßig nur Verkehrsdaten und nicht Inhaltsdaten erhoben werden.[86] Für den Zugriff auf Verkehrsdaten auch vorangegangener Telekommunikation existiert mit § 100 g StPO eine *lex specialis*, welche mit speziellen Schutzmechanismen (etwa der Pflicht zur Löschung binnen eines Monats nach Ablauf der sechsmonatigen Speicherpflicht, § 113 a Abs. 11 TKG) versehen ist, die durch einen Rückgriff auf §§ 99, 100 StPO umgangen würde. Allein *a fortiori* wäre ein Zugriff auch auf Inhaltsdaten, wenn sich die Nachricht etwa nur in Sicherungskopien des E-Mail-Providers befindet, engeren Schranken zu unterwerfen.[87]

Für ein Auskunftsverlangen verbleibt daher kein Raum: Verkehrsdaten laufender oder zukünftiger E-Mail-Kommunikation unterliegen dem Zugriff gem. § 100 g StPO; bei Inhaltsdaten ist, nach Auffassung des *1. Strafsenats* gem. §§ 99, 100 StPO, ein Zugriff auf noch im Postfach gespeicherte Nachrichten möglich. Die Nutzung darüber hinausgehender Zugriffsmöglichkeiten des E-Mail-Providers auf vom Benutzer »gelöschte« Nachrichten ist mangels Rechtsgrundlage *de lege lata* unzulässig.

3. Folgt man der Analogie des *1. Strafsenats*, so ist neben der Durchsicht auch die Überwachung, also die *Einlagerung neuer Nachrichten* (Phase 4) an §§ 99, 100 StPO zu messen, nach hier vertretener und mit § 110 TKG besser zu vereinbarender Auffassung an §§ 100 a, 100 b StPO. Allerdings bereitet die entsprechende Anwendung des Procedere des § 100 Abs. 3 Satz 4, Abs. 5 und Abs. 6 StPO Schwierigkeiten: Eine auf §§ 94 ff., 99 StPO gestützte Beschlagnahme dient primär zur Sicherung eines potentiellen Beweismittels, und in diesem Aspekt erschöpft sich an sich auch der Grund für eine Zurückbehaltung einer Postsendung.[88] Bei E-Mails ist eine solche Vorgehensweise aber grundsätzlich nicht erforderlich, da exakte elektronische Kopien einer E-Mail denselben potentiellen Beweiswert und Ermittlungsnutzen aufweisen. Daher ist an die bloße Erstellung von Kopien des Postfachs des Betroffenen und eingehender Nachrichten als milderes Mittel zu denken, welche dann verschlüsselt dem zuständigen Richter zugeleitet werden.[89] Insoweit erübrigt sich dann auch die Anwendung des § 100 Abs. 5, Abs. 6 StPO. Nun wird für zulässig erachtet, Sendungen, die sich aufgrund einer Postbeschlagnahme bereits bei den Ermittlungsbehörden befinden, auch zur Sicherstellung einer Einziehung zu beschlagnahmen (§§ 111 b ff. StPO),[90] etwa wenn es sich um eine kinderpornographische Schrift handelt (§ 184 b Abs. 4, Abs. 6 StGB i. V. m. §§ 74, 74 a StGB). Einer der Zwecke einer Einziehung, die Verhinderung einer Perpetuierung der durch den Gegenstand[91] ausgehenden Gefahr (arg. ex. § 74 Abs. 2 Nr. 2 StGB) – etwa eine weitere Verbreitung von kinderpornographischen Schriften –, würde durch eine Auslieferung einer einschlägigen E-Mail beeinträchtigt. Für solche Konstellationen muss daher ein Rückgriff auf die Methode des § 100 Abs. 5, Abs. 6 StPO verbleiben, so dass eine E-Mail erst nach richterlicher Freigabe in das Postfach des Empfängers gelangt.

4. Ein Abgreifen der E-Mail-Kommunikation in den *Übertragungsstadien* (Phasen 2, 3 und 5) ist im Rahmen des § 100 a StPO zulässig, da es sich hierbei unstreitig um einen laufenden Telekommunikationsvorgang handelt.[92] Nach nicht unumstrit-

82 Vgl. nur die Nachw. bei Meyer-Gossner (Fn. 32) § 136 Rdn. 25 sowie BGHSt 23, 329, 331 (Verwertungsverbot bei Verstoß gegen § 99 StPO).

83 Arg. e contrario § 100 b Abs. 3 StPO; BeckOK-StPO/Graf (Fn. 3) § 100 Rdn. 16.

84 Man denke allein an Sicherungskopien; vgl. oben bei und mit Fn. 8 sowie auch VGH Kassel NJW 2009, 2470, 2470.

85 LG Hamburg StV 2009, 404. In diese Richtung ebenfalls LR/Schäfer (Fn. 49) § 99 Rdn. 30; noch weitergehend die Gegenauffassung von BeckOK-StPO/Graf (Fn. 3) § 99 Rdn. 16; KK-StPO/Nack (Fn. 3) § 99 Rdn. 11 unter Verweis auf Nr. 84 RiStBV.

86 Vgl. Meyer-Gossner (Fn. 32) § 99 Rdn. 14 f.; LR/Schäfer (Fn. 49) § 99 Rdn. 29.

87 Zudem liefe das gegen höhere Schutzstandards bei bereits gelesenen Nachrichten ins Feld gebrachte Argument fehl, der Empfänger habe schließlich die Chance zur Löschung gehabt, wenn auf »gelöschte« Nachrichten gleichermaßen zugegriffen werden könnte.

88 Meyer-Gossner (Fn. 32) § 94 Rdn. 6 ff.; LR/Schäfer (Fn. 49) § 94 Rdn. 1.

89 Eine solche Reduktion des Eingriffs wird etwa auch für zulässig erachtet betreffend Auskunftsverlangen, jedenfalls soweit sie sich auf Sendungen beziehen, die sich noch im Gewahrsam des Postdienstleisters befinden und daher einer Postbeschlagnahme zur Verfügung stünden. Vgl. hierzu nur LR/Schäfer (Fn. 49) § 99 Rdn. 29.

90 Meyer-Gossner (Fn. 32) § 94 Rdn. 2; LR/Schäfer (Fn. 49) § 94 Rdn. 7 f. Diesen Aspekt übersieht Th. Böckenförde (Fn. 53) 410 ff.

91 Betreffend § 94 ff. StPO werden digital gespeicherte Informationen entweder als Gegenstände aufgefasst (so Meyer-Gossner [Fn. 32] § 136 Rdn. 25; BVerfGE 113, 29, 50; BVerfG – 2 BvR 902/06 – Rz. 63), oder aber es wird a maiore ad minus die Anfertigung einer digitalen Kopie als milderer Eingriff akzeptiert, gestützt auf dieselbe Eingriffsnorm (so etwa LR/Schäfer [Fn. 49] § 94 Rdn. 14 m.w.N). Diese Wertung dürfte auf §§ 74 ff. StGB, §§ 111 b ff. StPO übertragen werden können, wenn auch eine gesetzliche Klarstellung wünschenswert wäre. Kritisch jedoch OLG Celle, Urt. v. 17. 9. 2008 – 31 Ss 21/08 (»gesetzlich so nicht vorgesehen«).

92 Vgl. allein BGH NStZ 1997, 247 sowie KK-StPO/Nack (Fn. 3) § 100 a Rdn. 21; Th. Böckenförde (Fn. 53) 440 f.

tener Rechtsprechung[93] schließt diese Befugnis ein, dass das informationstechnische System manipuliert werden darf, um ausgehende E-Mails auch an Strafverfolgungsbehörden auszuleiten (Quellen-TKÜ). Angesichts des Bezugs nur auf Telekommunikationsdaten darf dies aber erst geschehen, sobald Daten vom Absender verschickt werden (Phase 2) und daher nicht Entwürfe erfassen.[94] Ob das zusätzliche verfassungsrechtliche Erfordernis einer technischen und rechtlichen Absicherung gegen überschießende Datenerhebungen durch § 100 b Abs. 2 Nr. 3 StPO möglich ist, muss angezweifelt werden.[95]

De lege lata fehlt eine weitergehende Rechtsgrundlage zu einem *verdeckten Zugriff* auf informationstechnische Systeme, d. h. ohne oder gegen den Willen der jeweiligen Administrationsberechtigten. Dies schließt »brute force«-Angriffe zum Erraten bzw. Ermitteln von Passwörtern gleichermaßen aus wie die Installation von RFS.

V. Verhältnismäßigkeit des Einzelfalls

Bei allem Streit über die strafprozessuale Ermächtigungsgrundlage als erste Stufe eines typisierten Grundrechtsschutzes darf – und insoweit muss dem *BVerfG* einschränkungslos zugestimmt werden – die zweite Stufe einer fallspezifischen Verhältnismäßigkeitsprüfung nicht übersehen werden. Neben den genannten Abwägungsfaktoren[96] muss hierbei auch Berücksichtigung finden, ob im Einzelfall Möglichkeiten zu einer Milderung des Eingriffs bestehen, insbesondere wenn diese die Effektivität der Strafverfolgung nur marginal beeinträchtigen.

So ist etwa technisch an eine zeitliche oder inhaltliche Begrenzung der zunächst abgegriffenen E-Mails zu denken, etwa unter Einsatz von geeigneten Suchbegriffen. Dies gilt auch für das Stadium einer Durchsicht vor einer endgültigen Beschlagnahme, wie es sowohl §§ 99, 100 StPO als auch § 110 StPO vorsehen. Auch wird es regelmäßig milder sein, einen Drittbetroffenen (etwa eine unverdächtige Kontaktperson) an der Sichtung nach verfahrensrelevanten Nachrichten zu beteiligen.

All diese Aspekte erwähnt das *BVerfG* zwar in seinem Beschluss. Angesichts des Verves, mit dem die *2. Kammer des 2. Senats* in ihren einstweiligen Anordnungen vorging und sogar eine Lagerung und Versiegelung bei einem Amtsgericht anordnete, verwundert die ausnahmslos positive Bewertung der Verhältnismäßigkeit durch den *Senat*. Nur als Beispiel sei genannt, dass in diesem eine unverdächtige Kontaktperson betreffenden Einzelfall *auch* eine Sicherstellung von Nachrichten eines neunmonatigen Zeitraums erfolgte, die nicht verfahrensrelevant sein konnten.

VI. Transnationale Komponenten

Sind Daten im Ausland gespeichert – angesichts der internationalen Natur des Internets eher der Regelfall –, so ist ein Zugriff eine völkerrechtlich relevante, extraterritoriale Ausübung von Hoheitsrechten,[97] welche ein Rechtshilfeersuchen erfordern und eigenständige, nicht-einvernehmliche Zugriffe ausschließen.[98] Vorläufige Sicherungsverfahren nach dem inzwischen auch von Deutschland ratifizierten Europarats-Übereinkommen über Computerkriminalität[99] ermöglichen es, Einwirkungen auf Beweismittel schnell Einhalt zu gebieten. Eingehende Rechtshilfeersuchen verlangen eine vollständige Umsetzung (§ 59 Abs. 3 IRG), so dass etwa eine TKÜ auch gem. § 100 a StPO durch einen deutschen Richter angeordnet werden muss, der dabei u. a. das Vorliegen eines qualifizierten Tatverdachts einer Katalogtat feststellen muss.[100] Eine internationale Herausgabe von E-Mail-Kopien etwa nach einer (Post-)Beschlagnahme, aber auch nach doppelfunktionalen Auskunftsverlangen – etwa gem. §§ 4 Abs. 3 Satz 1, 7 WpHG[101] – ist mindestens von der zusätzlichen Voraussetzung des § 66 Abs. 2 Nr. 1 IRG (beiderseitige Ahndbarkeit) abhängig: zutreffenderweise findet § 66 IRG direkt auf nichtkörperliche Gegenstände Anwendung;[102] die Gegenauffassung folgt der Verweisung des § 67 Abs. 2 Satz 1 IRG[103] und begrenzt insoweit nur den Drittrechtsschutz.[104]

Innerhalb der EU existiert für eine *laufende Überwachung der Telekommunikation* durch das Rechtshilfeübereinkommen von 2000[105] ein spezielles Regime.[106] Für die vorläufige Sicherung[107] von gespeicherten E-Mails kommt die Europäische Sicherstellungsanordnung[108] in Betracht, welche bei bestimmten Listendelikten die Prüfung der beiderseitigen Strafbarkeit (der vermuteten Tat) entbehrlich macht, vgl. § 94 Abs. 1 Nr. 1 IRG. Zudem sieht diese eine entsprechende, extraterritoriale Anwendung prozeduraler Bestimmungen vor – man denke etwa an § 100 StPO.[109] *De lege ferenda*[110] soll der Grundsatz der gegen-

93 BVerfGE 120, 274, 309. Vgl. Fn. 15.

94 Anderes gilt selbstredend, soweit Entwürfe nur zum Schein erstellt werden, dank des Zugriffs mehrerer auf dasselbe Postfach in Wahrheit aber bereits Telekommunikation vorliegt. Zu weitgehend allerdings Hornick StraFo 2008, 281, 284.

95 KK-StPO/Nack (Fn. 3) § 100 a Rdn. 16 (»derzeit keine Rechtsgrundlage«) will dennoch eine Quellen-TKÜ vorrübergehend auf diese Norm stützen. Vgl. ferner Hornung CR 2008, 299, 300 f. zu den technischen Schwierigkeiten (schlicht unerfüllbar).

96 S. oben III. 3.

97 LG Hamburg StV 2009, 70, 71; Gaede StV 2009, 96, 101 f.; Gercke StraFo 2009, 271, 272 f.

98 Zutr. unter Verweis auch auf die Regelungen des Europarats-Übereinkommens über Computerkriminalität Gaede StV 2009, 96, 101 m. umfangr. Nachw. Vgl. ferner HK-StPO/Gercke (Fn. 71) § 110 Rdn. 26 ff. zu den sich hieraus ergebenden Konsequenzen zu Überprüfungspflichten und Beweisverwertungsverboten.

99 Vgl. etwa Art. 16, 29 des Übereinkommens, abgedruckt in BGBl 2008 II, S. 1242.

100 Nr. 77 a Abs. 1 S. 2 RiVASt; Schuster NStZ 2006, 657, 659; Wilkitzki in: Grützner/Pötz/Kreß (Hrsg.) Internationaler Rechtshilfeverkehr in Strafsachen (Stand: Juli 2009) § 59 IRG Rdn. 20 Fn. 7.

101 Bei VGH Kassel NJW 2009, 2470 wäre wegen der verfahrensgegenständlichen doppelfunktionalen Maßnahme eine Prüfung auch der strafprozessualen Eingriffsgrundlagen notwendig gewesen; vgl. Vogel in: Assmann/Schneider (Hrsg.) WpHG, 5. Aufl. 2009, § 7 Rdn. 36 f., 41.

102 BGHSt 27, 222, 226 ff.; BGHSt 33, 196, 209 ff.; Lagodny in: Schomburg/Lagodny/Gleß/Hackner (Hrsg.) Internationale Rechtshilfe in Strafsachen, 4. Aufl. 2006, § 66 IRG Rdn. 7 f. Dies ist auch makrosystematisch stimmig, vgl. bei und mit Fn. 91.

103 Grützner/Pötz/Kreß/Wilkitzki (Fn. 100) § 66 Rdn. 3, § 67 IRG Rdn. 9 f.

104 § 61 Abs. 1 Satz 2 IRG bezieht sich nur auf § 66 IRG und nicht auch auf § 67 Abs. 2 IRG. Die Zulässigkeitsprüfung des OLG ist auf die Prüfung der Drittbelange (wie Geheimhaltungsinteressen, vgl. BGHSt 33, 196, 214 ff.) beschränkt. Dritter ist jeder, der nicht Verfolgter im ausländischen Strafverfahren ist (OLG Köln, Beschl. v. 27. 7. 2004 – Ausl 92/04). Neben Unternehmen (so bei VGH Kassel NJW 2009, 2470; vgl. hierzu bereits Fn. 101) kommen daher auch E-Mail-Provider als Antragsberechtigte in Betracht.

105 Übereinkommen vom 29. 5. 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, AblEG C 197 vom 12. 7. 2000, S. 3.

106 Vertiefend Schuster NStZ 2006, 657, 663.

107 Für den nachfolgenden Zugriff kann auf § 97 IRG und auf den noch umzusetzenden Rahmenbeschluss 2008/978/JI des Rates vom 18. Dezember 2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen (AblEU L 350 vom 29. 12. 2008, S. 72) verwiesen werden, welcher ebenfalls dem Grundsatz der gegenseitigen Anerkennung verpflichtet ist und erstmalig besondere Schutzmechanismen (in Art. 10 Abs. 3) vorsieht. Vgl. Kotzurek ZIS 2006, 123; Krüssmann StraFo 2008, 458.

108 Rahmenbeschluss 2003/577/JI des Rates vom 22. Juli 2003 über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union, AblEU L 196 vom 1. 11. 2003, S. 45.

109 Vgl. dessen Art. 5 Abs. 1 Unterabs. 2.

110 Vgl. KOM(2009) 262 endg. vom 10. 6. 2009, S. 19. Festgehalten werden soll aber an einem Zustimmungserfordernis vor einem extraterritorialen Zugriff (Ratsdok. 15569/08, S. 5). Zumindest in denjenigen Fällen eines offenen oder kollusiven Zugriffs, in denen keine Mitwirkung des anderen Staates erforderlich ist, erscheint der Weg der Art. 19, 20 des

seitigen Anerkennung ausgedehnt werden, was die Bedeutung europarechtlicher Garantien auch im Hinblick auf eine Typisierung und Effektivierung des Verhältnismäßigkeitsschutzes[111] bei der Anordnung von Ermittlungsmaßnahmen verdeutlicht.

Viele entscheidende Fragen müssen daher auf europäischer und internationaler Ebene geklärt werden: Was nützt deutschen Ermittlungsbehörden ein national umfangreiches Zugriffsrecht, wenn die Daten für diese Behörden unerreichbar im Ausland gespeichert sind; was nützt den Einwohnern Deutschlands ein hoher Schutzstandard, wenn dieser durch parallele Ermittlungen ausländischer Ermittlungsbehörden untergraben werden kann? Eine langfristige Effektivierung und Sicherung der vielfältigen Nutzungsmöglichkeiten des Internets erfordert daher neben einer Schließung der wenigen verbliebenen – oder vermeintlichen? – »rechtsfreien Räume« auch ein wachsendes, internationales rechtspolitisches Bewusstsein für die Notwendigkeit einer Verhältnismäßigkeit staatlicher Maßnahmen als Ausprägung des Rechtsstaatsprinzips.

VII. Konsequenzen

1. Die Rechtslage zum strafprozessualen Zugriff auf E-Mail-Kommunikation gestaltet sich demzufolge nach wie vor schwierig. Bis zu einem Federstrich des Gesetzgebers, der die bestehenden Unklarheiten und Widersprüche lösen und verfassungsrechtlich unbedenklich etwa § 99 oder § 100 a StPO auf alle benutzerfernen Zugriffe auf E-Mail-Kommunikation ausdehnen könnte, ist es notwendig, zwischen verschiedenen Fallgruppen – sowohl in Bezug auf eine einmalige Durchsicht als auch auf eine laufende Überwachung – zu differenzieren.

2. Bei einer einmaligen Durchsicht, d. h. wenn es in einem Ermittlungsverfahren erforderlich ist, *lagernde* bzw. archivierte E-Mail-Kommunikation durchzusehen, ist nach dem Speicherort zu unterscheiden:

a) *Privatrechner.*[112] Auf einen *offenen* Zugriff finden die herkömmlichen Durchsuchungs- und Beschlagnahmevorschriften der §§ 94 ff., 102 ff. StPO Anwendung. Allerdings ist bei der Sicherstellung, Beschlagnahme und Auswertung die besondere Schutzbedürftigkeit früherer Kommunikationsinhalte und kernbereichsrelevanter Daten zu berücksichtigen.[113] Ein *verdeckter* Zugriff (»Online-Durchsuchung«) ist *de lege lata* unzulässig.

b) *E-Mail-Provider.*[114] Lagern Nachrichten bei einem E-Mail-Provider – sei es bei einem dezidierten Unternehmen, bei einer IT-Abteilung oder bei einer Universitätseinrichtung – so ist nach der auch hier vertretenen Literaturauffassung stets § 100 a StPO heranzuziehen. Nach der Rechtsprechung ist grundsätzlich §§ 99, 100 StPO (analog) anzuwenden. Erfolgt aber der Zugriff im Kontext einer Durchsuchung beim Betroffenen, sei ein Zugriff gem. §§ 94 ff., 102 ff., 110 Abs. 3 StPO möglich. Ein dem E-Mail-Provider gegenüber *verdeckter* Zugriff ist unzulässig und angesichts § 100 b Abs. 3 StPO, § 110 TKG auch regelmäßig nicht erforderlich. Ebenso unzulässig ist eine Wiederherstellung bereits gelöschter Nachrichten, etwa mit Hilfe von Sicherungskopien. Die Diensteanbieter sind nur zur Mitwirkung an rechtmäßigen Maßnahmen verpflichtet.

Die Ermittlungsbehörden trifft eine Prüfungspflicht, ob der physikalische Speicherort im Ausland gelegen ist, da sodann ein Fall internationaler Rechtshilfe in Strafsachen vorliegt. Innerhalb der EU ist eine Beweissicherung durch die Europäische Sicherstellungsanordnung (vgl. § 94 IRG) erleichtert. Im Geltungsbereich des Übereinkommens über Computerkriminalität – praktisch bedeutsam sind hier die USA – stehen dessen vorläufige Sicherungsmaßnahmen zur Verfügung.[115]

c) *Sonstige Dritte.*[116] Bei sonstiger benutzerfremder Speicherung verwehrt die Rechtsprechung einen über §§ 94 ff. StPO erhöhten, typisierten Schutz. Dies ist trotz der besonders strikten Einzelfallprüfung der Verhältnismäßigkeit zumindest in Fällen eines kollusiven Zugriffs – nicht nur Art. 8 EMRK wegen – bedenklich.

3. Ist ein Zugriff (auch) auf *zukünftige* Nachrichten erforderlich, liegt also eine laufende Überwachung vor, so ist erneut der Zugriffsort entscheidend:

a) *Arbeitsplatz-* oder *Privatrechner.*[117] Bei einer lokalen Erstellung einer Nachricht ist ein *verdecktes* Abgreifen bereits des Entwurfs unzulässig. Erst mit dem Absenden kommt (zweifelhafterweise) eine auf § 100 a StPO gestützte Quellen-TKÜ in Betracht. Werden E-Mail-Entwürfe ganz oder teilweise an einen E-Mail-Provider übertragen, so greift nach der hier vertretenen Auffassung durchgängig der Schutz des § 100 a StPO. Nach der Rechtsprechung ist auch ein Zugriff beim E-Mail-Provider gemäß §§ 99, 100 StPO denkbar.

b) *Übertragungsweg.*[118] Ein Abgreifen laufender Telekommunikation ist in den Grenzen des § 100 a StPO zulässig; § 100 b Abs. 3 StPO, § 110 TKG verpflichten die Diensteanbieter zur Mitwirkung. In EU-Auslandskonstellationen erleichtert das Rechtshilfeübereinkommen von 2000 die Überwachung.

c) *E-Mail-Provider.*[119] Nach hier vertretener Auffassung greift § 100 a StPO auch zum Zugriff auf bei E-Mail-Providern neu eingehende Nachrichten und -entwürfe. Der *1. Strafsenat des BGH* wendet hingegen §§ 99, 100 StPO (analog) an.

4. *Zufallsfunde,* die im Rahmen einer rechtmäßig angeordneten und durchgeführten Telekommunikationsüberwachung gem. § 100 a StPO erlangt wurden, dürfen in den Grenzen des § 477 Abs. 2 S. 2 StPO verwertet werden. Zufallsfunde bei einer (Post-)Beschlagnahme sind stets verwertbar (vgl. § 108 StPO), sofern dies nicht im Einzelfall unverhältnismäßig wäre.

5. *Beweisverwertungsverbote* kommen – über den Kernbereichsschutz hinaus, vgl. § 100 a Abs. 4 StPO – jedenfalls dann in Betracht, wenn eine verdeckte Online-Durchsuchung erfolgte, wenn eine verdeckte bzw. kollusive Ermittlungsmaßnahme unter Umgehung jeglichen zusätzlichen Schutzes (sei es aus §§ 99, 100 StPO, sei es aus §§ 100 a, 100 b StPO) angeordnet wurde, oder aber wenn ohne jegliche Nachprüfung hingenommen wurde, dass (möglicherweise) auf im Ausland gespeicherte Nachrichten zugegriffen wurde, um ein sonst notwendiges Rechtshilfeverfahren zu umgehen.[120]

Hingegen mag zwar ein Zugriff gem. § 110 Abs. 3 StPO im Rahmen einer offenen Hausdurchsuchung genauso rechtsfehlerhaft (wenn auch verfassungsrechtlich durch den *2. Senat des BVerfG* akzeptiert) sein wie eine extensive, analoge Anwendung der §§ 99, 100 StPO. Allein dies überschreitet aber nicht die zur Annahme eines Beweisverwertungsverbots von der Rechtsprechung geforderten Hürden[121] eines willkürlichen oder erheblichen Verfahrensverstoßes zu Lasten des Betroffenen.

6. Fazit. Der Meinungsstreit über die verschiedenen Fallgruppen und die jeweils anwendbaren Rechtsgrundlagen zum strafprozessualen Zugriff auf E-Mail-Kommunikation – vorrangig

Rechtshilfeübereinkommens von 2000 (Fn. 105) vorzugswürdig, welcher zwischen den beteiligten Staaten lediglich Informationspflichten und nachträgliche Widerspruchsrechte vorsieht.

111 Vgl. hierzu oben II. 5.

112 S. weitergehend oben II. 3. a), IV. 4.

113 Vgl. nur BVerfGE 115, 166 (LS 3).

114 Ausführliche Darstellung oben II. 2. f), IV. 2.

115 S. oben VI. Zu den technischen Möglichkeiten vgl. nur HK-StPO/Gercke (Fn. 71) § 110 Rdn. 28.

116 S. oben II. 3. a), III. 3. c) (ii), IV. 2. a) sowie auch VGH Kassel NJW 2009, 2470.

117 S. oben II. 3. c), IV. 4.

118 S. oben II. 2. f), IV. 4. sowie zu Auslandskonstellationen VI.

119 S. oben II. 2. f), IV. 3.

120 Dies beruht auf dem Verstoß gegen ein faires Verfahren. So auch HK-StPO/Gercke (Fn. 71) § 110 Rdn. 29; ders. StraFo 2009, 271, 274.

121 Vgl. zuletzt BVerfG, Beschl. v. 2. 7. 2009 – 2 BvR 2225/08, aber auch den strengen Maßstab bzgl. § 99 StPO in BGHSt 23, 329, 331.

§§ 100 a, 100 b StPO (so die Literatur), vorrangig §§ 99, 100 StPO (so der *1. Strafsenat des BGH*) oder, zumindest bei offenen Zugriffen mit Wissen des Beschuldigten, §§ 94 ff., 110 Abs. 3 StPO (so der *2. Senat des BVerfG*) – ist auch nach den neueren höchstrichterlichen Entscheidungen nicht abschließend geklärt. Diese Diskussion beruht rechtspolitisch vor allem auf unterschiedlichen Auffassungen, ob angesichts der betroffenen Grundrechtspositionen (insbesondere aus Art. 10 GG) ein typisierter und näher spezifizierter Schutz der Verhältnismäßigkeit erforderlich ist. Das *BVerfG* verneint dies, legt aber immer größeren Wert auf eine umfassende *Einzelfallprüfung der Verhältnismäßigkeit*.[122] Das führt zu erhöhten Anforderungen an und Schwierigkeiten für die Rechtspraxis bei den zumeist amtsgerichtlichen Anordnungen von Ermittlungsmaßnahmen, der für diese Prüfung gesetzliche Leitlinien fehlen, wie sie etwa bei §§ 100 a, 100 b StPO vorlägen. Soweit die Rechtsanwender in jedem Einzelfall fundierte Bewertungen der Grundrechtspositionen und der Verhältnismäßigkeit vornehmen, ist es aber zweifelsohne auch auf diesem Wege möglich – wenn auch weniger effektiv – den verfassungsrechtlich gebotenen Grundrechtsschutz zu gewährleisten.

122 Näher oben V., zu den Kriterien vgl. ferner III. 3.