L e i t s a t z

zum Beschluss des Zweiten Senats vom 16. Juni 2009

- 2 BvR 902/06 -

Die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers sind am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen. §§ 94 ff. StPO genügen den verfassungsrechtlichen Anforderungen, die an eine gesetzliche Ermächtigung für solche Eingriffe in das Fernmeldegeheimnis zu stellen sind.

BUNDESVERFASSUNGSGERICHT

**- 2 BVR 902/06 -**

**Im Namen des Volkes**

**In dem Verfahren**
**über**
**die Verfassungsbeschwerde**

des Herrn B…

- Bevollmächtigte: Rechtsanwälte Johannes Eisenberg und Dr. Stefan König, Görlitzer Straße 74, 10997 Berlin -

gegen a) den Beschluss des Landgerichts Braunschweig vom 12. April 2006 - 6 Qs 88/06 und 97/06 -,

b) den Beschluss des Amtsgerichts Braunschweig vom 22. März 2006 - 3 Gs 844/06 -,

c) den Beschluss des Amtsgerichts Braunschweig vom 14. März 2006 - 3 Gs 844/06 -

und Antrag auf Erlass einer einstweiligen Anordnung

hat das Bundesverfassungsgericht - Zweiter Senat - unter Mitwirkung der Richterinnen und Richter

Vizepräsident Voßkuhle,
Broß,
Osterloh,
Di Fabio,
Mellinghoff,
Lübbe-Wolff,
Gerhardt,
Landau

am 16. Juni 2009 beschlossen:

Die Verfassungsbeschwerde wird zurückgewiesen.

Die einstweilige Anordnung wird mit der Entscheidung in der Hauptsache gegenstandslos.

## Gründe:

### A.

Die Verfassungsbeschwerde richtet sich gegen die Beschlagnahme von E-Mails des Beschwerdeführers auf dem Mailserver seines Providers in einem gegen Dritte gerichteten strafrechtlichen Ermittlungsverfahren. 1

### I.

1. Die vorläufige Sicherstellung und die förmliche Beschlagnahme von Beweisgegenständen ist in § 94 StPO geregelt. Die Vorschrift lautet in ihrer Fassung vom 7. April 1987 (BGBl I S. 1074, 1319): 2

§ 94 StPO 3

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. 4

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme. 5

(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen. 6

Die formellen Voraussetzungen einer Beschlagnahme von Beweisgegenständen sind in § 98 StPO geregelt. Die Vorschrift lautete in der bei Erlass der angegriffenen Beschlüsse geltenden Fassung vom 24. August 2004 (BGBl I S. 2198): 7

§ 98 8

(1) Beschlagnahmen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Die Beschlagnahme nach § 97 Abs. 5 Satz 2 in den Räumen einer Redaktion, eines Verlages, einer Druckerei oder einer Rundfunkanstalt darf nur durch den Richter angeordnet werden. 9

(2) Der Beamte, der einen Gegenstand ohne richterliche Anordnung beschlagnahmt hat, soll binnen drei Tagen die richterliche Bestätigung beantragen, wenn bei der Beschlagnahme weder der davon Betroffene noch ein erwachsener Angehöriger anwesend war oder wenn der Betroffene und im Falle seiner Abwesenheit ein erwachsener Angehöriger des Betroffenen gegen die Beschlagnahme ausdrücklichen Widerspruch erhoben hat. Der Betroffene kann jederzeit die richterliche Entscheidung beantragen. Solange die öffentliche Klage noch nicht erhoben ist, entscheidet das Amtsgericht, in dessen Bezirk die Beschlagnahme stattgefunden hat. Hat bereits eine Beschlagnahme, Postbeschlagnahme oder Durchsuchung in einem anderen Bezirk stattgefunden, so entscheidet das Amtsgericht, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat, die das Ermittlungsverfahren führt. Der Betroffene kann den Antrag auch in diesem Fall bei dem Amtsgericht einreichen, in dessen Bezirk 10

die Beschlagnahme stattgefunden hat. Ist dieses Amtsgericht nach Satz 4 unzuständig, so leitet der Richter den Antrag dem zuständigen Amtsgericht zu. Der Betroffene ist über seine Rechte zu belehren.

(3) Ist nach erhobener öffentlicher Klage die Beschlagnahme durch die Staatsanwaltschaft oder eine ihrer Ermittlungspersonen erfolgt, so ist binnen drei Tagen dem Richter von der Beschlagnahme Anzeige zu machen; die beschlagnahmten Gegenstände sind ihm zur Verfügung zu stellen. 11

(4) Wird eine Beschlagnahme in einem Dienstgebäude oder einer nicht allgemein zugänglichen Einrichtung oder Anlage der Bundeswehr erforderlich, so wird die vorgesetzte Dienststelle der Bundeswehr um ihre Durchführung ersucht. Die ersuchende Stelle ist zur Mitwirkung berechtigt. Des Ersuchens bedarf es nicht, wenn die Beschlagnahme in Räumen vorzunehmen ist, die ausschließlich von anderen Personen als Soldaten bewohnt werden. 12

2. Der Prüfung, ob die nach § 94 Abs. 1 StPO vorläufig sichergestellten Gegenstände gemäß § 94 Abs. 2 StPO als Beweismittel zu beschlagnahmen sind, dient die Durchsicht gemäß § 110 StPO. Ursprünglich war die Durchsicht dem Ermittlungsrichter vorbehalten. Seit dem Ersten Gesetz zur Reform des Strafverfahrensrechts vom 9. Dezember 1974 (BGBl I S. 3393, 3533) ist für die Durchsicht die Staatsanwaltschaft zuständig, sofern nicht der betroffene Inhaber die Durchsicht durch andere Beamte genehmigt. Durch das Erste Gesetz zur Modernisierung der Justiz vom 24. August 2004 (BGBl I S. 2198) wurde mit Wirkung zum 1. September 2004 die zusätzliche Möglichkeit geschaffen, dass auf Anordnung der Staatsanwaltschaft ihre Ermittlungspersonen die Papiere durchsehen. Gleichzeitig entfiel ohne nähere Begründung die Regelung, nach welcher der Inhaber für den Fall einer demnächst anzuordnenden Durchsicht der Papiere nach Möglichkeit zur Teilnahme aufzufordern war. Die Vorschrift lautete in der bei Erlass der angegriffenen Beschlüsse geltenden Fassung vom 24. August 2004 (BGBl I S. 2198): 13

§ 110 14

(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu. 15

(2) Im Übrigen sind Beamte zur Durchsicht der aufgefundenen Papiere nur dann befugt, wenn der Inhaber die Durchsicht genehmigt. Andernfalls haben sie die Papiere, deren Durchsicht sie für geboten erachten, in einem Umschlag, der in Gegenwart des Inhabers mit dem Amtssiegel zu verschließen ist, an die Staatsanwaltschaft abzuliefern. 16

Mit Wirkung zum 1. Januar 2008 - nach Erlass der hier angegriffenen Maßnahmen - wurde § 110 StPO ein neuer dritter Absatz angefügt. Dieser lautet: 17

(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durch- 18

suchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

**II.**

1. Die Staatsanwaltschaft führt ein Ermittlungsverfahren wegen Betrugs und Untreue gegen die Beschuldigten S. und G., die am 11. Oktober 2004 mit zwei Vertragspartnern einen Anlage- und Managementvertrag geschlossen hatten. Die Beschuldigten vermittelten laut Vertragsinhalt Investitions- und Handelsobjekte an Firmen ihrer Vertragspartner. Im Vertrag heißt es, dass alle Projekte über die Firma des Beschwerdeführers und die Firma E. realisiert und abgewickelt würden. Der Beschuldigte S. soll den Ermittlungen zufolge anlässlich der geplanten Errichtung einer Produktionsstätte in Indien wahrheitswidrige Angaben über eine bereits getroffene Entscheidung der V. AG gemacht und dadurch über einen Joint-Venture-Partner Geld erhalten haben. Das Geld soll auf das Konto der Firma I. gelangt sein, über das der Beschwerdeführer verfügungsberechtigt gewesen sein soll. Von dort aus soll er eine Barverfügung in Höhe von über 54.000 € und Überweisungen in Höhe von insgesamt mehr als 775.000 € auf das Konto der Firma E. vorgenommen haben, über das er ebenfalls verfügungsberechtigt gewesen sein soll. Von dem letztgenannten Konto sollen anschließend mehr als 100.000 € auf ein Privatkonto des Beschuldigten S. überwiesen worden sein. 19

2. Mit Beschluss vom 9. Februar 2006 ordnete das Amtsgericht im Zuge der Ermittlungen gegen die Beschuldigten S. und G. die Durchsuchung der Wohnung des Beschwerdeführers an, um Unterlagen und Datenträger zu den Unternehmen der Firmen I. und E. und deren Konten sowie Unterlagen und Dateien aufzufinden, die Aufschluss über den Grund von Bar- und Überweisungsverfügungen des über die Konten verfügungsberechtigten Beschwerdeführers geben könnten. Das Amtsgericht setzte hinzu: „Ferner wird gem. §§ 100g, 100h StPO die Auswertung von ggfls. zu beschlagnahmenden Datenträgern gestattet, insbesondere von Textdateien und e-mail-Verkehr.“ 20

3. Der Beschwerdeführer nutzte für den Zugriff auf seine E-Mails das so genannte Internet Message Access Protocol (IMAP). Empfangene E-Mails wurden nicht standardmäßig auf seinen lokalen Rechner übertragen, sondern blieben auch nach dem Abruf in einem zugangsgesicherten Bereich auf dem Mailserver seines Providers gespeichert. Zum Abruf der E-Mails war eine Internetverbindung herzustellen. Bei der Durchsuchung seiner Wohnung wies der Beschwerdeführer die Ermittlungspersonen auf diese Sachlage hin und stellte eine Internetverbindung her. Dann verwahrte er sich aber gegen einen Zugriff auf die E-Mails, weil der Durchsuchungsbeschluss dies nicht zulasse. 21

4. a) Das Amtsgericht ordnete daraufhin mit Beschluss vom 14. März 2006 gemäß §§ 94, 98 StPO die Beschlagnahme der Daten auf dem E-Mail-Account des Beschwerdeführers bei seinem Provider an. Die auf dem E-Mail-Account des Beschwerdeführers gespeicherten Daten seien als Beweismittel in dem nicht gegen ihn gerichteten Ermittlungsverfahren von Bedeutung. Der Beschwerdeführer wusste von diesem Beschluss, der fernmündlich von der Staatsanwaltschaft aus seinen Räumen beantragt und vom Amtsgericht dorthin übermittelt worden war. Am selben Tag wurden beim Provider die gesamten etwa 2.500 E-Mails des Beschwerdeführers, die seit Jahresbeginn 2004 bis zum 14. März 2006 auf dem Mailserver gespeichert worden waren, auf einen Datenträger kopiert und den Ermittlungsbehörden übergeben. 22

b) In seiner hiergegen gerichteten Beschwerde vertrat der Beschwerdeführer die Auffassung, für eine Beschlagnahme von E-Mails auf dem Mailserver des Providers sei eine Anordnung nach § 100a StPO erforderlich, die mangels Verdachts einer Katalogtat nicht habe ergehen können. Solange die E-Mails auf dem Mailserver des Providers gespeichert seien, unterfielen sie dem Schutzbereich von Art. 10 GG. Der Übermittlungsvorgang sei noch nicht abgeschlossen. Der Provider könne jederzeit auf die E-Mails zugreifen. Selbst wenn eine Beschlagnahme zulässig sein sollte, sei sie unverhältnismäßig. Er sei nicht Beschuldigter. Die bloße Annahme, er könne verfahrensrelevante Mitteilungen empfangen oder versandt haben, rechtfertige nicht den Zugriff auf seinen gesamten E-Mail-Bestand. Es handele sich größtenteils um geschäftliche Korrespondenz. Auch mit dem Vertragspartner B. der Beschuldigten stehe er zum Teil in Geschäftskontakten, die das anhängige Verfahren nicht berührten. Der Zugriff auf seine gesamte Geschäftskorrespondenz könne verheerende Konsequenzen haben, wenn Geschäftspartner und potenzielle Geschäftspartner davon Kenntnis erlangten. 23

c) Mit Beschluss vom 22. März 2006 half das Amtsgericht der Beschwerde nicht ab und legte sie dem Landgericht zur Entscheidung vor. Zugleich ordnete es die Beschlagnahme derjenigen Dateien an, in denen ein Zusammentreffen der Beschuldigten mit ihren beiden Vertragspartnern und dem Beschwerdeführer vermerkt sei, sowie derjenigen Daten, die sich auf Geschäftsbeziehungen mehrerer im Einzelnen benannter Unternehmen und Projekte bezögen. 24

d) Hierzu führte der Beschwerdeführer ergänzend aus, er habe den Speicherort seiner E-Mails den Ermittlungsbeamten nur offenbart, weil diese bei ihm den Irrtum erregt hätten, er müsse ihnen den Zugang zu den E-Mails eröffnen. Dieser Sachverhalt sei so zu behandeln, als wenn die Ermittlungsbehörden heimlich auf seine E-Mails zugegriffen hätten. Sollte die Beschlagnahme gleichwohl zulässig sein, sei ihr Umfang weiter einzuschränken. Jedenfalls sei ihm und seinem Rechtsanwalt zu gestatten, an der Durchsicht der E-Mails teilzunehmen. 25

e) Das Landgericht verwarf die Beschwerde mit Beschluss vom 12. April 2006. Der Beschluss vom 14. März 2006 sei zu Recht auf §§ 94, 98 StPO gestützt worden. Die bestimmungsgemäße Speicherung von E-Mails auf einem auswärtigen Speicher 26

beim Provider sei mit der Speicherung auf einem beim Teilnehmer vorgehaltenen Gerät vergleichbar. Der Übermittlungsvorgang sei abgeschlossen. Der Teilnehmer habe es in der Hand, seine E-Mails zu lesen, zu speichern oder zu löschen. Einen unbemerkten Zugriff Dritter könne er durch ein Passwort verhindern. Der Zugriff auf alle E-Mails sei angesichts der Erheblichkeit der gegen die Beschuldigten gerichteten Vorwürfe und wegen der ermittelten geschäftlichen Beziehungen des Beschwerdeführers zu ihnen verhältnismäßig. Eine Beschränkung anhand der Absenderangaben oder Betreffzeilen sei nicht geboten gewesen. Angesichts des bestehenden Firmengeflechts sei vor einer Sichtung aller E-Mails nicht erkennbar, welche E-Mails ermittlungsrelevant sein könnten. E-Mails, für die eine Durchsicht ergebe, dass sie nicht als Beweismittel in Betracht kämen, seien zurückzugeben. Über ihren Inhalt sei die Staatsanwaltschaft zur Geheimhaltung verpflichtet. Für eine Teilnahme des Beschwerdeführers und seines Rechtsanwalts an der Durchsicht gebe es keine Rechtsgrundlage.

**III.**

Der Beschwerdeführer rügt eine Verletzung seiner Grundrechte aus Art. 10 GG, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und Art. 2 Abs. 1 GG. 27

Die auf dem Mailserver seines Providers gespeicherten E-Mails seien durch Art. 10 GG geschützt, weil sie noch nicht endgültig in seinen Herrschaftsbereich gelangt seien. Aufgrund von § 94 StPO könne nicht in Art. 10 GG eingegriffen werden. Vielmehr bedürfe es einer Anordnung nach § 100a StPO, die mangels Verdachts einer Katalogtat nicht habe ergehen können. Jedenfalls werde in sein Recht und in das seiner Geschäftskunden auf informationelle Selbstbestimmung eingegriffen. Etwa 95 % der E-Mails enthielten Geschäftskorrespondenz, die seine Tätigkeit als Finanzdienstleister und Unternehmensberater beträfen. Seine Kunden vertrauten ihm hochsensible Daten an. Werde die umfassende Beschlagnahme bekannt, drohe der Verlust von Kunden. Angesichts dieser Auswirkungen auf seine wirtschaftliche Entfaltung liege auch ein Eingriff in Art. 2 Abs. 1 GG vor. 28

Die Ermittlungsbehörden hätten das Übermaßverbot missachtet, indem sie alle E-Mails beschlagnahmt hätten, statt nach einer groben Sichtung etwa anhand der Kommunikationspartner und einer zeitlichen Einschränkung nur verfahrensrelevante E-Mails zu beschlagnahmen. Die nur scheinbare Einschränkung im Nichtabhilfebeschluss greife zu kurz. Es sei zu berücksichtigen, dass er nicht Beschuldigter sei. Auch die mittelbaren Auswirkungen auf seine berufliche Tätigkeit seien zu gewichten. Die Fachgerichte hätten die strafprozessuale Reihenfolge von Sicherstellung, Durchsicht und Beschlagnahme verkannt. Er und sein Rechtsanwalt seien an der Durchsicht zu beteiligen. Da er ein nicht verdächtiger Dritter sei, bestehe kein Grund zur Annahme, er werde irreführende Hinweise erteilen. 29

**IV.**

Die 3. Kammer des Zweiten Senats hat mit Beschluss vom 29. Juni 2006 im Wege 30

einer einstweiligen Anordnung die Staatsanwaltschaft angewiesen, im Einzelnen bezeichnete Datenträger, Ausdrucke und Schriftstücke beim Amtsgericht in Verwahrung zu geben. Zugleich hat sie das Amtsgericht angewiesen, die Gegenstände zu versiegeln und in Verwahrung zu nehmen. Die einstweilige Anordnung wurde in der Folgezeit regelmäßig, zuletzt am 6. Mai 2009, wiederholt.

## V.

Zu der Verfassungsbeschwerde haben sich die Niedersächsische Landesregierung, der Bundesgerichtshof, der Generalbundesanwalt, das Bundesjustizministerium, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Deutsche Anwaltsverein und die Bundesrechtsanwaltskammer geäußert. 31

1. Die Niedersächsische Landesregierung, der Bundesgerichtshof, der Generalbundesanwalt und das Bundesjustizministerium halten die Verfassungsbeschwerde für unbegründet. Sie sind im Ergebnis übereinstimmend der Ansicht, auf dem Mailserver des Providers zwischen- und endgespeicherte E-Mails seien nicht durch Art. 10 GG geschützt. Der Kommunikationsvorgang sei beendet, sobald eine E-Mail auf dem Mailserver des Providers eingehe. Sie sei damit im Herrschaftsbereich des E-Mail-Adressaten angekommen, der darauf zugreifen dürfe und könne. Die Gefahr eines Zugriffs Dritter sei Folge der freiwilligen Entscheidung des Nutzers, seine E-Mails auf einem auswärtigen Speicherplatz zu verwalten. 32

Nach Auffassung der Niedersächsischen Landesregierung, des Generalbundesanwalts und des Bundesjustizministeriums sind die auf dem Mailserver des Providers gespeicherten E-Mails durch das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützt. §§ 94 ff. StPO seien eine hinreichende Ermächtigungsgrundlage für einen Zugriff auf die E-Mails mit Kenntnis des betroffenen Nutzers. Die Sicherstellung des gesamten E-Mail-Bestands, um diesen vor einer Beschlagnahme beweiserheblicher E-Mails einer groben Sichtung zu unterziehen, sei verhältnismäßig. 33

Das Bundesjustizministerium sieht den Schutzbereich von Art. 10 GG allenfalls dann als eröffnet an, wenn der Zugriff ohne Kenntnis des Nutzers erfolge. Ein etwaiger Eingriff in Art. 10 GG sei gemäß § 99 StPO analog gerechtfertigt. Für einen Zugriff auf beim Provider gespeicherte E-Mails dürften keine engeren Voraussetzungen gelten als für den Zugriff auf in einem Postfach liegende Postsendungen. Andernfalls komme es zu einer nicht gerechtfertigten Ungleichbehandlung zwischen elektronischer und nicht elektronischer Post. 34

2. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Deutsche Anwaltsverein und die Bundesrechtsanwaltskammer halten die Verfassungsbeschwerde für begründet. 35

a) Der Bundesbeauftragte für den Datenschutz ist der Ansicht, der Schutzbereich von Art. 10 GG ende, sobald der Empfänger die auf dem Mailserver eingegangene E-Mail zur Kenntnis genommen habe. Ab diesem Moment könne er mit ihr beliebig ver- 36

fahren und sie durch Löschung einem Zugriff durch Dritte entziehen. Eine E-Mail sei zur Kenntnis genommen, sobald sie geöffnet worden sei. Darüber hinaus sei die Kenntnisnahme ab einem bestimmten Zeitpunkt unter Heranziehung der Rechtsgedanken aus § 41 Abs. 2 VwVfG oder § 312e Abs. 1 Satz 2 BGB zu fingieren. Nur ein Zugriff auf E-Mails, die weder zur Kenntnis genommen noch als bekanntgegeben gälten, greife in Art. 10 GG ein. Ein solcher Zugriff könne allein aufgrund von § 100a StPO erfolgen. Der Zugriff auf zur Kenntnis genommene oder als bekannt gegeben fingierte E-Mails greife in das Recht auf informationelle Selbstbestimmung ein. Die §§ 94 ff. StPO seien hierfür eine hinreichende Ermächtigungsgrundlage.

Vorliegend seien aber besonders strenge Anforderungen an die Verhältnismäßigkeit zu stellen, da auf den Kommunikationsinhalt zugegriffen werde, die auf dem Mailserver des Providers gespeicherten E-Mails näher am Schutzbereich von Art. 10 GG anzusiedeln seien als auf dem Arbeitsplatzcomputer gespeicherte E-Mails, der Beschwerdeführer nicht Beschuldigter sei und Daten seiner Geschäftspartner und Kunden betroffen seien, die in keinem Zusammenhang mit dem Ermittlungsverfahren stünden. In einem solchen Fall sei die Beschlagnahme unter Berücksichtigung der Kommunikationspartner und -themen auf solche E-Mails zu beschränken, die mit hoher Wahrscheinlichkeit verfahrensrelevante Erkenntnisse lieferten. Diesen Anforderungen würden die angegriffenen Entscheidungen nicht gerecht. 37

b) Der Deutsche Anwaltsverein und die Bundesrechtsanwaltskammer sind der Auffassung, auf dem Mailserver des Providers gespeicherte E-Mails seien unabhängig davon, ob sie abgerufen worden seien oder nicht, durch Art. 10 GG geschützt, da sie sich nicht in einer allein vom Nutzer beherrschbaren Privatsphäre befänden. Dies ergebe sich aus der Notwendigkeit jederzeitiger Administratorenzugriffe, den Verpflichtungen der Betreiber von Kommunikationsanlagen aus §§ 110 bis 115 TKG sowie den umfangreichen in §§ 3 ff. TKÜV geregelten Maßnahmen. Eingriffe in noch nicht abgeschlossene Telekommunikationsvorgänge seien nur aufgrund von § 100a StPO zulässig. 38

Die Bundesrechtsanwaltskammer weist ergänzend darauf hin, dass sie die kaum eingeschränkte Beschlagnahme aller E-Mails für unverhältnismäßig halte. Die Ermittlungsbehörden hätten nur die nach einer Sichtung als verfahrenserheblich erkannten Daten kopieren dürfen. 39

## B.

Die zulässige Verfassungsbeschwerde ist unbegründet. Die angegriffenen Beschlüsse verletzen den Beschwerdeführer nicht in seinen Grundrechten. 40

Die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers zwischen- und endgespeicherten E-Mails sind am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen (I.). Die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers greifen in das Fernmeldegeheimnis ein (II.). Die strafprozessualen Vorschriften der §§ 94 ff. StPO 41

ermöglichen grundsätzlich die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers (III.). Der konkrete Eingriff aufgrund von §§ 94 ff. StPO muss jedoch verhältnismäßig sein (IV.). Der effektive Schutz von Art. 10 Abs. 1 GG bedarf zudem einer den sachlichen Erfordernissen entsprechenden Ausgestaltung des Verfahrens (V.). Die angegriffenen Entscheidungen genügen den verfassungsrechtlichen Vorgaben (VI.).

**I.**

1. Die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails sind am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen. 42

Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 115, 166 <182>; 120, 274 <306 f.>). Die Reichweite des Grundrechts erstreckt sich ungeachtet der Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) auf sämtliche Übermittlungen von Informationen mit Hilfe verfügbarer Telekommunikationstechniken (vgl. BVerfGE 106, 28 <36>; 115, 166 <182 f.>), auch auf Kommunikationsdienste des Internet (vgl. BVerfGE 120, 274 <307>). 43

Der Schutz des Fernmeldegeheimnisses umfasst in erster Linie den Kommunikationsinhalt (vgl. BVerfGE 100, 313 <358>; 107, 299 <312>; 115, 166 <183>), sei er privater, geschäftlicher, politischer oder sonstiger Natur (vgl. BVerfGE 100, 313 <358>; 106, 28 <36>). Daneben sind die Kommunikationsumstände vor Kenntnisnahme geschützt (vgl. BVerfGE 113, 348 <364 f.>; 115, 166 <183>; 120, 274 <307>). 44

Der Grundrechtsschutz erstreckt sich nicht auf die außerhalb eines laufenden Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist (vgl. BVerfGE 115, 166 <183 ff.>; 120, 274 <307 f.>). 45

Demgegenüber ist der zugangsgesicherte Kommunikationsinhalt in einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, durch Art. 10 Abs. 1 GG geschützt (vgl. auch BVerfGE 120, 274 <341>). Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an und will jenen Gefahren für die Vertraulichkeit begegnen, die sich gerade aus der Verwendung dieses Mediums ergeben, das einem staatlichem Zugriff leichter ausgesetzt ist als die direkte Kommunikation unter Anwesenden (vgl. BVerfGE 100, 313 <363>). Die auf dem Mailserver des Providers vorhandenen E-Mails sind nicht im Herrschaftsbereich des Kommunikationsteilnehmers, sondern des Providers gespeichert. Sie befinden sich nicht auf in den Räumen des Nutzers verwahrten oder in seinen Endgeräten installierten Datenträgern. Der Nutzer kann sie für sich auf einem Bildschirm nur lesbar machen, indem 46

er eine Internetverbindung zum Mailserver des Providers herstellt. Zwar kann der Nutzer versuchen, die auf dem Mailserver gespeicherten E-Mails durch Zugangssicherungen - etwa durch Verwendung eines Passworts - vor einem ungewollten Zugriff Dritter zu schützen. Der Provider und damit auch die Ermittlungsbehörden bleiben jedoch weiterhin in der Lage, jederzeit auf die auf dem Mailserver gespeicherten E-Mails zuzugreifen. Der Kommunikationsteilnehmer hat keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider zu verhindern. Dieser technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis. Dies gilt unabhängig davon, ob eine E-Mail auf dem Mailserver des Providers zwischen- oder endgespeichert ist. In beiden Fällen ist der Nutzer gleichermaßen schutzbedürftig, weil sie sich hinsichtlich der faktischen Herrschaftsverhältnisse nicht unterscheiden.

Dem Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch Art. 10 Abs. 1 GG steht nicht entgegen, dass während der Zeitspanne, während deren die E-Mails auf dem Mailserver des Providers „ruhen“, ein Telekommunikationsvorgang in einem dynamischen Sinne nicht stattfindet. Zwar definiert § 3 Nr. 22 TKG „Telekommunikation“ als den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen und bezieht sich nicht ausdrücklich auch auf statische Zustände. Art. 10 Abs. 1 GG folgt indes nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes, sondern knüpft an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an (vgl. BVerfGK 9, 62 <75>). 47

Der Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch das Fernmeldegeheimnis entfällt auch nicht dadurch, dass ihr Inhalt oder Eingang vom Empfänger möglicherweise schon zur Kenntnis genommen worden ist. Die Reichweite des Schutzes von Art. 10 Abs. 1 GG endet nicht in jedem Fall mit der Kenntnisnahme des Kommunikationsinhalts durch den Empfänger. Ob Art. 10 Abs. 1 GG Schutz vor Zugriffen bietet, ist mit Blick auf den Zweck der Freiheitsverbürgung unter Berücksichtigung der spezifischen Gefährdungslage zu bestimmen (vgl. BVerfGE 106, 28 <37 f.>; 115, 166 <186 f.>). Die spezifische Gefährdungslage und der Zweck der Freiheitsverbürgung von Art. 10 Abs. 1 GG bestehen auch dann weiter, wenn die E-Mails nach Kenntnisnahme beim Provider gespeichert bleiben. Durch die Endspeicherung wird der von Art. 10 Abs. 1 GG zuvörderst geschützte Kommunikationsinhalt infolge der Nutzung eines bestimmten Kommunikationsmediums auf einem vom Kommunikationsmittler bereit gestellten Speicherplatz in einer von keinem Kommunikationsteilnehmer beherrschbaren Sphäre abgelegt. Weder bei einer Zwischen- noch bei einer Endspeicherung der E-Mails auf dem Mailserver des Providers ist dessen Tätigkeit beendet; der Provider bleibt dauerhaft in die weitere E-Mail-Verwaltung auf seinem Mailserver eingeschaltet. 48

2. Da die auf dem Mailserver des Providers gespeicherten E-Mails durch Art. 10 Abs. 1 GG geschützt sind, ist der Zugriff auf sie nicht am Recht auf informationelle 49

Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu messen. In seinem Anwendungsbereich enthält Art. 10 Abs. 1 GG bezogen auf den Fernmeldeverkehr eine spezielle Garantie, die die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt (vgl. BVerfGE 100, 313 <358>; 107, 299 <312>; 110, 33 <53>; 113, 348 <364>; 115, 166 <188 f.>). Soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind aber die Maßgaben, die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gelten, grundsätzlich auf die speziellere Garantie in Art. 10 Abs. 1 GG zu übertragen (vgl. B. III. 1. b) aa).

3. Der Empfänger von E-Mails, die auf dem Mailserver des Providers gespeichert sind, kann sich nicht auf Art. 13 Abs. 1 GG berufen, wenn beim Provider auf seine E-Mails zugegriffen wird. Die einem solchen Zugriff regelmäßig vorausgehende Durchsuchung greift zwar in der Regel in die durch Art. 13 GG geschützte Unverletzlichkeit der Wohnung des betreffenden Wohnungsinhabers - also des Providers - ein. Der Empfänger der E-Mail kann insoweit aber keine eigene Grundrechtsverletzung geltend machen. Die Sicherstellung, Beschlagnahme oder Maßnahmen nach § 110 StPO unterfallen, auch wenn sie Resultat einer Wohnungsdurchsuchung sind, nicht mehr dem Schutzbereich des Art. 13 Abs. 1 GG (vgl. BVerfGE 113, 29 <45>). Die mit einer Sicherstellung, Beschlagnahme oder Durchsicht verbundene Belastung besteht in der Regel in der Entziehung des Besitzes an den betroffenen Beweisgegenständen und ist daher an Art. 14 GG (vgl. BVerfGK 1, 126 <133>) und - sofern Daten betroffen sind - am Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (vgl. BVerfGE 113, 29 <44 f.>) zu messen. 50

4. Der Zugriff auf die auf dem Mailserver des Providers gespeicherten E-Mails ist nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu messen. Dieses schützt vor Eingriffen in informationstechnische Systeme nur, soweit der Schutz nicht durch andere Grundrechte, insbesondere Art. 10 oder Art. 13 GG, sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist (vgl. BVerfGE 120, 274 <302 ff.>; Hoffmann-Riem, JZ 2008, S. 1009 <1019>). 51

**II.**

Die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails greift in den Schutzbereich des Fernmeldegeheimnisses ein. 52

Da Art. 10 Abs. 1 GG die Vertraulichkeit der Kommunikation schützen will, ist jede Kenntnisnahme, Aufzeichnung und Verwertung kommunikativer Daten ohne Einwilligung des Betroffenen ein Grundrechtseingriff (vgl. BVerfGE 85, 386 <398>). Die Auslagerung der E-Mails auf den nicht im Herrschaftsbereich des Nutzers liegenden Mailserver des Providers bedeutet nicht, dass der Nutzer mit dem Zugriff auf diese Daten durch Dritte einverstanden ist. Wer ein Teilnehmer- oder Benutzerverhältnis eingeht, weiß zwar in der Regel, dass es technische Möglichkeiten gibt, auf die Kommunikationsinhalte zuzugreifen. Er willigt damit aber nicht darin ein, dass auf die 53

Kommunikationsinhalte zugegriffen wird (vgl. BVerfGE 85, 386 <398>).

Ein Eingriff in das Fernmeldegeheimnis liegt nicht erst in der Kenntnisnahme staatlicher Stellen vom Inhalt des fernmeldetechnisch vermittelten Kommunikationsvorgangs und in seiner Aufzeichnung, sondern bereits in der Anordnung des Zugriffs (vgl. BVerfGE 100, 313 <366>; 107, 299 <313>). 54

**III.**

Die strafprozessualen Regelungen der §§ 94 ff. StPO ermöglichen grundsätzlich die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind. 55

1. Beschränkungen des Fernmeldegeheimnisses dürfen gemäß Art. 10 Abs. 2 Satz 1 GG nur aufgrund eines Gesetzes angeordnet werden. §§ 94 ff. StPO genügen den verfassungsrechtlichen Anforderungen, die an eine gesetzliche Ermächtigung für Eingriffe der genannten Art in das Fernmeldegeheimnis zu stellen sind. 56

a) § 94 StPO kann ohne Verfassungsverstoß als Ermächtigung auch zu Eingriffen in Art. 10 Abs. 1 GG verstanden werden (vgl. Amelung, in: AK-StPO, 1992, vor §§ 99, 100 Rn. 4; Engels, Die Grenzen des Brief-, Post- und Fernmeldegeheimnisses, 1972, S. 88 f.; Welp, Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, 1974, S. 47; Wohlers, in: SK-StPO, § 94 Rn. 2 <Feb. 2008>). Aus der systematischen Stellung von § 94 StPO und den Vorschriften über die Postbeschlagnahme (§ 99 StPO), die Überwachung der Telekommunikation (§ 100a StPO) und die Erhebung und Auskunftserteilung über Verkehrsdaten (§ 100g StPO) ist nicht der Schluss auf ein gesetzgeberisches Regelungskonzept zu ziehen, wonach nur aufgrund von § 99, § 100a und § 100g StPO in Art. 10 GG eingegriffen werden könnte. Alle genannten Vorschriften befinden sich im 8. Abschnitt des Ersten Buches der Strafprozessordnung. In diesem Abschnitt befinden sich auch Regelungen über den maschinellen Abgleich und die Übermittlung personenbezogener Daten (§ 98a StPO), Maßnahmen ohne Wissen des Betroffenen wie die Herstellung von Bildaufnahmen und die Verwendung technischer Mittel für Observationszwecke (§ 100h StPO), das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes innerhalb (§ 100c StPO) und außerhalb (§ 100f StPO) von Wohnungen, den Einsatz so genannter „IMSI-Catcher“ (§ 100i StPO), die Durchsuchung (§§ 102 ff.), den Einsatz verdeckter Ermittler (§ 110a StPO), die Einrichtung von Kontrollstellen an öffentlich zugänglichen Orten (§ 111 StPO), die vorläufige Entziehung der Fahrerlaubnis (§ 111a StPO) sowie Maßnahmen der Rückgewinnungshilfe und Rückgabe von Gegenständen einschließlich des dinglichen Arrests und der Vermögensbeschlagnahme (§§ 111b ff. StPO). Diese Aneinanderreihung unterschiedlicher Maßnahmen legt nicht den Schluss nahe, der Gesetzgeber habe Eingriffe in Art. 10 GG nur aufgrund von § 99, § 100a und § 100g StPO zulassen wollen. Auch die Gesetzesmaterialien enthalten keinen hinreichenden Anhaltspunkt dafür, dass der Gesetzgeber bei der Schaffung dieser Vorschriften von abschließenden Regelungen in Bezug auf Eingriffe in das Brief-, Post- und Fernmeldegeheimnis ausgegangen ist. Nach Wortlaut, 57

Systematik und Zweck handelt es sich bei den §§ 94 ff. StPO um Vorschriften über unterschiedliche strafprozessuale Maßnahmen, deren Anwendungsbereich nicht durchgehend jeweils in spezifischer Weise auf die Reichweite spezieller Grundrechte abgestimmt sind.

Soweit Eingriffe der hier zu beurteilenden Art auf § 99 StPO (vgl. dazu BGH, Beschluss vom 31. März 2009 - 1 StR 76/09 -, Juris; für den Zugriff auf zwischengespeicherte E-Mails aufgrund von § 99 StPO vgl. LG Ravensburg, NStZ 2003, S. 325 <326>) oder § 100a StPO (vgl. LG Hamburg, Beschluss vom 8. Januar 2008 - 619 Qs 1/08 -, MMR 2008, S. 186 <187>) gestützt werden, wird dadurch die Anwendbarkeit der §§ 94 ff. StPO nicht in Frage gestellt. 58

b) §§ 94 ff. StPO genügen hinsichtlich der Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails dem Gebot der Normenklarheit und Normenbestimmtheit. 59

aa) Soweit ein Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind die Anforderungen, die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gelten (vgl. BVerfGE 65, 1 <44 ff.>), grundsätzlich auf Eingriffe in das speziellere Grundrecht aus Art. 10 Abs. 1 GG zu übertragen (vgl. BVerfGE 110, 33 <53>; 115, 166 <189>). Zu diesen Anforderungen gehört, dass sich die Voraussetzungen und der Umfang der Beschränkungen aus dem Gesetz klar und für den Bürger erkennbar ergeben. Der Anlass, der Zweck und die Grenzen des Eingriffs in das Fernmeldegeheimnis müssen in der Ermächtigung bereichsspezifisch und präzise bestimmt sein (vgl. BVerfGE 100, 313 <359 f., 372>; 110, 33 <53>). 60

bb) Der Senat hat bereits entschieden, dass die §§ 94 ff. StPO diesen Anforderungen hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten genügen (vgl. BVerfGE 113, 29 <51 f.>; 115, 166 <191 ff.>). Gleiches gilt für die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind. 61

(1) Für die betroffenen Nutzer ist hinreichend erkennbar, dass die §§ 94 ff. StPO die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails ermöglichen. 62

Die Eingriffsbefugnisse gemäß §§ 94 ff. StPO sind zwar ursprünglich auf körperliche Gegenstände zugeschnitten; der Wortsinn von § 94 StPO gestattet es jedoch, als „Gegenstand“ des Zugriffs auch nichtkörperliche Gegenstände zu verstehen (vgl. BVerfGE 113, 29 <50>). § 94 StPO erfasst grundsätzlich alle Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können. Eine nähere gesetzliche Eingrenzung ist wegen der Vielgestaltigkeit möglicher Sachverhalte nicht geboten. Die verfahrensbezogenen Konkretisierungen hat von Verfassungs wegen der Ermittlungsrichter im jeweiligen Durchsuchungs- oder Beschlagnahmebeschluss zu leisten (vgl. BVerfGE 113, 29 <51>). 63

(2) Die allgemeinen strafprozessualen Sicherstellungs- und Beschlagnahmerege- 64

lungen genügen ferner der Vorgabe, wonach der Gesetzgeber den Verwendungszweck der erhobenen Daten bereichsspezifisch und präzise bestimmen muss. Die Ermittlungsmethoden der Strafprozessordnung sind zwar im Hinblick auf die Datenerhebung und den Datenumfang weit gefasst. Der den Datenzugriff begrenzende Verwendungszweck ist aber unter Beachtung des Normzusammenhangs, in welchen die §§ 94 ff. StPO eingebettet sind (vgl. § 152 Abs. 2, § 155 Abs. 1, § 160, § 170, § 244 Abs. 2, § 264 StPO), hinreichend präzise vorgegeben. Die jeweiligen Eingriffsgrundlagen stehen unter einer strengen Begrenzung auf den Ermittlungszweck. Strafprozessuale Ermittlungsmaßnahmen sind nur zulässig, soweit dies zur Vorbereitung der anstehenden Entscheidungen im Hinblick auf die in Frage stehende Straftat nötig ist. Auf die Ermittlung anderer Lebenssachverhalte und Verhältnisse erstrecken sich die Eingriffsermächtigungen nicht (BVerfGE 113, 29 <52>; vgl. auch BVerfGE 115, 166 <191>).

c) §§ 94 ff. StPO sind hinsichtlich der Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails auch verhältnismäßig. Die wirksame Strafverfolgung, die Verbrechensbekämpfung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren sind legitime Zwecke, die eine Einschränkung des Fernmeldegeheimnisses rechtfertigen können (vgl. BVerfGE 100, 313 <389>; 107, 299 <316>). Die Möglichkeit, auf der Grundlage der §§ 94 ff. StPO auf die auf dem Mailserver des Providers gespeicherten E-Mails zuzugreifen, ist zur Erreichung dieser Ziele nicht nur geeignet und erforderlich, sondern auch verhältnismäßig im engeren Sinne. 65

aa) Die Verhältnismäßigkeit im engeren Sinne verlangt, dass die Einbußen grundrechtlich geschützter Freiheiten nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient. Der Gesetzgeber muss zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen (vgl. BVerfGE 100, 313 <375 f.>). 66

Dabei ist einerseits das Gewicht der Ziele und Belange zu berücksichtigen, denen der Eingriff dient. Maßgeblich ist unter anderem, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen, und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist (vgl. BVerfGE 100, 313 <376>; 113, 348 <382>). Andererseits ist zu beachten, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigung (vgl. BVerfGE 100, 313 <376>; 113, 348 <382>). 67

Die Schwere eines Eingriffs erhöht sich, wenn er heimlich erfolgt (vgl. BVerfGE 107, 299 <321>; 110, 33 <53>; 113, 348 <383 f.>; 115, 166 <194>; 120, 274 <325, 342>). Ein längerfristiger Eingriff in einen laufenden Telekommunikationsvorgang wiegt schwerer als eine einmalige und punktuelle Datenerhebung, da Umfang und Vielfältigkeit des Datenbestands erheblich größer sind (vgl. BVerfGE 120, 274 <323 f.>). 68

Die Möglichkeit einer Verwendung erhobener Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken erhöht ebenfalls die Schwere des Eingriffs schon in der Phase der Erhebung (vgl. BVerfGE 113, 348 <384 f.>). Eine erhöhte Eingriffsintensität ist schließlich dann anzunehmen, wenn der Betroffene über keinerlei Einwirkungsmöglichkeiten auf seinen Datenbestand verfügt (vgl. BVerfGE 115, 166 <194>).

bb) Im Bereich der Strafverfolgung sind daher bei heimlichen Eingriffen in das Fernmeldegeheimnis sowie etwa bei Zugriffen auf umfassende Datenbestände, die verdachtlos vorgehalten werden (vgl. BVerfG, Beschluss des Ersten Senats vom 11. März 2008 - 1 BvR 256/08 -, NVwZ 2008, S. 543 <544 ff.>) und auf die die Betroffenen nicht einwirken können, besonders hohe Anforderungen an die Bedeutung der zu verfolgenden Straftat und den für den Zugriff erforderlichen Grad des Tatverdachts zu stellen (vgl. BVerfGE 100, 313 <394>; 107, 299 <318 ff.>). Geht es hingegen um eine aus einer Durchsuchung folgende, offene und durch den Ermittlungszweck begrenzte Maßnahme außerhalb eines laufenden Kommunikationsvorgangs - wie die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind - verlangt das Übermaßverbot angesichts des Gewichts des staatlichen Strafverfolgungsinteresses nicht, die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails nur bei der Verfolgung einer besonders schweren Straftat (wie § 100c StPO), einer schweren Straftat (wie § 100a StPO) oder einer Straftat von erheblicher Bedeutung (wie § 100g StPO) zuzulassen. Greifen Strafverfolgungsbehörden - wie bei Sicherstellungen und Beschlagnahmen - mit Kenntnis des Betroffenen, außerhalb eines laufenden Kommunikationsvorgangs auf Kommunikationsinhalte zu, kann der auch sonst im strafprozessualen Ermittlungsverfahren erforderliche Anfangsverdacht einer Straftat genügen. 69

(1) Im Rahmen der Abwägung ist einerseits zu berücksichtigen, dass der Inhalt der Kommunikation in höherem Maße als Kommunikationsdaten schutzwürdig ist. Zudem kann ein Zugriff auf E-Mails erhebliche Rückschlüsse auf das Kommunikationsverhalten des Betroffenen, sein soziales Umfeld und seine persönlichen Interessen zulassen. Der Eingriff gewinnt zusätzliches Gewicht, wenn an der aufzuklärenden Straftat unbeteiligte Kommunikationsteilnehmer in ihren Grundrechten betroffen sind. Hinzu kommen kann eine besondere Schutzbedürftigkeit vom Datenzugriff betroffener Vertrauensverhältnisse. 70

(2) Auf der anderen Seite ist das Gewicht des staatlichen Strafverfolgungsinteresses in Rechnung zu stellen. Die vermehrte Nutzung elektronischer und digitaler Kommunikationsmittel und ihr Vordringen in nahezu alle Lebensbereiche erschweren die Strafverfolgung. Moderne Kommunikationstechniken werden im Zusammenhang mit der Begehung unterschiedlichster Straftaten zunehmend eingesetzt und tragen zur Effektivierung krimineller Handlungen bei (vgl. Hofmann, NStZ 2005, S. 121). Das Schritthalten der Strafverfolgungsbehörden mit der technischen Entwicklung kann daher nicht lediglich als sinnvolle Abrundung des Arsenals kriminalistischer Ermittlungsmethoden begriffen werden, die weiterhin wirkungsvolle herkömmliche Ermitt- 71

lungsmaßnahmen ergänzt, sondern ist vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr einschließlich der anschließenden digitalen Verarbeitung und Speicherung zu sehen (vgl. BVerfGE 115, 166 <193>).

(3) Unter diesen Umständen ist es zur Wahrung der Verhältnismäßigkeit nicht geboten, den Zugriff auf beim Provider gespeicherte E-Mails auf Ermittlungen zu begrenzen, die zumindest Straftaten von erheblicher Bedeutung betreffen, und Anforderungen an den Tatverdacht zu stellen, die über den Anfangsverdacht einer Straftat hinausgehen. 72

(a) Eine Straftat von erheblicher Bedeutung liegt vor, wenn sie mindestens der mittleren Kriminalität zuzurechnen ist, den Rechtsfrieden empfindlich stört und geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vgl. BVerfGE 103, 21 <34>; 109, 279 <344>; BTDrucks 16/5846, S. 40). Zu den Straftaten, die im Höchstmaß mit Freiheitsstrafe unter fünf Jahren bedroht sind und die deshalb nicht mehr ohne weiteres dem Bereich der Straftaten von erheblicher Bedeutung zuzurechnen sind, gehören beispielsweise das unerlaubte Entfernen vom Unfallort (§ 142 StGB), die Beleidigung, die üble Nachrede und die nichtöffentliche Verleumdung (§§ 185 bis 187 StGB), das Ausspähen von Daten (§ 202a StGB), die fahrlässige Körperverletzung (§ 229 StGB), die Nötigung (§ 240 StGB) sowie die Verbreitung pornografischer Schriften einschließlich gewalt- oder tierpornografischer Schriften (§§ 184 und 184a StGB). 73

Mit dem verfassungsrechtlich anerkannten Strafverfolgungsinteresse wäre es nicht vereinbar, sämtliche E-Mails für derartige Deliktsbereiche generell und ohne Rücksicht auf den Einzelfall von einer Sicherstellung und Beschlagnahme auszunehmen. Andernfalls wäre es für jeden Nutzer ein Leichtes, belastende E-Mails durch eine Auslagerung auf den Mailserver seines Providers dem Zugriff der Strafverfolgungsbehörden zu entziehen. Insoweit ist auch zu berücksichtigen, dass nach dem Willen des Gesetzgebers für die Sicherstellung und Beschlagnahme von Mitteln herkömmlicher Kommunikation gemäß § 94 StPO und § 99 StPO der Anfangsverdacht einer einfachen Straftat genügen kann. Würden im Hinblick auf die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers höhere Anforderungen gestellt, bestünde zudem die Gefahr, dass die Strafrahmen für bestimmte Deliktsgruppen allein deshalb erhöht würden, um bei diesen Delikten einen Zugriff auf Daten und Kommunikationsinhalte zu ermöglichen. 74

(b) Soweit das Bundesverfassungsgericht im Rahmen der Verhältnismäßigkeitsprüfung von Einzelmaßnahmen, die auf Erlangung der bei einem Telekommunikationsmittler gespeicherten Verbindungsdaten gerichtet waren, eine Beschränkung auf Ermittlungen betreffend Straftaten von erheblicher Bedeutung für notwendig gehalten hat (vgl. BVerfGE 107, 299 <321>), kann dies auf die Sicherstellung und Beschlagnahme der beim Provider gespeicherten E-Mails nicht übertragen werden. Hierbei ist zu berücksichtigen, dass die Sicherstellung und Beschlagnahme von E-Mails auf 75

dem Mailserver des Providers in der Regel nicht heimlich, sondern offen vollzogen wird, die Daten punktuell und auf den Ermittlungszweck begrenzt außerhalb eines laufenden Kommunikationsvorgangs erhoben werden und der Betroffene Einwirkungsmöglichkeiten auf den von ihm auf dem Mailserver seines Providers gespeicherten E-Mail-Bestand hat.

Das besondere Gewicht grundrechtlichen Schutzes gegen heimliche Eingriffe in die Kommunikationsfreiheit beruht darauf, dass heimliche Maßnahmen spezifische Risiken für die Rechte der Betroffenen bergen; diese können sich gegen den Eingriff frühestens dann mit rechtlichen Mitteln wehren, wenn er bereits vollzogen ist, und auch dies nur, wenn sie über die Maßnahme informiert werden oder auf andere Weise Kenntnis erlangen (vgl. BVerfGE 107, 299 <321>; 113, 348 <384>). Demgegenüber bieten offene Maßnahmen dem Betroffenen die Möglichkeit, - gegebenenfalls unter Hinzuziehung anwaltlichen Beistands - bereits der Durchführung der Maßnahme entgegen zu treten, wenn es an den gesetzlichen Voraussetzungen fehlt, oder aber zumindest die Einhaltung der im Durchsuchungsbeschluss gezogenen Grenzen einschließlich der für die Beschlagnahme vorgegebenen Richtlinien selbst zu überwachen und Ausuferungen des Vollzugs der richterlichen Anordnungen entgegenzutreten (vgl. BVerfGE 115, 166 <194 f.>). 76

d) §§ 94 ff. StPO verstoßen auch nicht gegen das Zitiergebot aus Art. 19 Abs. 1 Satz 2 GG. Soweit nach dem Grundgesetz - wie gemäß Art. 10 Abs. 2 Satz 1 GG - ein Grundrecht durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden kann, muss zwar das Gesetz nach Art. 19 Abs. 1 Satz 2 GG grundsätzlich das Grundrecht unter Angabe des Artikels nennen. Das Zitiergebot findet aber auf die vor seiner Maßgeblichkeit entstandenen, insbesondere auf vorkonstitutionelle Gesetze und somit auch auf §§ 94 ff. StPO, keine Anwendung (stRspr seit BVerfGE 2, 121 <122 f.>). 77

## IV.

Beschränkungen des Fernmeldegeheimnisses bedürfen nicht nur einer gesetzlichen Ermächtigungsgrundlage, die dem Gebot der Normenklarheit und dem Verhältnismäßigkeitsgrundsatz genügt. Auch der konkrete Eingriff aufgrund von §§ 94 ff. StPO muss verhältnismäßig sein (vgl. BVerfGE 113, 29 <53>; 115, 166 <197 ff.>). 78

1. Die Maßnahme muss vor allem in angemessenem Verhältnis zu der Schwere der Straftat und der Stärke des Tatverdachts stehen (vgl. dazu bereits BVerfGE 113, 29 <53>; 115, 166 <197 ff.>). Hierbei ist nicht nur die Bedeutung des potentiellen Beweismittels für das Strafverfahren, sondern auch der Grad des auf die verfahrenserheblichen Gegenstände oder Daten bezogenen Auffindeverdachts zu bewerten. Auf die E-Mails darf nur zugegriffen werden, wenn ein konkret zu beschreibender Tatvorwurf vorliegt, also mehr als nur vage Anhaltspunkte oder bloße Vermutungen (vgl. BVerfGE 44, 353 <371 f.>; 115, 166 <198>). Beim Zugriff auf die bei dem Provider gespeicherten E-Mails ist auch die Bedeutung der E-Mails für das Strafverfahren sowie der Grad des Auffindeverdachts zu bewerten. Im Einzelfall können die Geringfü- 79

gigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der zu beschlagnahmenden E-Mails sowie die Vagheit des Auffindeverdachts der Maßnahme entgegenstehen.

Dem Schutz des Fernmeldegeheimnisses muss bereits in der Durchsuchungsanordnung, soweit die konkreten Umstände dies ohne Gefährdung des Untersuchungszwecks erlauben, durch Vorgaben zur Beschränkung des Beweismaterials auf den tatsächlich erforderlichen Umfang Rechnung getragen werden, etwa durch die zeitliche Eingrenzung oder die Beschränkung auf bestimmte Kommunikationsinhalte. 80

Bei dem Vollzug von Durchsuchung und Beschlagnahme - insbesondere beim Zugriff auf umfangreiche elektronisch gespeicherte Datenbestände - sind die verfassungsrechtlichen Grundsätze zu gewährleisten, die der Senat in seinem Beschluss zur Durchsuchung und Beschlagnahme eines umfangreichen elektronischen Datenbestands (vgl. BVerfGE 113, 29 <52 ff.>) entwickelt hat. Hierbei ist vor allem darauf zu achten, dass die Gewinnung überschießender, für das Verfahren bedeutungsloser Daten nach Möglichkeit vermieden wird. Die Beschlagnahme sämtlicher gespeicherter Daten und damit des gesamten E-Mail-Verkehrs wird regelmäßig nicht erforderlich sein. 81

2. Den sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Anforderungen kann bei der Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails in vielfältiger Weise Rechnung getragen werden. 82

a) Wird festgestellt, dass sich auf dem Mailserver überhaupt keine verfahrenserheblichen E-Mails befinden können, wäre eine Sicherstellung schon ungeeignet. 83

b) Soweit davon auszugehen ist, dass auf dem Mailserver unter anderem potenziell beweiserhebliche E-Mails gespeichert sind, ist zu prüfen, ob eine Sicherstellung aller gespeicherten E-Mails erforderlich ist. Der dauerhafte Zugriff auf den gesamten E-Mail-Bestand ist nicht erforderlich, wenn eine Sicherung allein der beweiserheblichen E-Mails auf eine andere, die Betroffenen weniger belastende Weise ebenso gut erreicht werden kann. Die Gewinnung überschießender und vertraulicher, für das Verfahren aber bedeutungsloser Informationen muss im Rahmen des Vertretbaren vermieden werden. 84

c) Soweit eine Unterscheidung der E-Mails nach ihrer potenziellen Verfahrenserheblichkeit vorgenommen werden kann, ist die Möglichkeit einer Trennung der potenziell beweiserheblichen von den restlichen E-Mails zu prüfen. In Betracht kommt neben dem Erstellen einer (Teil-)Kopie hinsichtlich der verfahrenserheblichen E-Mails das Löschen oder die Herausgabe der für das Verfahren irrelevanten E-Mails. 85

d) Je nach den Umständen des Einzelfalls können für die Begrenzung des Zugriffs unterschiedliche, miteinander kombinierbare Möglichkeiten der materiellen Datenzuordnung in Betracht gezogen werden. Sie müssen, bevor eine endgültige Beschlagnahme sämtlicher E-Mails erwogen wird, ausgeschöpft werden. Von Bedeutung ist hierbei vor allem die Auswertung der Struktur eines gespeicherten E-Mail-Bestands, 86

der beispielweise themen-, zeit- oder personenbezogen geordnet sein oder geordnet werden kann. Bei der Suche nach ermittlungsrelevanten E-Mails ist auch eine Auswahl anhand bestimmter Übermittlungszeiträume oder Sender- und Empfängerangaben in Betracht zu ziehen. Eine Zuordnung der E-Mails nach ihrer Verfahrensrelevanz kann unter Umständen auch mit Hilfe geeigneter Suchbegriffe oder Suchprogramme gelingen.

e) Eine sorgfältige Sichtung und Trennung der E-Mails nach ihrer Verfahrensrelevanz wird am Zugriffsort nicht immer möglich sein. Sofern die Umstände des jeweiligen strafrechtlichen Vorwurfs und die - auch technische - Erfassbarkeit des Datenbestands eine unverzügliche Zuordnung nicht erlauben, muss die vorläufige Sicherstellung größerer Teile oder gar des gesamten E-Mail-Bestands erwogen werden, an die sich eine Durchsicht gemäß § 110 StPO zur Feststellung der potenziellen Beweiserheblichkeit und -verwertbarkeit der E-Mails anschließt. 87

Das Verfahrensstadium der Durchsicht gemäß § 110 StPO ist der endgültigen Entscheidung über den Umfang der Beschlagnahme vorgelagert (vgl. BVerfGE 113, 29 <56>). Es entspricht dem Zweck des § 110 StPO, im Rahmen des technisch Möglichen und Vertretbaren lediglich diejenigen Informationen einem dauerhaften und damit vertiefenden Eingriff zuzuführen, die verfahrensrelevant und verwertbar sind. Während das Verfahren der Durchsicht auf der Grundlage der vorläufigen Sicherstellung zum Zweck der Feststellung der potenziellen Beweiserheblichkeit und -verwertbarkeit auf die Vermeidung eines dauerhaften und umfassenden staatlichen Zugriffs nebst den hiermit verbundenen Missbrauchsgefahren abzielt, würde bei einer endgültigen, bis zum Verfahrensabschluss wirkenden Beschlagnahme des gesamten E-Mail-Bestands der staatliche Zugriff zeitlich perpetuiert und damit erheblich intensiviert. 88

f) Ist den Strafverfolgungsbehörden im Verfahren der Durchsicht unter zumutbaren Bedingungen eine materielle Zuordnung der verfahrenserheblichen E-Mails einerseits oder eine Löschung oder Rückgabe der verfahrensunerheblichen E-Mails an den Nutzer andererseits nicht möglich, steht der Grundsatz der Verhältnismäßigkeit jedenfalls unter dem Gesichtspunkt der Erforderlichkeit der Maßnahme einer Beschlagnahme des gesamten Datenbestands nicht entgegen. Es muss dann aber im jeweiligen Einzelfall geprüft werden, ob der umfassende Datenzugriff dem Übermaßverbot Rechnung trägt. 89

g) Die nach Art. 1 Abs. 1 GG garantierte Unantastbarkeit der Menschenwürde fordert auch im Gewährleistungsbereich des Art. 10 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Es kann nicht ausgeschlossen werden, dass bei der Erfassung der Kommunikationsinhalte personenbezogene Daten betroffen sind, die sich auf den Kernbereich höchstpersönlicher Lebensgestaltung beziehen. Ob eine personenbezogene Kommunikation diesem Kernbereich zuzuordnen ist, hängt davon ab, ob sie nach ihrem Inhalt höchstpersönlichen Charakters ist und in welcher Art und Intensität sie aus sich heraus die 90

Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 <374>; 109, 279 <314>; 113, 348 <391>). Maßgebend sind die Besonderheiten des jeweiligen Einzelfalls (vgl. BVerfGE 80, 367 <374>; 109, 279 <314>). Nicht zu diesem Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten (vgl. BVerfGE 80, 367 <375>; 109, 279 <319>; 113, 348 <391>). Bestehen im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass ein Zugriff auf gespeicherte Telekommunikation Inhalte erfasst, die zu diesem Kernbereich zählen, ist er insoweit nicht zu rechtfertigen und hat insoweit zu unterbleiben (vgl. BVerfGE 113, 348 <391 f.>). Es muss sichergestellt werden, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist (vgl. BVerfGE 113, 348 <392>).

## V.

Der Grundsatz der Verhältnismäßigkeit vermag zwar den staatlichen Zugriff auf die auf dem Mailserver des Providers gespeicherten E-Mails zu begrenzen. Der effektive Schutz materieller Grundrechte bedarf einer den sachlichen Erfordernissen entsprechenden Ausgestaltung des Verfahrens (vgl. BVerfGE 73, 280 <296>; 82, 209 <227>; 113, 29 <57>). Dies gilt auch für die Wahrung der Grundrechte aus Art. 10 Abs. 1 GG. 91

Bei Eingriffen zur Erlangung von Informationen, deren Vertraulichkeit grundrechtlich geschützt ist, wird den Verfahrensgarantien seit jeher ein hoher Stellenwert eingeräumt. Als verfahrensrechtliche Schutzvorkehrungen sind insbesondere Unterrichtungs-, Auskunfts-, Löschungs- und Kennzeichnungspflichten, Teilnahmerechte und Verwertungsverbote anerkannt (vgl. BVerfGE 65, 1 <46>; 100, 313 <360 ff.>; 113, 29 <58>). Schon das geltende Strafprozessrecht enthält diesbezügliche verfahrensrechtliche Vorschriften. Soweit sie nicht genügen, um einen effektiven Schutz des Fernmeldegeheimnisses zu gewährleisten, sind von Verfassungs wegen zusätzliche Anforderungen zu stellen. 92

1. Art. 10 GG vermittelt dem betroffenen Grundrechtsträger einen Anspruch auf Kenntnis von Datenerhebungen, die ihn betreffen. Wie die Kenntnisgewährung im Einzelnen auszugestalten ist, gibt das Grundgesetz nicht vor. Die Mitteilungspflicht unterliegt allerdings dem Gesetzesvorbehalt des Art. 10 Abs. 2 GG (vgl. BVerfGE 100, 313 <361>). 93

Werden in einem Postfach auf dem Mailserver des Providers eingegangene E-Mails sichergestellt, ist zum Schutz des Postfachinhabers, in dessen Recht auf Gewährleistung des Fernmeldegeheimnisses durch die Sicherstellung eingegriffen wird, zu fordern, dass er im Regelfall zuvor von den Strafverfolgungsbehörden unterrichtet wird, damit er jedenfalls bei der Sichtung seines E-Mail-Bestands seine Rechte wahrnehmen kann. Ausnahmen von der Unterrichtungspflicht können geboten sein, wenn die Kenntnis des Eingriffs in das Fernmeldegeheimnis dazu führen würde, dass dieser 94

seinen Zweck verfehlt (vgl. BVerfGE 100, 313 <361>). Werden auf dem Mailserver des Providers gespeicherte E-Mails ausnahmsweise ohne Wissen des Postfachinhabers sichergestellt, so ist dieser so früh, wie es die wirksame Verfolgung des Ermittlungszwecks erlaubt, zu unterrichten. Andernfalls könnte er weder die Unrechtmäßigkeit der Erfassung noch etwaige Rechte auf Rückgabe oder Löschung der Daten geltend machen (vgl. BVerfGE 100, 313 <361>; 109, 279 <363 ff.>).

Diesen Anforderungen wird durch § 35 StPO und § 98 Abs. 2 Satz 6 StPO Rechnung getragen. Vor Anordnung einer Beschlagnahme oder anderer Maßnahmen - zu denen auch die Durchsuchung zählt (vgl. BVerfGE 49, 329 <342>) - ist der Betroffene zwar gemäß § 33 Abs. 4 Satz 1 StPO nicht zu hören, wenn die vorherige Anhörung den Zweck der Anordnung gefährden würde. Jedoch sind richterliche Anordnungen von Durchsuchungen - die bereits allgemeine Richtlinien für die Durchsuchungen beinhalten können und sich auf den Zugriff auf die auf dem Mailserver des Providers des Betroffenen gespeicherten E-Mails beziehen - und Beschlagnahmen in jedem Fall dem Betroffenen vor Durchführung der Maßnahmen gemäß § 35 StPO bekannt zu geben. Im Falle einer vorläufigen Sicherstellung oder Beschlagnahme durch die Staatsanwaltschaft oder ihre Ermittlungspersonen wegen Gefahr im Verzuge ist der Betroffene gemäß § 98 Abs. 2 Satz 6 StPO über sein Antragsrecht nach § 98 Abs. 2 Satz 2 StPO zu belehren. Dies beinhaltet notwendig eine Unterrichtung über die getroffene Maßnahme, sofern der Betroffene nicht ohnehin bei der Maßnahme anwesend war und auf diese Weise Kenntnis davon erlangt hat. 95

2. Die Durchsicht gemäß § 110 StPO bezweckt die Vermeidung einer übermäßigen und auf Dauer angelegten Datenerhebung und damit eine Verminderung der Intensität des Eingriffs in das Fernmeldegeheimnis. Zur Wahrung der Verhältnismäßigkeit kann es im Einzelfall von Verfassungs wegen geboten sein, den Inhaber der sichergestellten E-Mails in die Prüfung der Verfahrenserheblichkeit einzubeziehen. Die Regelung eines Anwesenheitsrechts des Inhabers der durchzusehenden Papiere und Daten in § 110 Abs. 3 StPO a.F. wurde zwar durch das Erste Gesetz zur Modernisierung der Justiz vom 24. August 2004 (BGBl I S. 2198) - ohne Begründung - ersatzlos gestrichen. Gleichwohl kann es im Einzelfall geboten sein, den oder die Inhaber des jeweiligen Datenbestands in die Prüfung der Verfahrenserheblichkeit sichergestellter Daten einzubeziehen. Konkrete, nachvollziehbare und überprüfbare Angaben vor allem Nichtverdächtiger zur Datenstruktur und zur Relevanz der jeweiligen Daten können deren materielle Zuordnung vereinfachen und den Umfang der sicherzustellenden Daten reduzieren (vgl. BVerfGE 113, 29 <58>). Von Verfassungs wegen ist es allerdings nicht geboten, in jedem Fall eine Teilnahme an der Sichtung sichergestellter E-Mails vorzusehen. Ob eine Teilnahme bei der Durchsicht geboten ist, ist im jeweiligen Einzelfall unter Berücksichtigung einer wirksamen Strafverfolgung einerseits und der Intensität des Datenzugriffs andererseits zu beurteilen. 96

3. Soweit E-Mails von den Ermittlungsbehörden gespeichert und ausgewertet werden, kann es geboten sein, den Betroffenen Auskunft über die Datenerhebung zu erteilen, um sie in den Stand zu versetzen, etwaige Grundrechtsbeeinträchtigungen ab- 97

zuwehren.

Dem wird durch die besonderen strafprozessualen Auskunftsregelungen gemäß § 147, § 385 Abs. 3, § 397 Abs. 1 Satz 2 in Verbindung mit § 385 Abs. 3, § 406e und § 475 StPO sowie bei Nichtverfahrensbeteiligten durch § 491 StPO Rechnung getragen. § 491 StPO regelt die Auskunft an von der Datenspeicherung betroffene Nichtverfahrensbeteiligte, sofern für diese die Erteilung oder Versagung von Auskünften in der Strafprozessordnung nicht besonders geregelt ist (vgl. Hilger, in: Löwe-Rosenberg, StPO und GVG, Bd. 6, 25. Aufl. 2001, § 491 Rn. 17). Da nicht sämtliche sichergestellten und hinsichtlich ihrer potenziellen Beweisgeeignetheit noch zu überprüfenden Daten Bestandteil der dem vorrangigen Auskunftsanspruch gemäß § 475 StPO unterliegenden Ermittlungsakten werden, ist hinsichtlich der am Strafverfahren unbeteiligten Drittbetroffenen des Datenzugriffs der subsidiäre Anwendungsbereich des datenschutzrechtlichen Auskunftsanspruchs eröffnet. Wenn nicht der Untersuchungszweck gefährdet werden könnte oder überwiegende schutzwürdige Interessen Dritter entgegenstehen, muss dem Betroffenen gemäß § 491 Abs. 1 Satz 1 StPO entsprechend § 19 BDSG Auskunft erteilt werden. Die Auskunfterteilung entsprechend § 19 BDSG unterbleibt, soweit die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde. Die Benachrichtigung setzt voraus, dass der verantwortlichen Stelle Name und Kontaktdaten des Betroffenen bekannt sind. Nach unbekannten Beteiligten muss und soll allerdings nicht geforscht werden (vgl. Mallmann, in: Simitis, BDSG, 6. Aufl. 2006, § 19a Rn. 18, 44). Ungeachtet des hiermit verbundenen Aufwands würde mit der Namhaftmachung und der damit zusammenhängenden Kenntnisnahme personenbezogener Daten der Rechtseingriff zusätzlich vertieft. Solange im Rahmen der Ermittlungen bestimmte Dateien nicht geöffnet werden oder sich aus geöffneten Dateien kein Betroffener ermitteln lässt, bedarf es daher keiner weitergehenden Recherchen in den sichergestellten Datenbeständen. 98

4. Der begrenzte Zweck der Datenerhebung gebietet grundsätzlich die Rückgabe oder Löschung aller nicht zur Zweckerreichung benötigten kopierten E-Mails (vgl. BVerfGE 100, 313 <362>; 113, 29 <58>). 99

§ 489 Abs. 2 StPO enthält entsprechende Schutzvorkehrungen. Danach sind Daten insbesondere dann von Amts wegen zu löschen, wenn sich aus Anlass einer Einzelfallbearbeitung ergibt, dass deren Kenntnis für den jeweils gesetzlich bezeichneten Zweck nicht mehr erforderlich ist. Diese auf die Aufhebung der Informationsfunktion zielende Regelung korrespondiert mit der strengen Zweckbindung des Datenzugriffs sowie mit der gesetzlich geregelten Bindung der Befugnis des § 483 StPO an den verfahrensbezogenen Erhebungszweck. Eine Löschung gespeicherter Daten ist gemäß § 489 Abs. 2 Nr. 1 StPO ferner dann vorzunehmen, wenn sich das Verfahren, in welchem die Daten verarbeitet wurden, im Sinne des § 489 Abs. 3 StPO erledigt hat. 100

5. In bestimmten Fällen kann von Verfassungs wegen ein Verwertungsverbot bestehen (vgl. BVerfGE 113, 29 <61>). 101

6. Einer Kennzeichnungspflicht - wie sie das Bundesverfassungsgericht in seiner Entscheidung zu den Befugnissen des Bundesnachrichtendienstes zur Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs sowie zur Übermittlung der daraus erlangten Daten an andere Behörden für erforderlich gehalten hat (vgl. BVerfGE 100, 313 <360 f.>) - bedarf es bei der Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails aus verfassungsrechtlicher Sicht nicht. Die jeweilige Zweckbindung ergibt sich aus dem strafprozessualen Ermittlungsverfahren. Auch lässt sich die Herkunft der Daten im Strafverfahren regelmäßig nachverfolgen. 102

**VI.**

Die angegriffenen Beschlüsse genügen den verfassungsrechtlichen Vorgaben für den damit verbundenen Eingriff in Art. 10 Abs. 1 GG. Das Landgericht hat zwar einen Eingriff in das Fernmeldegeheimnis unzutreffend verneint. Den aus Art. 10 Abs. 1 GG folgenden besonderen Anforderungen an die Verhältnismäßigkeit der Sicherung großer Datenmengen außerhalb eines laufenden Kommunikationsvorgangs und an das Verfahren ist es aber im Ergebnis gerecht geworden. 103

1. Die Annahme, die Schwere der den Beschuldigten vorgeworfenen Taten und die Schwierigkeit der Ermittlungen rechtfertigten einen Zugriff auf die E-Mails des Beschwerdeführers, ist verfassungsrechtlich nicht zu beanstanden. Willkürfrei haben die Fachgerichte den Betrugs- und Untreueverdacht im geschäftlichen Verkehr in Bezug auf Beträge von mehreren 100.000 € in ein angemessenes Verhältnis zu den Rechten des an diesen Taten unbeteiligten Beschwerdeführers gesetzt. Der Beschwerdeführer war nach den fachgerichtlichen Feststellungen Verfügungsberechtigter über die Konten, von denen aus und auf die die Gelder zum Teil überwiesen worden waren, und er stand in Kontakt zu den Tatverdächtigen. Die Fachgerichte durften daher die Verbindungen zwischen den Beschuldigten und dem Beschwerdeführer für aufklärungsbedürftig halten. 104

2. Es ist unschädlich, dass in den angegriffenen Beschlüssen von einer Beschlagnahme die Rede ist, obwohl es sich bei dem Zugriff auf die auf dem Mailserver des Providers des Beschwerdeführers gespeicherten E-Mails nicht um eine Beschlagnahme, sondern um eine vorläufige Sicherstellung zum Zwecke der Durchsicht und anschließender Beschlagnahme beweiserheblicher E-Mails handelt. 105

Eine endgültige Beschlagnahme liegt noch nicht vor. Sie hat sich auf konkrete Gegenstände zu beziehen, deren Beweiseignung und Beschlagnahmefähigkeit gegenstandsbezogen zu prüfen sind. Das dafür vorgesehene und der Beschlagnahme vorgelagerte Stadium der Durchsicht ist vorliegend noch nicht abgeschlossen. Die Durchsicht dient dazu, verfahrensrelevante von unerheblichen Daten zu trennen, um die Beschlagnahme sodann nur auf den relevanten Teil des Datenbestands zu erstrecken. Die E-Mails wurden indes noch nicht vollständig auf ihre Beweiserheblichkeit hin durchgesehen, weil das Bundesverfassungsgericht die weitere Durchsicht im Wege einer einstweiligen Anordnung unterbunden hat. 106

Das Landgericht, auf dessen Entscheidung es maßgeblich ankommt, hat im Beschwerdebeschluss ausgeführt, dass E-Mails, die nach der Durchsicht nicht als Beweismittel in Betracht kommen, an den Beschwerdeführer zurück zu geben seien. Dadurch hat es klargestellt, dass das Verfahren der Sichtung - welches noch zur Durchsuchung zählt - noch nicht abgeschlossen ist. Wird eine Beschlagnahmeanordnung im Zusammenhang mit einem Durchsuchungsbeschluss erlassen und erfolgt dabei noch keine genaue Konkretisierung der erfassten Gegenstände, sondern nur eine gattungsmäßige Umschreibung, so handelt es sich um eine bloße Richtlinie für die Durchsuchung (vgl. BVerfGK 1, 126 <133>). 107

3. Auf eine Missachtung der verfassungsrechtlich vorgegebenen Grenzen weist auch nicht die vollständige Kopie aller E-Mails hin. Dieses Vorgehen nimmt vielmehr Rücksicht sowohl auf die Interessen der Betroffenen als auch auf den Ermittlungszweck. Die Vielzahl der potenziell beweiserheblichen E-Mails erschwerte eine grobe Sichtung vor der Kopie vom Mailserver des Providers. Auch die Rechte dieses Unternehmens waren bei der Gestaltung der Ermittlungen zu beachten. Die Beeinträchtigung der durch Art. 13 Abs. 1 GG geschützten Integrität seiner Geschäftsräume war dadurch gering zu halten, dass aufwändige Sichtungen nicht dort stattfanden und ein längerer Aufenthalt der Ermittlungsbeamten dadurch weitestgehend vermieden wurde. Der durch die Ermittlungen erkennbar abgesteckte Zeitrahmen - der Anlage- und Managementvertrag datiert von Oktober 2004 und die Ermittlungen beziehen sich auf darauf in der Folgezeit gründende Geldflüsse - genügt hier zur zeitlichen Eingrenzung der Gegenstände, auf die sich Durchsuchung und Sicherstellung zu richten hatten. Dass tatsächlich E-Mails auch schon aus der Zeit seit Anfang 2004 sichergestellt worden sind, ist augenscheinlich darauf zurückzuführen, dass die E-Mails nicht bereits bei der Sicherstellung gesichtet wurden, und führt nicht zu verfassungsrechtlichen Bedenken gegen die angegriffenen Beschlüsse. 108

Das Landgericht hat ausdrücklich darauf hingewiesen, dass verfahrensirrelevante Daten weder dauerhaft gespeichert noch verwertet werden dürften. Die bloße Möglichkeit, dass die Grenzen einer erlaubten Ermittlungsmaßnahme pflichtwidrig überschritten werden könnten, kann die Rechtmäßigkeit der Ermittlungen nicht von vornherein in Frage stellen. 109

4. Die Vorgaben zur Auswertung großer Datenmengen bei betroffenen Vertrauensverhältnissen und zur Wahrung des absolut geschützten Kernbereichs privater Lebensgestaltung brauchten die Beschlüsse nicht näher auszuformulieren. Die Ermittlungsbehörden haben diese Vorgaben nicht erst aufgrund des richterlichen Beschlusses zu beachten. Die Beschränkungen ergeben sich aus dem Grundsatz der Verhältnismäßigkeit und sind bei der Rechtsanwendung ohne weiteres zu beachten. Umstände, die Anlass gegeben haben könnten, die verfassungsrechtlichen Vorgaben im Hinblick auf den Fall zu spezifizieren, sind nicht ersichtlich. 110

5. In verfahrensrechtlicher Hinsicht wurde der verfassungsrechtlichen Anforderung Genüge getan, den Beschwerdeführer vor dem Zugriff auf die auf dem Mailserver 111

seines Providers gespeicherten E-Mails hierüber zu unterrichten.

6. Von Verfassungs wegen ist nicht zu beanstanden, dass das Landgericht in seiner Beschwerdeentscheidung ein Teilnahmerecht des Beschwerdeführers und seines Rechtsanwalts an der Durchsicht der sichergestellten E-Mails verneint hat. Dahingestellt bleiben kann, ob das Landgericht insoweit überhaupt eine rechtsverbindliche Entscheidung getroffen hat. Jedenfalls lässt sich dem Vorbringen des Beschwerdeführers nicht entnehmen, dass es zur Sicherung der Verhältnismäßigkeit in seinem konkreten Fall von Verfassungs wegen geboten sein könnte, ihn in die Prüfung der Verfahrenserheblichkeit der sichergestellten E-Mails einzubeziehen. Allein aus dem Umstand, dass er Nichtverdächtiger ist, folgt kein verfassungsunmittelbares Teilnahmerecht an der Durchsicht der sichergestellten E-Mails. 112

**C.**

Die einstweilige Anordnung wird mit der Entscheidung in der Hauptsache gegenstandslos. 113

| | | |
|---|---|---|
| Voßkuhle | Broß | Osterloh |
| Di Fabio | Mellinghoff | Lübbe-Wolff |
| Gerhardt | Landau | |

**Bundesverfassungsgericht, Beschluss des Zweiten Senats vom 16. Juni 2009 - 2 BvR 902/06**

**Zitiervorschlag** BVerfG, Beschluss des Zweiten Senats vom 16. Juni 2009 - 2 BvR 902/06 - Rn. (1 - 113), http://www.bverfg.de/e/rs20090616_2bvr090206.html

**ECLI** ECLI:DE:BVerfG:2009:rs20090616.2bvr090206