CyLaw-Report XXVII (11/2009)
ISSN: 1867-1969

TECHNISCHE UNIVERSITÄT DARMSTADT

Cylaw-Report XXVII:
Zu Art. 10 GG bei der „Beschlagnahme“ von E-Mails auf dem Mailserver des Providers und beim Zugriff des Arbeitgebers auf E-Mails des Arbeitnehmers

Entscheidungen des Bundesverfassungsgerichts (BVerfG) vom 16.06.2009 – 2 BvR 902/06,des Verwaltungsgerichtshofs (VGH) Kassel vom 19.05.2009 – 6 A 2672/08.Z und des Verwaltungsgerichts (VG) Frankfurt vom 06.11.2008 – 1 K 628/08.F

Die CyLaw-Reports I-XIX wurden im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts (SICARI (2003 – 2007)) erstellt. Mit CyLaw-Report XX folgende wird dieses Online-Legal-Casebook vom Fachgebiet Öffentliches Recht an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) fortgeführt. Die CyLaw-Reports sind keine „Living Documents“, die ständig aktualisiert werden. Zitierungen können deswegen veraltet sein. Die Rechtfertigung für diese klassische Perspektive ist, dass den in den CyLaw-Reports präsentierten Entscheidungen der Gerichte nur die jeweils geltende Rechtslage zu Grunde gelegt werden konnte. Der Aufgabe der Aktualisierung stellt sich der Lehrstuhl in der integrierten Veranstaltung „Recht der Informationsgesellschaft“. Hier wird das Methodenwissen von Studierenden der Technikwissenschaft so gefördert, dass sie in Übungen an der notwendigen Aktualisierung selbst mitwirken können.

Im Sachverhalt der Entscheidung des BVerfG nehmen die Ermittlungsbehörden Zugriff auf E-Mails, die nicht auf einem Rechner des Durchsuchten, sondern nur beim Provider gespeichert sind. Die Herrschaft des E-Mail-Account-Inhabers ist also nicht absolut, sondern von der Entscheidung des Diensteanbieters über die Preisgabe der Daten abhängig. Im Sachverhalt der Entscheidung des VG Frankfurts verlangt die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) von einem Arbeitgeber, der die Privatnutzung des E-Mail-Accounts erlaubt hatte, die Vorlage der E-Mails seiner Arbeitnehmer. Auch hier behauptet der Arbeitgeber – ähnlich dem Provider – eigene Zugriffsoptionen auf die E-Mails der Arbeitnehmer zu haben und so das Andauern der in Art. 10 GG, § 88 TKG geschützten Telekommunikation. Dieser CyLaw-Report beschäftigt sich also mit zwei E-Mail- Sachverhalten, die zunächst grundlegende Fragen zur Eröffnung des Geltungsbereichs von Art. 10 Abs. 1 GG stellen. In beiden Fällen stellt sich die Frage, wann der von Art. 10 GG geschützte Übermittlungsvorgang abgeschlossen ist. Also abstrakt formuliert: ob geteilte Zugriffsrechte zu E-Mails den Zugang von E-Mails vereiteln und der „Mitgewahrsam“ von Provider und Arbeitgeber das Fortbestehen einer in Art. 10 GG geschützten Telekommunikation begründet. Darüber hinaus enthalten die Entscheidungen wegweisende Aussagen zur Geltung des spezialgesetzlichen Zitiergebots (§ 88 Abs. 3 TKG), das verlangt, dass Befugnisnormen zur Durchbrechung des Fernmeldegeheimnisses dieses ausdrücklich zitieren bzw. erkennbar sein muss, dass der Gesetzgeber eine Abwägung mit Art. 10 GG vorgenommen hat. Über die Fragen nach der Eröffnung des Geltungsbereichs von Art. 10 GG, der Reichweite des Zitiergebots des § 88 Abs. 3 S. 3 TKG hinaus entwirft das BVerfG die verfassungsrechtlichen Konturen eines „Beschlagnahmerechts“ für E-Mails anhand folgenden Sachverhalts:

Die Strafverfolgungsbehörden ordnen eine Durchsuchung der Wohnung des Verfassungsbeschwerdeführers B an. B selber ist nicht Beschuldigter einer Untreue bzw. eines Betrugs. Gegen ihn wird „nur“ ermittelt, weil er die zwei Beschuldigten dieser Vergehen kennt und Geldüberweisungen im Kontext des Betrugs- und Untreueverdachts über Konten erfolgten, zu denen B Zugriff hat. Bei der Wohnungsdurchsuchung wird festgestellt, dass B über einen PC verfügt. Die Ermittlungsbehörden interessieren sich für die E-Mails des B. Informationstechnologisch besteht in diesem dem Bundesverfassungsgericht (BVerfG) vorgelegten Sachverhalt die Besonderheit, dass B seine E-Mails nicht auf dem lokalen Rechner in der Wohnung speichert, sondern die E-Mails beim Provider sowohl zwischen- als auch endgespeichert bleiben. B muss also eine Internetverbindung zum Provider herstellen, um von seinen E-Mails Kenntnis nehmen zu können. B, der sich über seine Rechte nicht im Klaren ist, verrät den Ermittlungsbehörden bei der Wohnungsdurchsuchung, dass seine E-Mails bei einem bestimmten Provider gespeichert seien. Er weigert sich aber, sein Passwort bekannt zu geben bzw. den Zugriff auf die E-Mails zu ermöglichen. Die Ermittlungsbehörden veranlassen darauf hin, dass beim Provider ca. 2500 E-Mails von B kopiert werden und an die Ermittlungsbehörden herausgegeben werden. Die Entscheidung des BVerfG ist bedeutsam, weil sie höchstrichterlich die in Literatur und Rechtsprechung umstrittene Frage nach den Voraussetzungen für die vorläufige Sicherstellung, Durchsicht und Beschlagnahme von beim Provider gespeicherten E-Mails klärt. Der 2. Senat des BVerfG hat sich für die Entscheidung fast 3 Jahre Zeit gelassen. Im Ergebnis behandelt das BVerfG die Beschlagnahme von beim Provider endgespeicherten E-Mails wie die gewöhnliche Beschlagnahme von Gegenständen (§§ 94, 95, 98 StPO). Es unterscheidet sich damit von der Ansicht des Bundesgerichtshofs, der die E-Mail-Beschlagnahme den gleichen Voraussetzungen wie eine Postbeschlagnahme (§ 99 StPO; Parallelität von Realworld und Cyberspace) unterwirft wie auch von der Literatur und Rechtsprechung, die für die „Beschlagnahme“ von E-Mails beim Provider die erhöhten Voraussetzungen einer Telekommunikationsüberwachung (Vorliegen einer sogenannten Katalogtat, § 100a StPO) verlangen.

Gliederung:

Teil 1: Sachverhalt:

[1]Die Staatsanwaltschaft ermittelte gegen S und G wegen des Verdachts des Betrugs und der Untreue. Gegenüber dem Verfassungsbeschwerdeführer B[2] bestand hingegen kein Verdacht der Beteiligung an diesen Straftaten. B kannte nur S und G und er hatte Zugriffsberechtigung auf Konten (der Firmen I und E), über die Überweisungen zugunsten von S und G erfolgten. B war also nicht Verdächtiger und damit eine so genannte "andere Person", deren Wohnung im Kontext der Ermittlungen durchsucht wurde.

FEX: Durchsuchung beim Verdächtigen[3] und Durchsuchung bei anderen Personen
Das Strafprozessrecht (StPO) unterscheidet grundsätzlich zwischen Ermittlungsmaßnahmen gegenüber

- **dem Verdächtigen** (§ 102 StPO: „[…] welcher als Täter oder Teilnehmer einer Straftat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist […]") und

[1] Die Schilderung des Sachverhalts erfolgt in Anlehnung an BVerfG; einzelne Veränderungen aus didaktischen Gründen werden angekündigt.

[2] **FINT (Für Interessierte)**: **Zum Instanzenweg**
B wehrt sich hier gegen Entscheidungen eines Amts- und eines Landgerichts vor dem Bundesverfassungsgericht. Gegen die erste richterliche Anordnung legte B Beschwerde beim Amtsgericht ein. Weil das Amtsgericht nicht abhalf, wurde das Landgericht befasst. Dann erhob B Verfassungsbeschwerde.
§ 304 Strafprozessordnung (StPO) [Zulässigkeit]
(1) Die Beschwerde ist gegen alle von den Gerichten im ersten Rechtszug […] zulässig […]
(2)[…] andere Personen können gegen Beschlüsse und Verfügungen, durch die sie betroffen werden, Beschwerde erheben. [...]
§ 306 StPO [Einlegung; Abhilfe oder Vorlegung]
(1) Die Beschwerde wird bei dem Gericht, von dem […]die angefochtene Entscheidung erlassen ist […] eingelegt.
(2) Erachtet das Gericht […]die Beschwerde für begründet, so haben sie ihr abzuhelfen; andernfalls ist die Beschwerde sofort, spätestens vor Ablauf von drei Tagen, dem Beschwerdegericht vorzulegen. [...]
§ 60 Gerichtsverfassungsgesetz (GVG) [Zivil- und Strafkammern]
Bei den Landgerichten werden Zivil- und Strafkammern gebildet.
§ 73 GVG [Allgemeine Zuständigkeit in Strafsachen]
(1) Die Strafkammern entscheiden über Beschwerden gegen Verfügungen des Richters beim Amtsgericht […]
§ 309 StPO [Entscheidung]
(1) Die Entscheidung über die Beschwerde ergeht ohne mündliche Verhandlung, in geeigneten Fällen nach Anhörung der Staatsanwaltschaft.
(2) Wird die Beschwerde für begründet erachtet, so erlässt das Beschwerdegericht zugleich die in der Sache erforderliche Entscheidung.
Art. 93 GG [Bundesverfassungsgericht, Zuständigkeit]
(1) Das Bundesverfassungsgericht entscheidet:
[…]
4a.über Verfassungsbeschwerden, die von jedermann mit der Behauptung erhoben werden können, durch die öffentliche Gewalt in einem seiner Grundrechte oder in einem seiner in Artikel 20 Abs. 4, 33, 38, 101, 103 und 104 enthaltenen Rechte verletzt zu sein;

[3] Die Verwendung männlicher Sprache erfolgt im Interesse von Kürze und Klarheit der Sprache, will aber nicht die Existenz weiblicher Kompetenz ignorieren.

- **der „anderen Person**“, also jemandem, der vielleicht Kontakt zu den Verdächtigen oder zur Tat hat, aber selber nicht im Verdacht steht, straffällig geworden zu sein (siehe § 103 StPO).[4]

Konsequent gelten für die Durchsuchung unterschiedliche Vorschriften, je nachdem ob beim Verdächtigen oder bei anderen Personen ermittelt wird.

Bei der Wohnungsdurchsuchung wurde im Beisein des B ein Computer gefunden. Die Strafverfolgungsbehörden interessierten sich für die E-Mails des B – insbesondere solche, die er vielleicht mit S und G ausgetauscht hatte. B teilt den Behörden nur mit, dass auf seinem Rechner keine E-Mails gespeichert seien – er greife auf die bei Provider P zwischen- und endgespeicherten Mails mit dem Internet Message Access Protocol (IMAP) zu:

BVerfG:

„[…] 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. […]“[5]

FÖR-Technik: Phasen der Speicherung und des Zugriffs beim Provider

Der Vorgang der Übertragung einer E-Mail unter Verwendung von IMAP kann – nach der Literatur - in **vier Phasen** unterteilt werden[6]:

Phase 1: die Übertragung der E-Mails vom Absender auf den Mailserver des Providers,

Phase 2: die Phase des „Ruhens“ der E-Mails auf dem Mailserver des Providers nach ihrer dortigen Zwischenspeicherung **(Zwischenspeicherung)**,

Phase 3: der Abruf- beziehungsweise Lesevorgang durch den Empfänger mittels Herstellung einer Internetverbindung zum Mailserver des Providers,

Phase 4: die Aufbewahrung der (gelesenen) E-Mails auf dem Mailserver des Providers **(Endspeicherung)**.

Nach Ansicht von FÖR könnte man theoretisch auch noch unterscheiden zwischen Mails, die bereits zur Kenntnis genommen wurden und solchen, die noch nicht abgerufen wurden. Bedeutung hätte diese Unterscheidung, weil man argumentieren könnte, dass **in jedem Fall bei den nicht abgerufenen Mails der Telekommunikationsvorgang (Art. 10 Abs. 1 GG)** noch nicht abgeschlossen ist (Phase 2).[7]

[4] Nack, in: Karlsruher Kommentar zur StPO, 6. Auflage 2008, § 103 StPO Rn. 1.

[5] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 21.

[6] Schlegel: "Beschlagnahme" von E-Mail-Verkehr beim Provider, in: HRRS Februar 2007, S.44, 47 (letzter Abruf: 27.11.2009); Störing: Anmerkung zu LG Hamburg, Beschluss vom 08.01.2008, Az. 619 Qs 1/08 in MMR 2008, S. 186, 188; vgl. zum „4-Phasen-Modell" auch Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 102ff. Neuere Ansätze entwickeln sogar ein 7-Phasen-Modell (Brodowski: „Strafprozessualer Zugriff auf E-Mail-Kommunikation“, in: JR 2009, 402ff).

[7] So der Bundesbeauftragte für Datenschutz in seiner Stellungnahme zu der Verfassungsbeschwerde: BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 36. – Das BVerfG folgt dieser Auffassung nicht, weil es auch bei den gelesenen Mails noch vom Schutz von Art. 10 Abs. GG ausgeht. Die Differenzierung zwischen gelesenen und nicht gelesenen Mails, die nur beim Provider gespeichert sind, spiegelt sich damit nicht in der Rechtsprechung des BVerfG.

B verweigerte der Staatsanwaltschaft nach Herstellung einer Internetverbindung zu seinem Provider den Zugriff auf seine E-Mails. Daraufhin erging auf fernmündlichen Antrag der Staatsanwaltschaft ein auf §§ 94, 98, 103 Abs. 1, 105 Abs. 1 StPO gestützter Beschluss des Amtsgerichts, durch den die „Beschlagnahme" der Daten des B auf dem E-Mail-Account seines Providers angeordnet wurde.

§ 103 Strafprozessordnung (StPO) [Durchsuchung bei anderen Personen]

(1) Bei **anderen Personen** sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. […]

§ 105 StPO [Anordnung; Ausführung]

(1) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. [ ]

§ 94 StPO [Gegenstand der Beschlagnahme]

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

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

§ 98 StPO [Anordnung der Beschlagnahme]

(1) Beschlagnahmen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. […]

FEX: „Beschlagnahme" von beim Provider zwischen- und endgespeicherten E-Mails – Zahl der Anordnungen und Zeitpunkt der Benachrichtigung

Nach **FÖR-Ansicht** setzt die „Beschlagnahme" in dieser Konstellation zwei strafprozessuale Anordnungen voraus:

- zum einen eine Anordnung gegenüber dem Provider, dass er die Daten herausgeben muss (grundsätzlich darf er das ohne Anordnung nicht, weil er vertraglich und gesetzlich zur Wahrung des Fernmeldegeheimnisses[8] verpflichtet ist (§ 88 TKG)).

§ 88 Telekommunikationsgesetz (TKG) [Fernmeldegeheimnis]

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. […]

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. […]

[8] Soweit man eben davon ausgeht, dass etwa Phase 4 noch Telekommunikation ist. Andernfalls ist der Provider zur Wahrung des Rechts auf informationelle Selbstbestimmung bzw. auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme verpflichtet (Schutzpflicht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs.1 GG)

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Beim Provider ist keine Durchsuchung gewollt – Rechtsgrundlage des Herausgabeanspruchs („Vorläufige Sicherstellung“) ist die Beschlagnahmevorschrift (§ 95 StPO).[9]

§ 95 StPO [Herausgabepflicht]
(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.
[…]

- Zum anderen eine weitere Anordnung gegenüber dem B, damit er weiß, dass sein E-Mails nun „beschlagnahmt werden“, sie nun bei den Ermittlungsbehörden sind und er seine Rechte geltend machen kann.

FÖR-Kritik: Das BVerfG kann sich zu dieser klaren Aussage nicht durchringen. Es verlangt keine zweite Anordnung gegenüber B, sondern im „Regelfall“ nur die „Benachrichtigung“ des B über die Anordnung gegen P:

BVerfG:
„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 […].
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.** […]“[10]

Bei der Benachrichtigung sollte eigentlich zwischen

- der Bekanntmachung der Anordnung (FEX: siehe Rechtsgedanke des § 35 StPO) und

[9] Anderer Meinung wohl der BGH (Beschluss vom 5.8.2003, Az 2 BJs 11/03-5 StB 7/03), der bezüglich der vorläufigen Sicherstellung allein auf die Vorschriften der Durchsuchung und Durchsicht abstellen will (§ 103, 110 StPO). Zu § 95 StPO siehe auch Schlegel: „Beschlagnahme“ von E-Mail-Verkehr beim Provider, in: HRRS Februar 2007, S. 44, 49f.

[10] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 93f.

- der Anhörung des B zu dieser Anordnung – vor ihrem Vollzug - (FEX: siehe Rechtsgedanke des § 33 Abs. 4 S. 1 StPO) unterschieden werden.

In Ermangelung klarer gesetzlicher Vorgaben rekurriert das BVerfG auf den Rechtsgedanken von § 33 Abs. 4 StPO und seine Rechtsprechung zur Fernmeldeüberwachung durch den Bundesnachrichtendienst (BVerfG 100, 313, 361) und bejaht die Ausnahme von der Anhörungspflicht und damit die Rechtmäßigkeit einer heimlichen „Beschlagnahme“ beim Provider.

BVerfG:
„Ausnahmen von der Unterrichtungspflicht können geboten sein, wenn die Kenntnis des Eingriffs in das Fernmeldegeheimnis dazu führen würde, dass dieser 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 […].“[11]

Theoretisch wäre denkbar, dass B dem P (mit einstweiligem Rechtschutz) aufgibt, der seiner Meinung nach rechtswidrigen Anordnung nicht Folge zu leisten. Nach der Rechtsprechung des BVerfG wäre es in solchen Fällen nicht ausgeschlossen, dass heimlich „beschlagnahmt“ wird – auch wenn salvatorisch regelmäßig (grammatische Auslegung aber eben nicht immer) eine Benachrichtigung vor der Anordnung postuliert wird.

BVerfG:
„[…] 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.“[12]

Zusammenfassend ist festzuhalten, dass das BVerfG auch eine rechtswidrige „Beschlagnahme“ beim Provider in Kauf nimmt, wenn B dann nach der „Beschlagnahme“ seine Rechte bei der Durchsicht der Daten wahrnehmen kann. Insoweit reicht nach dieser BVerfG-Rechtsprechung in Einzelfällen die Benachrichtigung **nach** „Beschlagnahme“ beim Provider aus.[13]

Auf der Grundlage dieses Beschlusses wurde der gesamte E-Mail-Bestand des B – 2500 E-Mails aus dem Zeitraum von Anfang 2004 bis 14. März 2006 - kopiert, aus den Räumen des

[11] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 94.
[12] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 95.
[13] von Brodowski, JR 2009, 402ff als „kollusiver Zugriff“ bezeichnet.

Providers entfernt und zu den Ermittlungsbehörden zur Durchsicht gebracht. B beanstandet, dass die Ermittlungsbehörden die falschen Rechtsgrundlagen zugrundegelegt hätten und die Systematik von Sicherstellung, Durchsicht und Beschlagnahme verkannt hätten.

BVerfG:

„[…] Die Fachgerichte hätten die strafprozessuale Reihenfolge von Sicherstellung, Durchsicht und Beschlagnahme verkannt. Er und sein Rechtsanwalt seien an der Durchsicht zu beteiligen. […]“[14]

FÖR-Dogmatik und FÖR-Hintergrund: „Beschlagnahme“ - Verfahrensstadien

Zunächst sind die Leser dieses CyLaw-Reports, die über keine juristischen Spezialkompetenzen verfügen, darüber zu informieren, dass die Kenntnis der strafprozessualen Terminologie und Systematik hinsichtlich

- Durchsuchung
- (vorläufige) Sicherstellung
- Durchsicht und
- endgültige Beschlagnahme

weder einem Generalbundesanwalt noch dem BVerfG als selbstverständlich unterstellt werden kann. So hat der Bundesgerichtshof 2003 den Generalbundesanwalt kritisiert, weil er eine „vorläufige Sicherstellung“ mit einer „Beschlagnahme“ verwechselt habe[15]. Auch das BVerfG ist zweideutig, wenn es in der hier präsentierten Entscheidung zum einen auf Beschlagnahmevorschriften (§§ 94, 95 StPO) abstellt, dann aber über eine „vorläufige Sicherstellung“ und den Kontext zur „Durchsuchung“ (§ 103 StPO) schreibt.

BVerfG:

„[…] 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.

[…]

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 […].“[16]

[14] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 29.

[15] BGH, Beschluss vom 05.08.2003, Az. 2 BJs 11/03-5 - StB 7/03.

[16] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 105, 107.

Diese Kritik am BVerfG erfolgt, um den Lesern der Entscheidung zu verdeutlichen, wie umstritten und dogmatisch ungeklärt die aufgeworfenen Rechtsfragen sind. **FÖR** schlägt zur Systematisierung der Streitfragen folgende Terminologie und Systematik vor, wobei ein kontradiktorisches Szenario zugrundegelegt wird (also nicht der Fall, dass eine „andere Person" freiwillig den Zugang zu ihren beim Provider zwischen- und endgespeicherten Mails ermöglicht). Zunächst erfolgt

(1) eine **Durchsuchung**. Bei der Durchsuchung eines nicht Verdächtigen gilt:

§ 103 StPO [Durchsuchung bei anderen Personen]
(1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder **zur Verfolgung von Spuren einer Straftat** oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. […]
§ 105 StPO [Anordnung; Ausführung]
(1) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. […]

Grundsätzlich kann die Durchsuchung in der Wohnung erfolgen – wie hier bei B geschehen. Die Durchsuchung der Wohnung hatte nach der richterlichen Durchsuchungsanordnung den Zweck, Informationen über die Kontenführung des B (über die Konten der Firmen I und E, auf die er zugriffsberechtigt war) sowie die rechtlichen Hintergründe seiner und anderer Verfügungen zu erhalten.

BVerfG:
„[…] 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. […]"[17]

(2) An eine Durchsuchung schließt sich, wenn die Ermittlungsbehörden fündig werden, regelmäßig eine **„vorläufige Sicherstellung**" an. Weil dies so ist, nimmt die Literatur und Rechtsprechung an, dass die Befugnis zur Durchsuchung die Befugnis zur vorläufigen Sicherstellung grundsätzlich umfasst.[18] Diese Sicherstellung setzt aber voraus, dass B freiwillig die Daten zur Verfügung stellt. Wenn die Freiwilligkeit fehlt, bedarf es entweder

- einer Anordnung entsprechend den Vorschriften über eine endgültige Beschlagnahme (§§ 94, 95 StPO) oder

[17] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 20.

[18] BGH, Beschluss vom 05.08.2003, Az. 2 BJs 11/03-5 - StB 7/03; OLG Jena, Beschluss vom 20.11.2000, Az. 1 WS 313/00; Radtke: „Rechtsbehelfe gegen die „Durchsicht" (§ 110 StPO) von EDV-Anlagen durch Strafverfolgungsbehörden", JurPC Web-Dok. 173/1999, Abs.19 (letzter Abruf: 27.11.2009);

- einer Anordnung zur Überwachung der Telekommunikation (§ 100a StPO – dazu später).

§ 94 StPO [Gegenstand der Beschlagnahme]
(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.
(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme. […]
§ 95 StPO [Herausgabepflicht]
(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.
(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.
§ 98 StPO [Anordnung der Beschlagnahme]
1) Beschlagnahmen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. […]

(3) Wenn die vorläufige Sicherstellung abgeschlossen ist, erfolgt die **Durchsicht** der elektronischen Dokumente (§ 110 StPO).

§ 110 StPO[19] [Durchsicht von Papieren und elektronischen Speichermedien]
(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu.
(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.
(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung 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.

(4) Nach der Durchsicht der Dokumente erfolgt die Entscheidung über **die endgültige Beschlagnahme von Dokumenten für das Strafverfahren**. Zusammenfassend ist festzuhalten, dass eine „Beschlagnahme“ vier voneinander zu trennende Verfahrensschritte verlangt.

Festzuhalten ist, dass der Ermittlungsvorgang sich im Sachverhalt im Verfahrensstadium (2) (siehe oben unter FEX) befindet – es geht um die vorläufige Sicherstellung der ca. 2500 E-Mails vor einer Durchsicht der E-Mails. Weil diese vorläufige Sicherstellung und ihre Rechtsgrundlagen umstritten waren, hatte das BVerfG bis zur vorliegenden Entscheidung die Versiegelung der E-Mails (des Datenträgers, auf den sie kopiert wurden) verlangt und eine

[19] Aus didaktischen Gründen wird hier eine aktuelle – und nicht die zum Zeitpunkt der kritisierten Entscheidungen geltende - Fassung des Gesetzes zugrundegelegt.

Durchsicht verboten.[20] Die Vorinstanzen (Amtsgericht und Landgericht) folgten den Einwänden des B **nicht**, der sich

- **von den Ermittlungsbehörden getäuscht fühlt**,

BVerfG:

„[…] **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**."[21]

- **das Fehlen der Voraussetzungen für die richtige Rechtsgrundlage – nämlich für die Bestimmungen über die Telekommunikationsüberwachung (§ 100a StPO) – beanstandet**,

§ 100a StPO [Überwachung der Telekommunikation] (**FEX:** aus didaktischen Gründen wird hier die aktuelle Fassung zugrundegelegt; zur Dynamik dieser Ermächtigungsgrundlage siehe im Anhang)

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1.**bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat**,

2.**die Tat auch im Einzelfall schwer wiegt** und

3.**die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre**.

(2) **Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind**:

1.aus dem Strafgesetzbuch:

a)Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82, 84 bis 86, 87 bis 89a, 94 bis 100a,

b)Abgeordnetenbestechung nach § 108e,

c)Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,

d)Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

e)Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,

f)Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2,

[20] BVerfG, einstweilige Anordnung durch Beschluss vom 29.06.2006, Az. 2 BvR 902/06; zuletzt wiederholt durch Beschluss vom 06.05.2009.

[21] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 25.

g)Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Abs. 1 bis 3, § 184c Abs. 3,

h)Mord und Totschlag nach den §§ 211 und 212,

i)Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,

j)Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k)Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l)gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m)Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,

n)Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,

o)Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,

p)Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,

[…]

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

(4) **Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.**

Im Unterschied zu dieser aktuellen Fassung war damals der Betrug (§ 100a Abs. 2 Nr. 1n) StPO) keine Katalogtat **und berechtigte nicht zur Telekommunikationsüberwachung und damit nach Ansicht von B auch nicht zur „Überwachung" seiner E-Mails.** Außerdem wurde mit Abs.4 eine gesetzliche Regelung zum Schutz des Kernbereichs privater Lebensgestaltung eingeführt, um den verfassungsrechtlichen Vorgaben aus der Rechtsprechung des BVerfG zu entsprechen

- **ein eigenes Anwesenheitsrecht bzw. Anwesenheitsrecht seines Rechtsanwalts bei der Durchsicht verlangt.**

BVerfG:

Ergänzung der Verfasserin: Die Vorinstanz hatte geurteilt:

„Für eine Teilnahme des Beschwerdeführers und seines Rechtsanwalts an der

Durchsicht gebe es keine Rechtsgrundlage.“[22]

FEX: Ermächtigungsgrundlage für die Sicherstellung, Durchsicht und Beschlagnahme von E-Mails, die beim Provider gespeichert sind:
Festzuhalten ist, dass der vorliegende Sachverhalt von Literatur und Rechtsprechung unterschiedlich beurteilt wird:

(1) Mit der Argumentation, der Abruf der E-Mails setze eine Telekommunikation voraus (Internetverbindung), vertritt ein Teil der Literatur[23] und der Rechtsprechung[24], dass die spezifischen Voraussetzungen einer Telekommunikationsüberwachung vorliegen müssten. So setzt im Strafprozessrecht der Eingriff in das Fernmeldegeheimnis (Art. 10 GG) das Vorliegen

- des Verdachts einer Katalogtat (§ 100a Abs. 2 StPO) und
- den Respekt vor dem absolut geschützten Kernbereich privater Lebensgestaltung (§ 100a Abs. 4 StPO) voraus.

Zusammenfassend ist festzuhalten, dass nach diesen Rechtsprechungs- und Literaturmeinungen die Eingriffsvoraussetzungen in das Fernmeldegeheimnis qualifiziert und relativ hoch sind.

(2) Einer anderen Meinung ist der Bundesgerichtshof (BGH)[25], der E-Mails wie Briefe behandelt und als Ermächtigungsgrundlage für den Eingriff in das Fernmeldegeheimnis § 99 StPO zugrundelegt.

§ 99 StPO [Postbeschlagnahme]
Zulässig ist die Beschlagnahme **der an den Beschuldigten gerichteten Postsendungen** und Telegramme, die sich im Gewahrsam von Personen oder Unternehmen befinden, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder daran mitwirken. Ebenso ist eine Beschlagnahme von Postsendungen und Telegrammen zulässig, bei denen **aus vorliegenden Tatsachen zu schließen ist, dass sie von dem Beschuldigten herrühren oder für ihn bestimmt sind und dass ihr Inhalt für die Untersuchung Bedeutung hat.**
§ 100 StPO [Zuständigkeit]
(1) Zu der Beschlagnahme (§ 99) ist **nur das Gericht**, **bei Gefahr im Verzug** auch die **Staatsanwaltschaft befug**t.

[22] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn.26.
[23] Schlegel: "Beschlagnahme" vom E-Mail-Verkehr beim Provider, in: HRRS Februar 2007, S. 44, 51 (letzter Abruf: 27.11.2009); Gaede: „Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Überwachung“, in: StV 2/2009, S. 96, 99ff (letzter Abruf: 27.11.2009).
[24] Für eine Anwendung des § 100a StPO beim Zugriff auf beim Provider zwischengespeicherte E-Mails: LG Hanau, Beschluss vom 23.09.1999, Az.: 3 Qs 149/99; für eine Anwendung des § 100a StPO unabhängig davon, ob die E-Mails beim Provider zwischen- oder endgespeichert sind: LG Hamburg, Beschluss vom 08.01.2008, Az.:619 Qs 1/08;
[25] BGH, Beschluss vom 31.03.2009, Az.: 1 StR 76/09;

(2) Die **von der Staatsanwaltschaft verfügte Beschlagnahme tritt**, auch wenn sie eine Auslieferung noch nicht zur Folge gehabt hat, **außer Kraft, wenn sie nicht binnen drei Werktagen gerichtlich bestätigt wird.**
(3) Die Öffnung der ausgelieferten Postsendungen steht dem Gericht zu. Es kann diese Befugnis der Staatsanwaltschaft übertragen, soweit dies erforderlich ist, um den Untersuchungserfolg nicht durch Verzögerung zu gefährden[…]

Dies hat zur Folge, dass „Beschlagnahmen" nur hinsichtlich der an den Beschuldigten gerichteten Post rechtmäßig sind. Damit wird Post, die an andere Personen – hier den B - gerichtet ist, nicht erfasst. § 99 StPO stellt sich damit als eine besondere und beschränkende Ausformung der „Beschlagnahme"-Vorschriften über Gegenstände dar.

(3) Nur vereinzelt wurde bisher vertreten,[26] dass die beim Provider gespeicherten Mails wie „Gegenstände" zu behandeln seien und deswegen die Ermächtigungsgrundlage für die „Beschlagnahme" keine Katalogstraftat sei und auch im Gesetz kein ausdrücklich (vgl. § 100a Abs. 4 StPO) geschützter Kernbereich privater Lebensgestaltung vorgesehen werden müsse. Als Rechtsgrundlage reichten §§ 94, 95 (nach FÖR-Ansicht im Kontext von §§ 103, 110 StPO). Eine solche Meinung könnte nach FÖR-Ansicht als Parallelwertung von Cyber- und Realworldsachverhalten bewertet werden.

Wenn die Durchsicht von Daten in einer Parallelwertung wie die Durchsuchung von Gegenständen zu behandeln wäre (vgl. oben FEX Nr. 3.), dann müsste B ein Anwesenheitsrecht aus § 106 Abs. 1 S. 1 StPO haben. Der Rechtsanwalt der Beschuldigten S und G (Verteidiger) soll ein Anwesenheitsrecht aus Vernehmungsrecht haben – so jedenfalls Literaturstimmen[27].

§ 106 StPO [Zuziehung des Inhabers]

(1) Der Inhaber der zu durchsuchenden Räume oder Gegenstände darf der Durchsuchung beiwohnen. Ist er abwesend, so ist, wenn möglich, sein Vertreter oder ein erwachsener Angehöriger, Hausgenosse oder Nachbar zuzuziehen. […]

Wie aus CyLaw-Report XX: „Verdeckte Online-Durchsuchungen" bekannt ist, handelt es sich bei dieser gesetzlichen Regelung des Anwesenheitsrechts des B jedenfalls nach der Ansicht des 3. Strafsenats des BGH nicht nur um eine Ordnungsvorschrift. [28] Ein Anwesenheitsrecht des Rechtsanwalts des nicht Beschuldigten B könnte – nachdem mit Wirkung zum 31.8.2004

[26] Für eine Anwendung der Bestimmungen über die Sicherstellung und Beschlagnahme von Gegenständen (§§ 94ff. StPO): Nack, in: Karlsruher Kommentar zur StPO, 6. Auflage 2008, § 100a StPO Rn. 22; LG Braunschweig in dem von B mit der Verfassungsbeschwerde angegriffenen Beschluss vom 12.04.2006, Az.: 6 Qs 88/06.

[27] So auch die Argumentation von Knauer/Wolf: „Zivilprozessuale und strafprozessuale Änderungen durch das Erste Justizmodernisierungsgesetz", in: NJW 2004, S. 2932, 2937f und von Burhoff, Handbuch für das strafrechtliche Ermittlungsverfahren, 5. Auflage 2009, Rn. 578.

[28] Dies setzt voraus, dass man nicht § 110 StPO auf die Durchsicht elektronischer Dokumente anwendet.

§ 110 Abs. 3 StPO alter Fassung außer Kraft trat – gegebenenfalls aus dem Hausrecht[29] des B resultieren

§ 110 Abs. 3 StPO alter Fassung

(3) Dem Inhaber der Papiere oder dessen Vertreter ist die Beidrückung seines Siegels gestattet; auch ist er, falls demnächst die Entsiegelung und Durchsicht der Papiere angeordnet wird, wenn möglich, zur Teilnahme aufzufordern.

B hatte mit seiner Beschwerde vor dem Landgericht keinen Erfolg. Gegen diesen Beschluss des Landgerichts erhob B Verfassungsbeschwerde zum BVerfG.

Art. 93 GG [Bundesverfassungsgericht, Zuständigkeit]

(1) Das Bundesverfassungsgericht entscheidet:

[…]

4.a) über Verfassungsbeschwerden, die von jedermann mit der Behauptung erhoben werden können, durch die öffentliche Gewalt in einem seiner Grundrechte oder in einem seiner in Artikel 20 Abs. 4, 33, 38, 101, 103 und 104 enthaltenen Rechte verletzt zu sein;

[…]

Er sieht sich durch den Zugriff auf seine auf dem E-Mail-Account beim Provider gespeicherten E-Mails in seinen Grundrechten verletzt. Er rügt unter anderem eine Verletzung

- des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) und
- des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Art. 10 GG [Brief-, Post- und Fernmeldegeheimnis]

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. […]

Art. 1 GG [Schutz der Menschenwürde, Menschenrechte, Grundrechtsbindung]

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. […]

[29] Schlothauer, in: Widmaier: Münchener Anwaltshandbuch Strafverteidigung, 1. Auflage 2006, Teil B § 3 Rn. 66.

B bringt vor, dass die Vorschriften über die Sicherstellung und Beschlagnahme (§§ 94 ff. StPO) nicht als gesetzliche Grundlage für Eingriffe in das Fernmeldegeheimnis dienen könnten. Der Zugriff auf die auf dem Mailserver des Providers gespeicherten E-Mails dürfe nur unter den gesetzlichen Voraussetzungen des § 100 a StPO (in der bei Erlass der gerichtlichen Beschlüsse geltenden Fassung) erfolgen, die aber mangels des Verdachts der Begehung einer der in § 100 a S. 1 Nr. 1-5 StPO genannten Straftatbestände nicht erfüllt seien.

§ 100 a StPO alte Fassung[30] [Überwachung der Telekommunikation]

Die Überwachung und Aufzeichnung der Telekommunikation darf angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer

1.a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80 bis 82, 84 bis 86, 87 bis 89, 94 bis 100a des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),

b) Straftaten gegen die Landesverteidigung (§§ 109d bis 109h des Strafgesetzbuches),

c) Straftaten gegen die öffentliche Ordnung (§§ 129 bis 130 des Strafgesetzbuches, § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes),

[…]

2. eine Geld- oder Wertpapierfälschung (§§ 146, 151, 152 des Strafgesetzbuches),

einen schweren sexuellen Missbrauch von Kindern nach § 176a Abs. 1 bis 3 oder 5 des Strafgesetzbuches oder einen sexuellen Missbrauch von Kindern mit Todesfolge nach § 176b des Strafgesetzbuches,

eine Verbreitung pornografischer Schriften nach § 184b Abs. 3 des Strafgesetzbuches

einen Mord, einen Totschlag (§§ 211, 212 des Strafgesetzbuches) oder einen Völkermord (§ 6 des Völkerstrafgesetzbuches)

eine Straftat gegen die persönliche Freiheit (§ 232 Abs. 3, 4 oder Abs. 5, § 233 Abs. 3, je-

weils soweit es sich um Verbrechen handelt, §§ 234, 234a, 239a, 239b des Strafgesetzbuches),

einen Bandendiebstahl (§ 244 Abs. 1 Nr. 2 des Strafgesetzbuches) oder einen schweren Bandendiebstahl (§ 244a des Strafgesetzbuches),

einen Raub oder eine räuberische Erpressung (§§ 249 bis 251, 255 des Strafgesetzbuches),

eine Erpressung (§ 253 des Strafgesetzbuches),

eine gewerbsmäßige Hehlerei, eine Bandenhehlerei (§ 260 des Strafgesetzbuches) oder eine gewerbsmäßige Bandenhehlerei (§ 260a des Strafgesetzbuches),

eine Geldwäsche, eine Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 oder 4 des Strafgesetzbuches,

[…]

[30] § 100 a StPO in der vom 19.02.2005 bis zum 29.11.2007 geltenden, für die Entscheidung des BVerfG maßgeblichen Fassung.

begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

B macht zudem eine Verletzung des Verhältnismäßigkeitsprinzips geltend. Die Beschlagnahme des gesamten E-Mail-Bestands sei nicht erforderlich gewesen. Zudem seien er und sein Rechtsanwalt an der Durchsicht der E-Mails zu beteiligen.
Das BVerfG hat die zulässige Verfassungsbeschwerde zur Entscheidung angenommen.

FÖR-Pragmatik: Zulässigkeit der Verfassungsbeschwerde
In diesem CyLaw-Report wird die Zulässigkeit der Verfassungsbeschwerde unterstellt und deswegen mit der Begründetheitsprüfung fortgeschritten.

Teil 2: Verfassungsmäßigkeit der Ermächtigungsgrundlage zur Beschlagnahme (abstrakt)

Die Verfassungsbeschwerde ist begründet, wenn B durch die von ihm angegriffenen gerichtlichen Entscheidungen in seinen Grundrechten verletzt worden ist. Eine Grundrechtsverletzung liegt vor, wenn

- der Geltungsbereich eines Grundrechts des B eröffnet ist **(Recht - R)**,
- in den durch einen Akt öffentlicher Gewalt eingegriffen worden ist **(Eingriff - E)** und
- dieser Eingriff nicht gerechtfertigt ist **(Rechtfertigung - R)**.

FEX: Prüfungsreihenfolge:
Grundsätzlich ist zu differenzieren zwischen der Prüfung

- der Ermächtigungsgrundlage für den Zugriff auf beim Provider gespeicherte Mails (**abstrakte Betrachtung in Teil 2**) und
- der Rechtmäßigkeit der konkreten Durchführung des Zugriffs auf die ca. 2500 E-Mails des B **(konkrete Betrachtung in Teil 3**).

A. Eröffnung des Geltungsbereichs von Grundrechten - (R)

I. Fernmeldegeheimnis (Art. 10 Abs. 1 GG) - Recht

Der Geltungsbereich des Grundrechts auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG könnte eröffnet sein.

BVerfG:

„Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs […]. 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 […], auch auf Kommunikationsdienste des Internet […].“[31] „Der Schutz des Fernmeldegeheimnisses umfasst in erster Linie den Kommunikationsinhalt […], sei er privater, geschäftlicher, politischer oder sonstiger Natur […]. Daneben sind die Kommunikationsumstände vor Kenntnisnahme geschützt […]“.[32]

In ihren Stellungnahmen zu der Verfassungsbeschwerde des B haben die Niedersächsische Landesregierung, der Bundesgerichtshof, der Generalbundesanwalt und das Bundesjustizministerium die Eröffnung des Geltungsbereichs von Art. 10 Abs. 1 GG mit der Begründung verneint, **der von Art. 10 Abs. 1 GG geschützte Kommunikationsvorgang sei mit Eingang der E-Mail auf dem Mailserver des Providers beendet**. Die E-Mail sei dann in den Herrschaftsbereich ihres Adressaten gelangt.[33] Diese Auffassung wird grundsätzlich vom BVerfG bestätigt, das mit der Ankunft (Kenntnisnahme?) der E-Mail beim Betroffenen den Weiterbestand der Eröffnung des Geltungsbereichs verneint.

BVerfG:

„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** […].“[34]

In einer teleologischen Auslegung konturiert das BVerfG den Geltungsbereich des Art. 10 Abs. 1 GG durch das Kriterium der Beherrschbarkeit der Inhalte. Das BVerfG ordnet die auf dem Mailserver des Providers gespeicherten E-Mails, die der Nutzer nur durch Herstellung einer Internetverbindung zum Mailserver des Providers abrufen kann, dem Herrschaftsbereich des Providers zu. Die besondere Schutzbedürftigkeit des Nutzers B sei gerade durch den Mangel an technischen Möglichkeiten, die Weitergabe der E-Mails durch den Provider an die Ermittlungsbehörden zu verhindern, begründet.

BVerfG:

„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 […]. 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 […]. **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

[31] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 43.
[32] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 44.
[33] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 32,f
[34] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 45.

Nutzer kann sie für sich auf einem Bildschirm nur lesbar machen, indem 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."[35]

Der Eröffnung des Geltungsbereichs des Art. 10 Abs. 1 GG stünde auch nicht entgegen, dass in den Phasen, in denen die E-Mails lediglich auf dem Mailserver des Providers abgespeichert sind, ohne dass sie gerade vom Nutzer abgerufen werden, kein dynamischer Telekommunikationsvorgang entsprechend der Definition nach § 3 Nr. 22 TKG stattfindet.

§ 3 TKG [Begriffsbestimmungen]

Im Sinne dieses Gesetzes ist oder sind

[…]

22.„Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen

[…]

BVerfG:

„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 […]."[36]

Unter Berufung auf die Normenhierarchie betont das BVerfG, dass sich das verfassungsrechtlich geschützte Fernmeldegeheimnis vom einfachgesetzlich geschützten Vorgang der Telekommunikation unterscheidet (§ 3 Nr. 22 TKG). Das BVerfG sieht den Geltungsbereich des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG als eröffnet an.

[35] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 46.
[36] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 47.

II. Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art.1 Abs. 1 GG)

Das Recht auf informationelle Selbstbestimmung, das vom BVerfG im Volkszählungsurteil[37] als besondere Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt worden ist, wird vorliegend von Art. 10 Abs. 1 GG als so genannter lex specialis verdrängt.

BVerfG:

„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 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 […].** 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.“[38]

FÖR-Hintergrund und Kritik:

Nicht verschwiegen werden soll für Interessierte (FINT), dass das BVerfG dogmatisch inkonsequent weiterprüft. Es ist nach FÖR-Ansicht nicht überzeugend zu begründen, wieso bei einer Spezialität von Art. 10 GG in der weiteren Prüfung bei der Rechtfertigung doch wieder die Schranken von Art. 2 Abs. 1 GG geprüft werden sollen.

BVerfG:

„[…] 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>).“[39]

Die Kritik, dass auf der einen Seite filigrane Grundrechtsabgrenzungen getroffen werden, im Ergebnis aber im Wesentlichen der gleiche Prüfungsmaßstab zugrundegelegt wird – nämlich Kernbereichsschutz und Verhältnismäßigkeitsgrundsatz – wird auch andernorts erhoben.[40]

III. Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)

Bezüglich des Zugriffs auf die E-Mails beim Provider, wird die Eröffnung des Geltungsbereichs der Unverletzlichkeit der Wohnung vom BVerfG verneint. Der Zugriff auf die E-Mails habe in den Räumlichkeiten des Providers stattgefunden, so dass eine Verletzung des Be-

[37] BVerfGE 65, S. 1 ff.
[38] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 49.
[39] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 60.
[40] Härting: „Beschlagnahme und Archivierung von Mails“, in: CR 2009, 581, 583.

schwerdeführers in seinem Grundrecht aus Art. 13 Abs. 1 GG ausscheide. Zudem stelle der Zugriff auf die E-Mails eine eigene, nicht mehr dem Geltungsbereich von Art. 13 Abs.1 GG unterfallende Maßnahme dar, auch wenn sie aus einer vorausgehenden Wohnungsdurchsuchung resultiere.

BVerfG:
„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 […]. 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 […] und - sofern Daten betroffen sind - am Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG […] zu messen."[41]

IV. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Recht auf IT-Sicherheit") (Art. 2 Abs.1 i.V.m. 1 Abs. 1 GG)

Im Rahmen seiner Entscheidung zu der Online-Durchsuchung auf Grundlage des nordrhein-westfälischen Verfassungsschutzgesetzes hat das BVerfG als weiteren Ausfluss des allgemeinen Persönlichkeitsrechts das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anerkannt.[42] Wie schon das Recht auf informationelle Selbstbestimmung wird das „Recht auf IT-Sicherheit" (siehe CyLaw-Report XXI) durch den spezielleren Art. 10 Abs. 1 GG verdrängt.

BVerfG:

„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** […]."[43]

[41] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 50.
[42] CyLaw-Report XXI: "Verdeckte Online-Durchsuchungen - zur IT-(Un)Sicherheit in Deutschland (06/2008/Version 3.0)" (26.06.2008).
[43] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 51.

B. Eingriff – (E)

Die richterliche Anordnung des Zugriffs auf die auf dem Mailserver des Providers gespeicherten E-Mails stellt einen Eingriff in das Grundrecht des B aus Art. 10 Abs. 1 GG dar.

BVerfG: „**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** […].“[44]

Der Eingriff scheidet auch nicht wegen einer Einwilligung des B in den Zugriff auf seine E-Mails aus.

BVerfG:

„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 […]. **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 Kommunikationsinhalte zugegriffen wird […].[45]

C. Rechtfertigung – (R)

I. Spezielle Schranke: einfacher Gesetzesvorbehalt (Art. 10 Abs. 2 S. 1 GG)

Nach Art. 10 Abs. 2 S. 1 GG darf in das Fernmeldegeheimnis aufgrund **eines Gesetzes** eingegriffen werden. Fraglich ist, aufgrund welchen Gesetzes der Zugriff auf die E-Mails des B bei seinem Provider erfolgen konnte.

1. In Betracht kommende gesetzliche Grundlagen: Beschlagnahme (§§ 94 ff. StPO, Postbeschlagnahme (§§ 99, 100 StPO) und Telekommunikationsüberwachung (§§ 100a, b StPO)

Hinsichtlich der Frage nach der Rechtsgrundlage für den beschriebenen Zugriff auf beim Provider gespeicherte E-Mails wird die Anwendung folgender Normen – mit unterschiedlichen Tatbestandsvoraussetzungen beziehungsweise Verfahrensanforderungen - in Literatur und Rechtsprechung diskutiert:

[44] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 54.
[45] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 53.

- die Vorschriften über Sicherstellung und Beschlagnahme (§§ 94 ff. StPO)
- gesetzlichen Regelungen zur Postbeschlagnahme (§§ 99, 100 StPO analog).
- die Bestimmungen zur Überwachung der Telekommunikation (§§ 100a, b StPO).

FÖR- Wiederholung:
Hierbei kann der Vorgang der Übertragung einer E-Mail in vier Phasen unterteilt werden[46]:
- Phase 1: die Übertragung der E-Mails vom Absender auf den Mailserver des Providers,
- Phase 2: die Phase des „Ruhens" der E-Mails auf dem Mailserver des Providers nach ihrer dortigen Zwischenspeicherung (Zwischenspeicherung),
- Phase 3: der Abruf- beziehungsweise Lesevorgang durch den Empfänger mittels Herstellung einer Internetverbindung zum Mailserver des Providers,
- Phase 4: die Aufbewahrung der (gelesenen) E-Mails auf dem Mailserver des Providers (Endspeicherung).

Für den Fall des strafprozessualen Zugriffs auf die E-Mails in den Phasen 1 und 3 wird § 100a StPO nach der Kommentarliteratur als Rechtsgrundlage angewandt[47], da der Zugriff dann in einer Maßnahme der Überwachung oder Aufzeichnung der laufenden Telekommunikation im Sinne des § 3 Nr. 22 TKG besteht. Für die Zugriffe in den Phasen 2 und 4, die Zeiträume also, in denen die E-Mails auf dem Mailserver des Providers vor und nach Kenntnisnahme des B „ruhen", war die Frage nach der anzuwendenden Rechtsgrundlage umstritten.

a) Postbeschlagnahme (§§ 99, 100 StPO (analog?))

In einer Entscheidung[48] vertritt der Bundesgerichtshof (BGH) die Auffassung, dass der Zugriff auf die beim Provider abgespeicherten E-Mails in diesen Phasen den gesetzlichen Regeln über die Postbeschlagnahme (§§ 99, 100 StPO) unterliegt.[49]

---

[46] Schlegel: "Beschlagnahme" vom E-Mail-Verkehr beim Provider, in: HRRS Februar 2007, S.44, 47 (letzter Abruf: 27.11.2009); Störing: Anmerkung zu LG Hamburg, Beschluss vom 08.01.2008, Az. 619 Qs 1/08 in MMR 2008, S. 186, 188.

[47] Nack, in: Karlsruher Kommentar zur StPO, 6. Auflage 2008, Rn. 21.

[48] BGH, Beschluss vom 31.03.2009, Az.: 1 StR 76/09.

[49] FINT (Für Interessierte): Nicht ganz eindeutig ist, ob der BGH von einer analogen Anwendung („entsprechend") oder einer teleologischen Auslegung (E-Mails als elektronische Post) ausgeht.

FEX: Analogie
Die analoge Anwendung von Rechtsnormen dient der Ausfüllung von Gesetzeslücken. Sie kommt dann in Betracht, wenn
eine planwidrige Regelungslücke vorliegt und
eine vergleichbare Interessenlage zwischen dem gesetzlich geregelten und dem gesetzlich nicht geregeltem Fall besteht.
Voraussetzung ist also, dass der Norminterpret zunächst alle Auslegungsmethoden anwendet – insbesondere die teleologische Auslegung. Erst wenn der Norminterpret offen verzichtet, bestehendes Recht auszulegen, darf er sich der Analogie – und damit der Normsetzung durch Interpretation – bedienen. Die Analogie ist also ein dogmatisches Instrument, um die Verschiebung von Rechtssetzungsmacht (Unterlassen des Gesetzgebers) auf den Interpreten zu begründen

Das LG Ravensburg (Beschluss vom 09.12.2002 Az. 2 Qs 153/02) ging ausdrücklich von einer Analogie aus.

§ 99 StPO [Postbeschlagnahme]

Zulässig ist die Beschlagnahme **der an den Beschuldigten gerichteten Postsendungen und Telegramme**, die sich im Gewahrsam von Personen oder Unternehmen befinden, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder daran mitwirken. Ebenso ist eine Beschlagnahme von Postsendungen und Telegrammen zulässig, bei denen aus vorliegenden Tatsachen zu schließen ist, dass sie von dem Beschuldigten herrühren oder für ihn bestimmt sind und dass ihr Inhalt für die Untersuchung Bedeutung hat.

§ 100 StPO [Zuständigkeit][50]

(1) Zu der Beschlagnahme (§ 99) ist **nur der Richter, bei Gefahr im Verzug auch die Staatsanwaltschaft** befugt.

[…]

(3) Die Öffnung der ausgelieferten Gegenstände steht dem Richter zu. Er kann diese Befugnis der Staatsanwaltschaft übertragen, soweit dies erforderlich ist, um den Untersuchungserfolg nicht durch Verzögerung zu gefährden. Die Übertragung ist nicht anfechtbar; sie kann jederzeit widerrufen werden. Solange eine Anordnung nach Satz 2 nicht ergangen ist, legt die Staatsanwaltschaft die ihr ausgelieferten Gegenstände sofort, und zwar verschlossene Postsendungen ungeöffnet, dem Richter vor.

(4) Über eine von der Staatsanwaltschaft verfügte Beschlagnahme entscheidet der nach § 98 zuständige Richter. Über die Öffnung eines ausgelieferten Gegenstandes entscheidet der Richter, der die Beschlagnahme angeordnet oder bestätigt hat.

BGH:

„Jedoch bedurfte es für die im Postfach beim E-Mail-Provider abgespeicherten E-Mails, ob bereits gelesen oder noch ungelesen, **auch nicht der Voraussetzungen des § 100a StPO, denn während der möglicherweise auch nur Sekundenbruchteile andauernden Speicherung in der Datenbank des MailProviders ist kein Telekommunikationsvorgang (mehr) gegeben**. […] Vielmehr ist die Beschlagnahme von E-Mails bei einem E-Mail-Provider, welche dort bis zu einem ersten oder weiteren Aufruf abgespeichert sind, auch unter Berücksichtigung des heutigen Kommunikationsverhaltens in jeder Hinsicht vergleichbar mit der Beschlagnahme anderer Mitteilungen, welche sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdiensteleister befinden, bspw. von Telegrammen, welche gleichfalls auf dem Telekommunikationsweg dorthin übermittelt wurden. Daher können **beim Provider gespeicherte, eingegangene oder zwischengespeicherte, E-Mails -** auch ohne spezifische gesetzliche Regelung **- jedenfalls unter den Voraussetzungen des § 99 StPO beschlagnahmt werden**."[51]

Demnach würde in einer Parallelbetrachtung, die elektronische wie die Realworld-Mail behandelt (teleologische Auslegung). Bei der Anwendung der Postbeschlagnahmevorschriften sind drei Erkenntnisse hervorzuheben:

[50] § 100 StPO in der vom 01.01.2000 bis 31.12.2007 geltenden Fassung.
[51] BGH, Beschluss vom 31.03.2009, Az.: 1 StR 76/09, S.3.

- Nur an den Beschuldigten einer Straftat gerichtete „Post“ darf beschlagnahmt werden. Bei B handelt es sich aber gerade nicht um einen Beschuldigten, sondern um einen Dritten, bei dem man nur Informationen über Verdächtige vermutet. § 99 StPO analog **könnte also keine Ermächtigungsgrundlage darstellen.**
- Voraussetzung ist grundsätzlich die Anordnung eines Richters.
- Nicht erforderlich ist, dass die Verfolgung einer schweren Straftat, einer sogenannten Katalogstraftat, bezweckt wird. § 99 StPO steht für die Verfolgung jeder Straftat zur Verfügung.

b) Telekommunikationsüberwachung (§§ 100a, 100b StPO)

Demgegenüber will etwa das Landgericht (LG) Hamburg in einer Entscheidung aus 2008[52] den strafprozessualen Zugriff auf die beim Provider gespeicherten E-Mails in den Phasen ihrer Zwischen- und Endspeicherung (Phasen 2 und 4) an den §§ 100a, b StPO messen. Das LG Hamburg begründet die Anwendung des § 100a StPO mit dem Geltungsbereich des Fernmeldegeheimnisses (Art. 10 GG), in den auch die Phasen der Zwischenspeicherung auf dem Mailserver vor Kenntnisnahme der E-Mails und der endgültigen (dortigen) Abspeicherung nach Kenntnisnahme fielen.

LG Hamburg:

„Das verfassungsrechtlich geschützte Fernmeldegeheimnis, das auch in Art. 8 Abs. 1 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) seinen Niederschlag gefunden hat, soll die vertrauliche Nutzung des Kommunikationsmediums gewährleisten […] und vermeiden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt anders verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Erkenntnisse über die Kommunikationsbeziehungen oder –inhalte gewinnen [...].

Dieses Bedürfnis, freie Kommunikation zu gewährleisten, besteht auch dann, wenn sich ein Kommunikationsteilnehmer der E-Mail-Kommunikation unter Einsatz von serverbasierten E-Mail-Postfächern bedient. In diesem Fall begibt er sich seiner alleinigen Herrschaftsbefugnis über die elektronischen Daten; insbesondere der E-Mail-Provider und damit auch die Ermittlungsbehörden sind in der Lage, auf diese Daten beliebig und jederzeit zuzugreifen. Dieser Mangel an Beherrschbarkeit unterscheidet den Nutzer eines servergestützten E-Mail-Postfachs auch von demjenigen, der die Nachrichten vom Server abruft und auf seinen eigenen Computer gelangen lässt. Jedenfalls dann unterstehen die Daten nur noch seinem alleinigen Gewahrsam, so dass jedenfalls der Schutzbereich von Art. 10 Abs. 1 GG nicht mehr eröffnet ist.

[…]

Im Übrigen kommt es für diese (verfassungs-)rechtliche Betrachtung auch nicht darauf an, ob der Nutzer die in seinem Postfach lagernden E-Mails nur zwischengespeichert, oder – nach Kenntnisnahme – endgültig abgespeichert hat. In beiden Fällen ist der Nutzer gleichermaßen schutzbedürftig, weil jeweils keine Änderung der Gewahrsams- und Herrschaftsverhältnisse an den physisch beim Provider befindlichen Daten erfolgt. Es ist zudem für Dritte (Provider oder Ermittlungsbehörden) nicht möglich zu erkennen, ob die von dem Zugriff betroffene E-Mail nur zwischen- oder endgültig abgespeichert ist. Eine solche, an

[52] LG Hamburg, Beschluss vom 08.01.2008, Az.: 619 Qs 1/08.

Zufälligkeiten orientierte Bewertung ließe außer Betracht, dass es nicht auf den (subjektiven) Bestimmungszweck der Nachrichten, sondern auf ihre – in beiden Fällen für den Nutzer nur unvollkommene – Beherrschbarkeit ankommt."[53]

Aus Sicht des LG Hamburg können nur §§ 100a, 100b StPO den verfassungsrechtlichen Anforderungen, die das Fernmeldegeheimnis an einen Zugriff auf die beim Provider abgespeicherten E-Mails stellt, genügen.

LG Hamburg:

„Hinsichtlich des ermittlungsbehördlichen Zugriffs auf die bei einem Provider in einem Server-Postfach gespeicherten E-Mails kommen aufgrund der vorgenannten Erwägungen allein die §§ 100a, 100b StPO als gesetzliche, den verfassungsrechtlichen Anforderungen genügende Eingriffsgrundlage in Betracht […]. Die bloße Anwendung der Beschlagnahmevorschriften nach näherer Maßgabe der §§ 94, 98, 99 StPO […] würde die spezifischen, oben aufgezeigten Anforderungen, die der staatliche Zugriff auf E-Mail-Kommunikation voraussetzt, unterlaufen. Einerseits sind die Eingriffsvoraussetzungen dieser Normen vergleichsweise gering (vgl. dagegen die Beschränkung der Telekommunikationsüberwachung auf "schwere Straftaten", § 100a Abs. 1 Nr. 1 und Abs. 2 StPO), andererseits tragen sie den Besonderheiten dieser Kommunikationsform – insb. dem Schutz des Kernbereichs privater Lebensgestaltung (vgl. § 100a Abs. 4 StPO) – nicht hinreichend Rechnung."[54]

Hervorzuheben bei der Anwendung von Bestimmungen über die Telekommunikationsüberwachung sind drei Erkenntnisse:

- **Die Zugrundelegung von § 100a, b StPO hätten den „logischen Charme", dass zwischen den Phasen 1 und 4 nicht mehr differenziert werden müsste. Insbesondere im Lichte der Aussage des BVerfG, dass es sich in allen Phasen um Telekommunikation im Sinne von Art. 10 Abs. 1 GG handele (siehe oben unter A.I.) wäre der Zeitpunkt des Zugriffs für die Zugriffsvoraussetzungen nicht mehr bestimmend.**
- Voraussetzung ist grundsätzlich die Anordnung eines Richters.
- Erforderlich ist die Verfolgung einer schweren Straftat, einer sogenannten Katalogstraftat. An dieser fehlt es bei dem zum Zeit der Entscheidung geltenden Recht, weil der Betrug und die Untreue damals (2006) noch nicht zu den Katalogstraftaten zählten.

FÖR-Kritik: Logik der Argumentation des BVerfG?
Warum sollen Eingriffe in Phase 1 und 3 unter erschwerten Bedingungen (§§ 100a, b StPO) rechtmäßig sein; Eingriffe in Phase 2 und 4 unter erleichterten Bedingungen, wenn es sich doch bei allen vier Phasen um in Art. 10 Abs. 1 GG geschützte Telekommunikation handeln soll. **Das BVerfG etabliert für die Phasen 2 und 4 ein Fernmeldegeheimnis zweiter**

[53] LG Hamburg, Beschluss vom 08.01.2008, Az.: 619 Qs 1/08, 2.a).
[54] LG Hamburg, Beschluss vom 08.01.2008, Az.: 619 Qs 1/08, 2.b).

Klasse.[55] Hervorzuheben ist, dass das BVerfG hierzu keine Ausführungen macht – insbesondere weder zum Rechtsprechungsansatz §§ 100a, b StPO noch zu § 99 StPO erklärt, warum es anderer Meinung ist.

BVerfG:
„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."[56]

Das BVerfG beschränkt sich darauf, eine systematische einfachgesetzliche Auslegung (§§ 100a, b, g StPO) bei einfachgesetzlichen Eingriffen in das Fernmeldegeheimnis abzulehnen (siehe unter c).

c) Sicherstellung und Beschlagnahme (§§ 94ff. StPO)

Das BVerfG zieht die Vorschriften über Sicherstellung und Beschlagnahme als Rechtsgrundlage für den strafprozessualen Zugriff auf die beim Provider gespeicherten E-Mails heran.

BVerfG:

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

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."[57]

Hervorzuheben ist, dass damit beim Provider gespeicherte Mails wie sonstige Gegenstände beschlagnahmt werden dürfen. Grundsätzlich ist zwar eine richterliche Anordnung erforderlich; die Beschlagnahme darf aber auch gegenüber Dritten und zur Verfolgung jeder Straftat erfolgen. Das BVerfG wendet sich ausdrücklich gegen eine systematische Auslegung, die der Telekommunikationsüberwachung (§§ 100a, b StPO – Inhaltsüberwachung)) und der Auskunft über Telekommunikationsverkehrsdaten (§ 100g StPO) einen Grundsatz dergestalt entnimmt, dass der Zweck der „Datenorganisation" grundsätzlich die Verfolgung (eines Ver-

[55] Vgl. auch die Anmerkung von Krüger zu BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, in: MMR 2008, S. 673, 680ff, zum „Schutz des Fernmeldegeheimnisses zweiter Klasse" (S. 683); so auch Härting, in: CR 2009, S. 581, 583, zum „Fernmeldegeheimnis light".
[56] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 58.
[57] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 55f.

dächtigen) einer Katalogstraftat bzw. einer mittels Telekommunikation begangenen Straftat sein müsse.

§ 100g StPO [Erhebung von Verkehrsdaten]

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1.eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2.eine Straftat mittels Telekommunikation begangen hat,

so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. […]

BVerfG:

„§ 94 StPO kann ohne Verfassungsverstoß als Ermächtigung auch zu Eingriffen in Art. 10 Abs. 1 GG verstanden werden […]. **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, 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**.“[58]

Zusammenfassend ist festzuhalten, dass das BVerfG eine bisher in der Rechtsprechung nicht mehrheitlich vertretene Auffassung etabliert hat. Im Folgenden muss es im Rahmen der

[58] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 57.

materiellen Rechtmäßigkeit von § 94 ff StPO aber noch prüfen, inwieweit diese Ermächtigungsgrundlagen mit weiteren verfassungsrechtlichen Prinzipien vereinbar sind.
Zu diesen Prinzipien gehören

- zum einen der aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG)[59] abgeleitete Grundsatz der Normenklarheit und Normenbestimmtheit;

Art. 20 Abs. 3 GG

(3) Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.

- des Weiteren als Unterfall dieses Prinzips im Kontext des Einsatzes von Informationstechnologien der „Schutz eines Kernbereichs privater Lebensgestaltung“ und
- zum Dritten die Einhaltung des Zitiergebots (Art. 19 Abs. 1 S. 2 GG)

2. Normenklarheit und Normenbestimmtheit der Beschlagnahmevorschriften (§§ 94ff. StPO) – „Verwendungszweck“

Der unter anderem aus dem Rechtsstaatsprinzip abgeleitete Grundsatz der Normenklarheit und Normenbestimmtheit hat nicht zu überschätzende Bedeutung für das Cyberlaw: so hat der 1. Senat das BVerfG seine Online-Durchsuchungsentscheidung maßgeblich auf die Verletzung dieses Grundsatzes gestützt (CyLaw-Report XXI – Entscheidung des 1. Senats). Von umso größerem Interesse ist, wie der 2. und andere Senat mit der Klarheit und Bestimmtheit informationstechnologischer Surveillancenormen umgeht. Das Besondere an dieser Entscheidung ist, dass der 2. Senat Normen des traditional law informationstechnologisch auslegt – Realworldnormen also auf die Informationstechnologie mittels Auslegung erstreckt. Grundsätzlich verlangt der 2. Senat auch hierfür die Beachtung der Gebote von Normenklarheit und Normenbestimmtheit.

BVerfG:

„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** […].“[60]

Nachdem das BVerfG in seiner Entscheidung zum strafprozessualen Zugriff auf elektronische Datenbestände bei Berufsgeheimnisträgern die §§ 94 ff. StPO für hinreichend klar und bestimmt befand[61], bejaht es die Normenklarheit und –bestimmtheit dieser Vorschriften nun auch hinsichtlich des strafprozessualen Zugriffs auf E-Mails auf dem Mailserver des Provi-

[59] FEX: Die Ableitung dieser Grundsätze ist strittig; das BVerfG scheint sie auch aus den Grundrechten selbst – etwa dem Grundrecht auf informationelle Selbstbestimmung – abzuleiten (vgl. BVerfG a.a.O. Rn. 60).

[60] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 60.

[61] BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 97 ff; vgl. hierzu: CyLaw-Report IX: "Strafprozessualer Zugriff auf Datenbestände" (10.05.2006)

ders. An seine Rechtsprechung zum Zugriff auf Datenbestände bei Berufsgeheimnisträgern[62] anknüpfend hält das BVerfG als für den Bürger hinreichend erkennbar, dass die in den E-Mails enthaltenen Daten unter den Begriff des „Gegenstandes" gemäß § 94 Abs. 1 StPO fallen und fasst die gesetzliche Formulierung „als Beweismittel von Bedeutung sein können" nicht als zu vage auf.

BVerfG:

„**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**. 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 […]. **§ 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** […]."[63]

FÖR-Kritik: „**Nutzerhorizont" als Klar- und Bestimmtheitsmaßstab**
Anzumerken ist, dass jedenfalls den Richtern beim Bundesgerichtshof und etwa bei den Landgerichten Hanau, Mannheim und Hamburg[64] nicht erkennbar war, dass § 94 StPO die rechtmäßige Ermächtigungsgrundlage war.

Darüber hinaus legt der 2. Senat „Gegenstände" sehr weit aus und verzichtet auf eine analoge Anwendung. Jedenfalls nach Ansicht des 2. Senats erfüllen §§ 94ff. StPO das weitere Bestimmtheitskriterium, dass der Verwendungszweck der erhobenen Daten vom Gesetzgeber bereichsspezifisch und präzise benannt sein muss.

BVerfG:

„Die allgemeinen strafprozessualen Sicherstellungs- und Beschlagnahmeregelungen 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 [...] ."[65]

[62] BVerfG, Beschluss vom 12.04.2005, Az.: 2 BvR 1027/02, Rn. 99ff.
[63] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 62f.
[64] LG Hanau, Beschluss vom 23.09.1999, Az. 3 Qs 149/99; LG Mannheim, Beschluss vom 30.11.2001, Az.: 22 KLs 628 Js 15705/00; LG Hamburg, Beschluss vom 08.01.2008, Az.: 619 Qs 1/08.
[65] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 64.

3. Normenklarheit und Normenbestimmtheit der Beschlagnahmevorschriften (§§ 94ff. StPO) – Schutz des absolut geschützten Kernbereichs privater Lebensgestaltung (Art. 79 Abs. 3 i.V.m. Art. 1 Abs. 1 GG)

Es ist eine vom BVerfG postulierte Selbstverständlichkeit, dass bei (informationstechnologischer) Surveillance ein absolut geschützter Kernbereich privater Lebensgestaltung „tabu“ ist (Entscheidungen zur Online-Durchsuchung wie zur akustischen Wohnraumüberwachung (CyLaw-Reports XVI, XXI). Der Gesetzgeber hat diesen Schutzauftrag etwa bei der Telekommunikationsüberwachung wie bei der akustischen Wohnraumüberwachung im Wortlaut der Norm umgesetzt:

§ 100a Abs. 4 StPO

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

§100c Abs. 4 StPO

(4) Die Maßnahme darf nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Gespräche in Betriebs- oder Geschäftsräumen sind in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen. Das Gleiche gilt für Gespräche über begangene Straftaten und Äußerungen, mittels derer Straftaten begangen werden.

Auch beim Zugriff auf beim Provider gespeicherte E-Mails besteht die Gefahr des Eingriffs und der Verletzung des Kernbereichs privater Lebensgestaltung. Eine Verletzung droht, wenn eine Erhebung und Speicherung kernbereichsbezogener Daten erfolgt bzw. nach der Speicherung nicht unverzüglich gelöscht wird:

BVerfG:

„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 Sphäre anderer oder Belange der Gemeinschaft berührt […]. Maßgebend sind die Besonderheiten des jeweiligen Einzelfalls […]. 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 […]. 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 […]. 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 […]."[66]

Hervorzuheben ist, dass der 2. Senat des BVerfG bei § 94 ff StPO auf eine ausdrückliche Verankerung des Kernbereichsschutzes im Gesetz (grammatische Auslegung) verzichtet – im Gegensatz zu § 100a und c Abs. 4 StPO. Das Gericht begnügt sich mit der Kenntnis des Richters (der Juristen) im konkreten Einzelfall.

FÖR-Kritik: Kein grammatisch verankerter Schutz des Kernbereichs privater Lebensgestaltung bei auf § 94 ff StPO gestützten E-Mail-Beschlagnahmen
Das BVerfG vertraut dem „Domänenwissen" der Juristen und Strafverfolger, die ein verfassungsrechtliches essentiale „ungeschrieben" in die Ermittlungsmaßnahmen integrieren sollen. Es bleibt der Zukunft vorbehalten, inwieweit im konkreten Fall Ermittlungsrichter tatsächlich die Beschlagnahmeanordnungen insoweit differenziert ausformulieren.

4. Zitiergebot (Art. 19 Abs. 1 S. 2 GG)

Das Zitiergebot besagt, dass das förmliche Gesetz, das ein Grundrecht einschränkt oder hierzu ermächtigt, dieses Grundrecht ausdrücklich benennen muss.

Art. 19 GG [Einschränkung von Grundrechten; Grundrechtsträger; Rechtsschutz]

(1) Soweit nach diesem Grundgesetz ein Grundrecht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden kann, muss das Gesetz allgemein und nicht nur für den Einzelfall gelten. **Außerdem muss das Gesetz das Grundrecht unter Angabe des Artikels nennen.** […]

Es gilt zumindest[67] für solche Grundrechte, die nach der Formulierung ihres Gesetzesvorbehalts im Grundgesetz „durch oder aufgrund eines Gesetzes eingeschränkt werden" können, wozu auch das Fernmeldegeheimnis zählt, das „aufgrund eines Gesetzes" (Art. 10 Abs. 2 S. 1 GG) eingeschränkt werden kann. Allerdings wird das verfassungsrechtliche Zitiergebot nicht auf vorkonstitutionelle Gesetze angewandt, die bereits **vor Inkrafttreten des Grundgesetzes** entstanden sind[68]. Grund dafür ist, dass der vorkonstitutionelle Gesetzgeber Art. 19 Abs. 1 S. 2 GG nicht kennen konnte. Daher ist es für das BVerfG unschädlich, dass die vorkonstitutionellen Bestimmungen der §§ 94 ff. StPO als Rechtgrundlage für einen in das Fernmeldegeheimnis eingreifenden Zugriff auf E-Mails das Fernmeldegeheimnis nicht zitieren.

[66] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 90.
[67] zur Diskussion, ob das Zitiergebot nur für solche Grundrechte gilt, die nach der Formulierung ihres Gesetzesvorbehalts „durch oder aufgrund eines Gesetzes eingeschränkt" werden können: Remmert, in: Maunz/Dürig, Grundgesetz, 53. Auflage 2009, Rn. 53f..
[68] BVerfGE Band 2, S. 121, 122f..

FÖR-Kritik: BVerfG verkennt Bedeutung des § 88 Abs. 3 S. 3 Telekommunikationsgesetz (TKG)

Die Rechtsprechungs-"Lösung", dass es „Telekommunikation" im verfassungsrechtlichen Sinne" gäbe, die nicht zugleich „Telekommunikation im einfachgesetzlichen Sinne" sei, führt dazu, **dass eine zentrale Schutzvorschrift für das Fernmeldegeheimnis vom BVerfG umgangen wird.** Es handelt sich um § 88 Abs. 3 TKG:

§ 88 Abs. 3 TKG:
(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, **soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht**. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Nach der amtlichen Begründung (historische Auslegung) muss in einer gesetzlichen Befugnisnom zur Durchbrechung des Fernmeldegeheimnisses entweder im Wortlaut oder bei den Beratungen zum Ausdruck kommen, dass ein vorrangiges Rechtfertigungsrechtsgut gefunden wurde:

Bundestagsdrucksache 13/3609 vom 30.01.1996, S. 53:
[…] Das Fernmeldegeheimnis tritt nur dann zurück, wenn sich die Befugnisnorm ausdrücklich auf Telekommunikationsvorgänge bezieht. **Dies heißt, die Befugnisnorm für den Eingriff muss so gestaltet sein, dass der Wille des Gesetzgebers, das Fernmeldegeheimnis zurücktreten zu lassen, deutlich wird.** […] Ausgegrenzt werden sollen jedoch solche Normen, die Auskunftspflichten in allgemeiner Form regeln, ohne besonders auf Telekommunikationsvorgänge Bezug zu nehmen. Hierdurch wird gewährleistet, dass diese Ausnahmen vom Fernmeldegeheimnis auf einer bewussten Abwägung des Gesetzgebers beruhen und als solche deutlich erkennbar sind.

Diese spezialgesetzliche Ausformung des Art. 19 Abs. 2 GG wird vom BVerfG ignoriert. §§ 94, 95 StPO wurden vom Gesetzgeber nie in Hinblick auf Art. 10 GG geschaffen.[69] Und nach hier vertretener Ansicht kann die „Auslegung" des BVerfG in Hinblick auf § 88 Abs. 3 TKG nur als **ultra vires** kritisiert werden. Vor dem Hintergrund von § 88 Abs. 3 TKG waren die §§ 94, 95 ff StPO gar nicht auslegungsfähig, wenn man – wie das BVerfG - Art. 10 GG zugrundelegt. Eingriffe in die Telekommunikation können nach der Verfassung nur durch den Gesetzgeber erfolgen (Art. 10 Abs. 2 GG), der eben nach § 88 Abs. 3 TKG nachvollziehbar abgewogen haben muss. Eine Rechtsprechung des 2. Senats, die die fehlende Entscheidung des Gesetzgebers durch eine ausufernde „Auslegung" ersetzt, ist als inkonsequent abzulehnen. Das BVerfG hat hier ein **Fernmeldegeheimnis zweiter Klasse** geschaffen – eines das nicht durch § 88 Abs. 3 TKG geschützt ist. Das spezielle Zitiererfordernis des § 88 Abs. 3 S.

[69] Siehe aber die Anmerkung zu einem Referentenentwurf, der dem Zitiergebot genügen wollte, bei Bock, in: Beck'scher TKG-Kommentar, 3. Auflage 2006, § 88 TKG, Rn. 52.

3 TKG sollte nach hier vertretener Ansicht eine Sperrwirkung gegenüber zukünftigen Einschränkungen des Fernmeldegeheimnisses haben – die nämlich nur durch den Gesetzgeber und nicht durch die Rechtsprechung erfolgen sollten. Dafür spricht auch, dass die oben wiedergegebene Gesetzesbegründung (historische Auslegung) ausdrücklich nur einen Ausnahmetatbestand nennt – nämlich § 138 StGB - der evident ohne Beachtung des Zitiergebots zur Einschränkung des Fernmeldegeheimnisses ermächtigt.

§ 138 StGB [Nichtanzeige geplanter Straftaten]
(1) Wer von dem Vorhaben oder der Ausführung
1.einer Vorbereitung eines Angriffskrieges (§ 80),
[…]
5.eines Mordes (§ 211) oder Totschlags (§ 212) oder eines Völkermordes (§ 6 des Völkerstrafgesetzbuches) oder eines Verbrechens gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches) oder eines Kriegsverbrechens (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches),
[…]
7.eines Raubes oder einer räuberischen Erpressung (§§ 249 bis 251 oder 255)
[…]
zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer
1.von der Ausführung einer Straftat nach § 89a oder
2.von dem Vorhaben oder der Ausführung einer Straftat nach § 129a, auch in Verbindung mit § 129b Abs. 1 Satz 1 und 2,
zu einer Zeit, zu der die Ausführung noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde unverzüglich Anzeige zu erstatten. 2§ 129b Abs. 1 Satz 3 bis 5 gilt im Fall der Nummer 2 entsprechend.
(3) Wer die Anzeige leichtfertig unterlässt, obwohl er von dem Vorhaben oder der Ausführung der rechtswidrigen Tat glaubhaft erfahren hat, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Festzuhalten bleibt nach FÖR-Ansicht: wenn man § 88 Abs. 3 TKG konsequent ignorieren will, dann bietet sich eher der Weg des VGH Kassel an (siehe unter Teil 5) – der Gang über Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

FÖR-Kritik: Wertungswiderspruch zu § 100 g StPO
Darüber hinaus ist die BVerfG-Entscheidung zu kritisieren, weil mit dieser Entscheidung ein informationsrechtlicher Wertungswiderspruch verbunden ist. Die in Hinblick auf den effektiv notwendigen Schutz wesentlich sensibleren **Inhaltsdaten** von Kommunikation können nunmehr unter leichteren Voraussetzungen „beschlagnahmt“ werden als die **Verkehrsdaten** (§ 100g StPO) – nämlich etwa beim Verdacht auch von Straftaten von verhältnismäßig geringer Schwere.

§100 g StPO [Erhebung von Verkehrsdaten]
(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1.eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder
2.eine Straftat mittels Telekommunikation begangen hat,
so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig. […]

Nicht nur in juristischer Perspektive ist ein Wertungswiderspruch zu attestieren, sondern auch in informationstechnologischer Perspektive. Die nach §§ 94, 95 StPO „beschlagnahmten“ E-Mails enthalten nämlich im Header Verkehrsdaten, die – eigentlich - nur unter den Voraussetzungen des § 100g StPO erhoben werden dürfen.

II. Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Schwere des Eingriffs in das Eingriffsrechtsgut darf nicht außer Verhältnis zur Qualität der Förderung des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

Damit die §§ 94 ff. StPO eine geeignete Rechtsgrundlage für den Zugriff auf die beim Provider gespeicherten E-Mails im strafrechtlichen Ermittlungsverfahren sind, müssen die Normen in Bezug auf einen solchen Eingriff in das Fernmeldegeheimnis verhältnismäßig sein.

1. Geeignetheit

Die wirksame Strafverfolgung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung stellen legitime Zwecke dar (Rechtfertigungsrechtsgut). Die Möglichkeit, durch eine Sicherstellung/Beschlagnahme auf der gesetzlichen Grundlage der §§ 94 ff. StPO auf die beim Provider gespeicherten E-Mails zuzugreifen ist, ist zur Förderung des Rechtfertigungsrechtsguts geeignet,[70] weil nicht ausgeschlossen ist, dass über Dritte Informationen

[70] vgl. BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 65.

über Kontenbewegungen hinsichtlich Beschuldigter erhalten werden. Ungeeignet wäre eine „Beschlagnahme“ nur dann, wenn keine Mails beim Provider gespeichert werden.

BVerfG:

„Wird festgestellt, dass sich auf dem Mailserver überhaupt keine verfahrenserheblichen E-Mail befinden können, wäre eine Sicherstellung schon ungeeignet.“ [71]

2. Erforderlichkeit

Bei einer „Beschlagnahme“ sind – wie bereits anfänglich geschildert – vier Verfahrensstadien zu unterscheiden. Im Rahmen der Erforderlichkeit enthält die BVerfG-Entscheidung Kriterien, wie in welchem Verfahrensstadium der minimal invasive Eingriff zu suchen ist (Auslegung der §§ 94 ff StPO durch das BVerfG).

a) Verfahrensschritt (1) – Durchsuchung der Wohnung des B

Hier enthalten weder die Verfassungsbeschwerde des B noch die Entscheidung Ausführungen. Evident wird zugrundegelegt, dass eine Wohnungsdurchsuchung auch bei einem nichtverdächtigen Dritten im Interesse einer effektiven Strafverfolgung erforderlich sein kann.

b) Verfahrensschritt (2) – „vorläufige Sicherstellung“

aa) Strafprozessrechtliches Prinzip der Datensparsamkeit

Von großer praktischer Bedeutung ist, ob die Behörden bei der vorläufigen Sicherstellung schon Daten ausfiltern müssen. Mit anderen Worten: ob sie also pauschal auf Datenobjekte zugreifen dürfen, oder schon beim ersten Kontakt mit den Datenobjekten sich selbst beschränken müssen. Zunächst verlangt das BVerfG, dass „im Rahmen des Vertretbaren“ für das Verfahren bedeutende und bedeutungslose Informationen getrennt werden müssten. Es begründet nach FÖR-Ansicht ein strafprozessrechtliches „Prinzip der Datensparsamkeit“:

BVerfG:

„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.**“[72]

[71] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06,Rn. 83.

[72] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 84. FEX: Das BVerfG bezieht sich in dieser Randnummer zwar wörtlich auf den „dauerhaften Zugriff“. Nach FÖR-Ansicht gilt das hier zum Ausdruck kommende verfassungs- und strafprozessrechtliche Prinzip der Datensparsamkeit bereits für die Sicherstellung in Verfahrensschritt (2) und nicht erst bei Verfahrensschritt (4).

FINT (Für Interessierte): Datenschutzrechtliches Prinzip der Datensparsamkeit (§ 3a BDSG)

§ 3a BDSG [Datenvermeidung und Datensparsamkeit]
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Die Entscheidung enthält darüber hinaus informationstechnologische Hinweise, wie die Minimalinvasivität des Eingriffs in der Praxis umgesetzt werden kann.

BVerfG:

„**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.“[73]

BVerfG:

„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, 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**.“[74]

bb) Datensparsamkeit steht vorläufiger Sicherstellung aller verfügbarer Datenobjekte nicht immer entgegen

BVerfG:

„**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.“[75]

[73] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 85.
[74] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 86.
[75] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 87,

Das BVerfG erlaubt also, dass unter bestimmten Umständen – praktische Erschwerung der Filterung bei der vorläufigen Sicherstellung – das Prinzip der Datensparsamkeit erst im Verfahrensschritt (3) – der Durchsicht – gewahrt wird.

c) Verfahrensschritt (3) – Durchsicht

§ 110 Abs. 1, 2 StPO in der seit 01.09.2004 geltenden Fassung [Durchsicht von Papieren und elektronischen Speichermedien]

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

(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.

FEX:
Mit Wirkung zum 01.01.2008 ist § 110 StPO um einen Absatz 3 erweitert worden. Mit der Regelung des § 110 Abs. 3 StPO als Sonderfall der Durchsicht von Papieren nach § 110 Abs. 1, 2 wird zudem klargestellt, dass auch elektronische Datenträger dem Papierbegriff der Absätze 1 und 2 unterfallen[76].

§ 110 StPO [Durchsicht von Papieren und elektronischen Speichermedien]
[…]
(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung 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.

Mit dieser Regelung, die zum Zeitpunkt der mit der Verfassungsbeschwerde angegriffenen richterlichen Beschlüsse noch nicht in Kraft war, sollen die Vorgaben aus Art. 19 Abs.2 der Konvention über Computerkriminalität (Convention on Cybercrime) des Europarats umgesetzt werden.

Artikel 19 Konvention über Computerkriminalität [Durchsuchung und Beschlagnahme gespeicherter Computerdaten]
(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,
a)ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und
b)einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,

[76] Schlegel: ""Online-Durchsuchung light" - Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung", in: HRRS Januar 2008, S. 23, 25 (letzter Abruf: 27.11.2009). FINT: Der Aufsatz enthält auch Ausführungen dazu, dass § 110 Abs. 3 StPO nicht – wie im vorliegenden Sachverhalt – den Zugriff auf beim Provider gespeicherte Daten rechtfertigt.

in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.
(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können. […]

§ 110 Abs. 3 StPO erlaubt den Ermittlungsbehörden, die Durchsicht eines elektronischen Speichermediums (beziehungsweise entsprechend der Konvention: Computersystem) von diesem aus auf ein räumlich getrenntes Speichermedium (Computersystem) auszudehnen.[77] Hierunter fallen seit der Geltung des **§ 110 Abs. 3** StPO mit der Ausgangskonstellation des Sachverhalts dieses CyLaw-Reports vergleichbare Situationen, in denen die Ermittlungsbehörden vom Rechner des Betroffenen aus eine Internetverbindung zum Mailserver seines Provider herstellen wollen, um eine Durchsicht der dort gespeicherten E-Mails des Betroffenen vorzunehmen. Ausdrücklich (grammatische Auslegung) ist die vorläufige Sicherstellung, die Durchsicht und die endgültige Beschlagnahme von (nicht auf abgegrenzten, körperlichen Datenträgern[78] organisierten) **Daten** in der StPO nicht geregelt. Auch die seit 1.1.2008 geltende Vorschrift des § 110 Abs. 3 StPO gilt nach FÖR- und Literaturansicht[79] für den Fall, dass von einem Computer auf das Netzwerk des Providers **konkret** nicht zugegriffen werden kann (weil das Passwort nicht gefunden wurde) nicht.

BVerfG:

Das Verfahrensstadium der Durchsicht gemäß § 110 StPO ist der endgültigen Entscheidung über den Umfang der Beschlagnahme vorgelagert […]. 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."[80]

[77] Zur Frage, in wie weit ausländische Server betroffen sein könnten und deswegen eine Rechtswidrigkeit zu bejahen ist, Sankol: „Verletzung fremdstaatlicher Souveränität durch ermittlungsbehördliche Zugriffe auf E-Mail-Postfächer", in: KR 2008, 279ff.

[78] Etwa USB-Stick, DVD, CD-Rom... Die Daten sind hier zwar auf dem Server des Providers, der selbstverständlich auch über hardware verfügt; die Daten müssen aber für den Zugriff erst ausausgesondert werden – eine Sicherstellung sämtlicher beim Provider organisierter Daten wäre evident unverhältnismäßig.

[79] vgl. Schlegel: „Online-Durchsuchung light", in HRRS Januar 2008, S. 23, 29. (letzter Abruf: 27.11.2009), der die „abstrakte" Möglichkeit des Zugriffs auf die E-Mails beim Provider für die Eröffnung des Geltungsbereichs nicht ausreichen lassen will (m.w.N.).

[80] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 88.

Das BVerfG verlangt also die Wahrung des Prinzips der Datensparsamkeit auch bei der und durch die Durchsicht. Nur dann, wenn die Filterung und Trennung im Verfahren (3) nicht zumutbar ist, dürfen alle Datenobjekte dauerhaft beschlagnahmt werden. Es muss dann allerdings im Rahmen der Verhältnismäßigkeitsprüfung („Übermaßverbot) im engeren Sinne der endgültigen Beschlagnahme (4) abgewogen werden:

BVerfG:

„**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.“**[81]

d) Verfahrensschritt (4) – „endgültige Beschlagnahme“

Das oben zugrundegelegte strafprozessrechtliche Prinzip der Datensparsamkeit hat selbstverständlich auch Auswirkungen auf die Entscheidung, welche Daten für die Dauer des Verfahrens (und die Archivierung) gespeichert werden.

3. Verhältnismäßigkeit im engeren Sinne

FÖR Dogmatik:
Für die Prüfung der Verhältnismäßigkeit im engeren Sinne wird empfohlen, folgende Prüfungsreihenfolge[82] gedanklich einzuhalten:
(1) Bestimmung des **Eingriffsrechtsguts**
(2) Bestimmung des **Eingriffs**
(3) Ermittlung der **Eingriffsqualität** (Intensität des Eingriffs)
(4) Bestimmung des Rechtfertigungsrechtsguts
(5) Förderung des Rechtfertigungsrechtsguts durch den Eingriff
(6) Bewertung der **Qualität der Förderung des Rechtfertigungsrechtsguts**
(7) Abwägung zwischen der Schwere des Eingriffs in das Eingriffsrechtsgut und der Qualität der Förderung des Rechtfertigungsrechtsguts

Die Verhältnismäßigkeitsprüfung im engeren Sinne ist der Prüfungspunkt, der regelmäßig von entscheidender Bedeutung ist – und zwar nicht nur im deutschen, sondern auch im europäischen Recht (principle of proportionality)[83].

[81] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 89.

[82] nähere Erläuterungen zu diesem Schema in: CyLaw-Report XXI: "Verdeckte Online-Durchsuchungen - zur IT-(Un)Sicherheit in Deutschland (06/2008/Version 3.0)" (26.06.2008).

[83] **FEX: Art. 5 Abs. 3 EG**
Die Maßnahmen der Gemeinschaft gehen nicht über das für die Erreichung der Ziele dieses Vertrags erforderliche Maß hinaus.

(1) Bestimmung des Eingriffsrechtsguts
Eingriffsrechtsgut ist Art. 10 GG (siehe oben unter A.I.).

(2) Bestimmung des Eingriffs
Eingriff ist die richterliche Anordnung des Zugriffs (siehe oben unter B.).

(3) Ermittlung der Eingriffsqualität (Intensität des Eingriffs)
Zu der Schwere, die der Eingriff beim staatlichen Zugriff auf E-Mails annehmen kann, führt das BVerfG aus:

BVerfG:

„[…] 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**."[84]

Gegen die Schwere des Eingriffs argumentiert das BVerfG mit vier Kriterien, die es bereits in früheren Verfahren zur Begründung eines schweren Eingriffs in das Fernmeldegeheimnis herangezogen hat, nämlich

- die Heimlichkeit des Eingriffs,
- ein längerfristiger Eingriff in einen laufenden Telekommunikationsvorgang an Stelle einer einmaligen, punktuellen Datenerhebung,
- die Möglichkeit einer Verwendung der Daten, die erhoben werden, zu unbestimmten oder noch nicht bestimmbaren Zwecken,
- die fehlende Einwirkungsmöglichkeit des Betroffenen auf seinen Datenbestand.[85]

BVerfG:

Die Schwere eines Eingriffs erhöht sich, wenn er heimlich erfolgt […]. Ein längerfristiger Eingriff in einen laufenden Telekommunikationsvorgang wiegt schwerer als eine einmalige und punktuelle Datenerhebung, da Umfang und Vielfältigkeit des Datenbestands erheblich größer sind […]. 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 […]. Eine erhöhte Eingriffsintensität ist schließlich dann anzunehmen, wenn der Betroffene über keinerlei Einwirkungsmöglichkeiten auf seinen Datenbestand verfügt […].

Im Bereich der Strafverfolgung sind daher bei heimlichen Eingriffen in das Fernmeldegeheimnis sowie etwa bei Zugriffen auf umfassende Datenbestände, die verdachtlos vorgehalten werden […] 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 […]. Geht es hingegen um eine aus einer Durchsuchung folgende, offene und durch den Ermittlungszweck begrenzte Maßnahme

[84] BVerfG, Beschluss vom 16.06.2009, Az.:,2 BvR 902/06, Rn. 70.
[85] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 68.

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.[86]

BVerfG:

„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 […], 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 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.**“[87]

Grundsätzlich geht das BVerfG bei dem nicht Beschuldigten B nicht von einem so schweren Grundrechtseingriff aus.

(4) Bestimmung des Rechtfertigungsrechtsguts

Zweck des Eingriffs ist die Verfolgung von Straftaten.

FÖR-Kritik: Unbestimmtheit des Rechtfertigungsrechtsguts bei §§ 94 StPO

Weil bei § 94 StPO keine Katalogstraftaten genannt sind, können abstrakte bestimmte Aussagen über die Rechtfertigungsrechtsgüter und ihre Bedeutung nicht getroffen werden. Straftaten reichen von Beleidigungen im Internet (etwa Erstellung falscher Persönlichkeitsprofile in sozialen Netzwerken; dazu demnächst der CyLaw-Report „Datenschutz oder Tatenschutz ?“ zum Urteil des Europäischen Gerichtshofs für Menschenrechte vom 02.12.2008 in Sachen K.U. gegen Finnland (application no. 2872/02)) bis zu Mord- und Totschlag – und damit ist auch deutlich, dass die Bedeutung der Strafverfolgung für das Allgemeinwohl differiert. Das BVerfG weicht dieses Prüfungskriterium auf, wenn es die Strafverfolgung beim Zugriff auf die E-Mails undifferenziert rechtfertigt:

BVerfG

„[…] Unter diesen Umständen ist es zur Wahrung der Verhältnismäßigkeit nicht geboten, den Zugriff auf beim Provider gespeicherte E-Mails auf Ermittlungen zu begrenzen, die

[86] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 68, 69.
[87] BVerfG, Beschluss vom 16.06.2009, Az.: 2 BvR 902/06, Rn. 75.

zumindest Straftaten von erheblicher Bedeutung betreffen, und Anforderungen an den Tatverdacht zu stellen, die über den Anfangsverdacht einer Straftat hinausgehen.

[…] 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 […]. 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).

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 […].“[88]

FÖR-Kritik: Parallelwertung mit dem traditional law der Beschlagnahme
Das BVerfG scheint nicht zu realisieren, dass § 94 ff StPO für die „Beschlagnahme“ von unter Umständen tausenden von E-Mails eines Nichtbeschuldigten zur Verfolgung einer Straftat, die in 2006 nicht zu Katalogtaten gehört hat, keine Abwägungskriterien enthält.

FINT (Für Interessierte): Anzumerken ist dass der 2. Senat des BVerfG dem Gesetzgeber beim Erlass von Strafrahmen und damit dem Indiz für die Qualität des Rechtfertigungsrechtguts zutiefst misstraut:

BVerfG:
„[…] 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.“[89]

Im Klartext: **Wenn das Gericht eine dogmatisch saubere und grammatisch ausdrückliche Prüfung verlangen würde, bestünde die Gefahr, dass der an Surveillancetechnologien interessierte Gesetzgeber willkürlich die Strafrahmen hochsetzt.**

Zusammenfassend ist festzuhalten, dass das BVerfG die Beschlagnahme von beim Provider gespeicherten E-Mails prinzipiell für alle Straftaten rechtfertigt.

[88] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 72-74.
[89] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 74.

BVerfG:

„[…] 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).

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. […]“[90]

(5) Förderung des Rechtfertigungsrechtsguts durch den Eingriff

BVerfG:

„[…] 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 […]. 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 Ermittlungsmaßnahmen ergänzt, sondern ist vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr einschließlich der anschließenden digitalen Verarbeitung und Speicherung zu sehen […].“[91]

Grundsätzlich wird also durch die dynamisch-technikorientierte Auslegung von Beschlagnahmenormen des traditional law dem digitalen Handeln der Täter begegnet.

6) Bewertung der Qualität der Förderung des Rechtfertigungsrechtsguts

FÖR-Kritik: Unbestimmtheit
Weil das Rechtfertigungsrechtsgut in der Auslegung des BVerfG nicht grammatisch benannt wird und abstrakt nicht zwischen schweren und anderen Straftaten differenziert wird. Weil auch die Ermittlungsmaßnahmen nicht näher konturiert werden (Beschlagnahme von Gegenständen), scheidet eine dogmatisch überzeugende Prüfung der „Qualität der Förderung des Rechtfertigungsrechtsguts“ aus.

[90] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn.73f.
[91] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 71.

(7) Abwägung zwischen der Schwere des Eingriffs in das Eingriffsrechtsgut und der Qualität der Förderung des Rechtfertigungsrechtsguts

Das BVerfG hält einen E-Mailzugriff dann nicht für verhältnismäßig, wenn an Stelle eines konkreten Tatvorwurfs für die Straftat nur bloße Vermutungen bestünden. Ebenso könnten im Einzelfall die geringe Bedeutung der Straftat, die geringe Beweisbedeutung der E-Mails und die Vagheit des „Auffindeverdachts" der „Angemessenheit" (FÖR-Terminologie: Verhältnismäßigkeit im engeren Sinne) des Zugriffs auf die E-Mails entgegenstehen.

BVerfG:

„[…] Die Maßnahme muss vor allem in angemessenem Verhältnis zu der Schwere der Straftat und der Stärke des Tatverdachts stehen […]. 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 […]. 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 Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der zu beschlagnahmenden E-Mails sowie die Vagheit des Auffindeverdachts der Maßnahme entgegenstehen." [92]

Wie sich aus dem Vorangegangenem ergibt, geht das BVerfG insgesamt von einem nicht so schweren Eingriff aus und rechtfertigt die Verhältnismäßigkeit im engeren Sinne mit der Bedeutung der Strafverfolgung. Das BVerfG legt eine Umgehungsratio zugrunde, der zufolge sich Beschuldigte und Dritte der Strafverfolgung nicht dadurch entziehen können sollen, dass die E-Mails beim Provider ausgelagert werden.

III. Grundrechtsschutz durch Verfahren

Auch materiell verfassungsmäßige Eingriffe rechtfertigt das BVerfG nur, wenn darüber hinaus der Gesetzgeber die effektiven Garantiebereiche der Grundrechte durch die rechtliche und tatsächliche Ausgestaltung der Verfahrensvoraussetzungen des Eingriffs möglichst effektiv geschützt hat. Diese Dogmatik wird unter der Terminologie **„Grundrechtsschutz durch Verfahren"** zusammengefasst. Aus dem Grundsatz des effektiven Grundrechtschutzes leitet das BVerfG also die Notwendigkeit von Verfahrensgarantien ab, die insbesondere auch bei Eingriffen in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) beachtet werden müssten.[93] Es unterscheidet hierbei, seiner bisherigen Rechtsprechung - etwa zur Telekommunikationsüberwachung[94] oder zum Zugriff auf elekronische Datenbestände bei Berufsgeheimnisträgern[95]- entsprechend zwischen

[92] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 79.
[93] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 91f..
[94] BVerfGE Band 100, S. 313, 360ff.
[95] BVerfGE Band 113, S. 129, 58; vgl. hierzu: CyLaw-Report IX: "Strafprozessualer Zugriff auf Datenbestände" (10.05.2006).

- **Unterrichtungspflicht,**
- **Teilnahmerecht,**
- **Auskunftspflicht,**
- **Löschungspflicht und**
- **Beweisverwertungsverbot**

BVerfG:

„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 […]. 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."[96]

In Bezug auf den strafprozessualen Zugriff auf E-Mails beim Provider konkretisiert das BVerfG diese Verfahrensanforderungen, wie folgt:

1. Unterrichtungspflicht (Bekanntmachung § 35 StPO)

Hier sind zwei Konstellationen zu unterscheiden:

- zum einen die Unterrichtung von B

Richterliche Durchsuchungsanordnungen, die sich auf den Zugriff auf die auf dem Mailserver des Providers gespeicherten E-Mails des Betroffenen beziehen und Anordnungen der Beschlagnahme solcher E-Mails sind vor der Durchführung der Anordnung dem Betroffenen bekanntzugeben (§ 35 StPO). Bei Gefährdung des Ermittlungszwecks durch eine vorherige Bekanntgabe, kann diese unterbleiben. Erforderlich ist dann aber eine so bald wie mögliche nachträgliche Unterrichtung. Sofern die Ermittlungsbehörden wegen Gefahr im Verzug die E-Mails ohne vorausgehende richterliche Anordnung vorläufig sicherstellen, ist der Betroffene über sein Recht, eine richterliche Entscheidung über diese Maßnahme zu beantragen, zu belehren und wird damit über die Maßnahme auch unterrichtet (§ 98 Abs. 2 Satz 2, 7 StPO).

§ 35 StPO [Bekanntmachung]

(1) Entscheidungen, die in Anwesenheit der davon betroffenen Person ergehen, werden ihr durch Verkündung **bekanntgemacht.** Auf Verlangen ist ihr eine Abschrift zu erteilen.

(2) Andere Entscheidungen werden durch Zustellung bekanntgemacht. Wird durch die Bekanntmachung der Entscheidung keine Frist in Lauf gesetzt, so genügt formlose Mitteilung.

[…]

§ 98 [Anordnung der Beschlagnahme]

[…]

[96] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 92.

(2) Der Beamte, der einen Gegenstand ohne gerichtliche Anordnung beschlagnahmt hat, soll binnen drei Tagen die gerichtliche Bestätigung beantragen, wenn […]. Der Betroffene kann jederzeit die gerichtliche Entscheidung beantragen. […]Der Betroffene ist über seine Rechte zu belehren.

[…]

- und zum anderen die Unterrichtung anderer Nichtbeteiligter (die etwa an B eine E-Mail versandt oder von ihm erhalten haben). Hervorzuheben ist, dass E-Mails von und an völlig Unbeteiligte (also weder die Beschuldigten noch B) nicht gelesen werden müssen, damit man sie informieren kann:

BVerfG:

„[…] 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 […]. 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."[97]

2. Teilnahmerecht

Grundsätzlich rügte der B, dass weder er noch sein Rechtsanwalt beim Verfahrensschritt 3 - bei der Durchsicht – anwesend sein darf und damit protokollieren darf, wie mit den e-Mails umgegangen wird. Grundsätzlich enthält die Strafprozessordnung bei Durchsuchungen von Gegenständen und Wohnungen ein Anwesenheitsrecht des Inhabers.

§ 106 StPO [Zuziehung des Inhabers]

(1) Der Inhaber der zu durchsuchenden Räume oder Gegenstände darf der Durchsuchung beiwohnen. Ist er abwesend, so ist, wenn möglich, sein Vertreter oder ein erwachsener Angehöriger, Hausgenosse oder Nachbar zuzuziehen. […]

Dieses Recht könnte bedeutsam sein, weil der Inhaber etwa mitbekommen kann, ob ihm Gegenstände untergeschoben werden. Nicht verschwiegen werden soll, dass die Wertigkeit von § 106 StPO beim Bundesgerichtshof umstritten war: ein Ermittlungsrichter sah ihn als „bloße Ordnungsvorschrift", während der dritte Senat ihm konstitutive Bedeutung zumaß und deshalb die heimliche Onlinedurchsuchung für rechtswidrig erachtete (vergleiche CyLaw-Report XX). **Auch für die Durchsicht von Papieren sah eine Vorgängervorschrift ein Teilnahmerecht vor (siehe oben zu § 110 Abs. 3 alter Fassung). Dieses war aber ohne Begründung aufgehoben worden**. Das BVerfG verlangt von Verfassungs wegen kein abstraktes Teilnahmerecht des B oder seines Rechtsanwalts – sondern es überlässt dies der konkreten Anordnung (siehe Teil 3).

[97] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 98.

BVerfG:

„[…] 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 […]. 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.“[98]

Zusammenfassend ist insoweit festzuhalten, dass die in der Literatur vorgebrachte Begründung für das Anwesenheitsrecht des Rechtsanwalts des B (Hausrecht) bei der „Beschlagnahme“ in den Räumen des Providers bzw. die Durchsicht in den Amtsräumen keine Rolle spielt. Diese Verkürzung des rechtlichen Schutzes der Datenvertraulichkeitsinteressen ist angesichts der besonderen Qualität von Daten hervorzuheben: anders als bei der Durchsuchung und Beschlagnahme von Gegenständen können rechtswidrige Ermittlungsmaßnahmen nicht mit einem begrenzten Schaden wieder aufgehoben werden: Nach der Durchsicht sind die Datenschutzinteressen des B unwiderruflich verletzt.

3. Auskunftspflicht

Zum effektiven Schutz seiner Grundrechte kann dem Betroffenen im Einzelfall ein Anspruch auf Auskunft darüber zustehen, welche in seinen E-Mails enthaltenen Daten von den Ermittlungsbehörden gespeichert worden sind und ausgewertet werden (Verfahrensschritte 2 und 3). Für den Beschwerdeführer kann sich ein solcher Auskunftsanspruch insbesondere aus § 491 Abs. 1 S. 1 StPO i.V.m § 19 BDSG ergeben.

§ 491 StPO [Auskunft an Betroffene]

1) Dem Betroffenen ist, soweit die Erteilung oder Versagung von Auskünften in diesem Gesetz nicht besonders geregelt ist, **entsprechend § 19 des Bundesdatenschutzgesetzes Auskunft** zu erteilen. […]

§ 19 BDSG Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1.die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2.die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

[98] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 96.

3.den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

[…]

(4) Die Auskunftserteilung unterbleibt, soweit

1.die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2.die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3.die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

BVerfG:

„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 […]. 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 Auskunftserteilung entsprechend § 19 BDSG unterbleibt, soweit die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde. […]“[99]

[99] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 98.

4. Löschungspflicht

Grundsätzlich sind die personenbezogenen Daten so früh wie möglich zu löschen.[100]

§ 3 BDSG [Weitere Begriffsbestimmungen]

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). […]

§ 489 StPO [Berichtigung, Löschung und Sperrung gespeicherter Daten]

[…]

(2) Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder sich aus Anlass einer Einzelfallbearbeitung ergibt, dass die Kenntnis der Daten für die in den §§ 483, 484, 485 jeweils bezeichneten Zwecke nicht mehr erforderlich ist. Es sind ferner zu löschen

1.nach § 483 gespeicherte Daten mit der Erledigung des Verfahrens, soweit ihre Speicherung nicht nach den §§ 484, 485 zulässig ist,

2.nach § 484 gespeicherte Daten, soweit die Prüfung nach Absatz 4 ergibt, dass die Kenntnis der Daten für den in § 484 bezeichneten Zweck nicht mehr erforderlich ist und ihre Speicherung nicht nach § 485 zulässig ist,

3. nach § 485 gespeicherte Daten, sobald ihre Speicherung zur Vorgangsverwaltung nicht mehr erforderlich ist. […]

5. Beweisverwertungsverbot

Das BVerfG sichert die Einhaltung des (Verfassungs-)Rechts durch die Konturierung eines Beweisverwertungsverbots: evidente und grobe Rechtsfehler können dazu führen, dass die Informationen im Verfahren nicht verwertet werden dürfen („Beweisverwertungsverbot“ - siehe auch CyLAW-Report XXIII: „GPS 2“).

BVerfG:

Die bisher in der Rechtsprechung entwickelten und anerkannten Beweisverwertungsverbote im Zusammenhang mit der Durchsuchung und Beschlagnahme schützen teilweise vor unerlaubten Eingriffen in Grundrechte. Zum wirksamen Schutz des Grundrechts auf informationelle Selbstbestimmung jedenfalls Unbeteiligter und zur effektiven Wahrung des Vertrauensverhältnisses zum Berufsgeheimnisträger wird aber zu prüfen sein, ob ergänzend ein Beweisverwertungsverbot in Betracht zu ziehen ist. Dieses würde der Effektuierung des Grundrechts aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG und des verfassungsrechtlich geschützten Vertrauensverhältnisses zum Rechtsberater dienen.

Zumindest **bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, in denen die Beschränkung auf den Ermittlungszweck der Datenträgerbeschlagnahme planmäßig oder systematisch außer Acht gelassen wird, ist ein Beweisverwertungsverbot als Folge einer fehlerhaften Durchsuchung und Beschlagnahme von Datenträgern und der darauf vorhandenen Daten geboten**.[101]

[100] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 100.

[101] BVerfG, Beschluss vom 12. April 2005; Az 2 BvR 1027/02 Rn. 134, f.;

FEX: Das BVerfG prüft auch noch eine sechste Verfahrensanforderung, die Kennzeichnungspflicht:

FINT (Für Interessierte): Beweisverwertungsverbot ohne Nutzen für B
Anzumerken ist, dass aus der Sicht des B das Beweisverwertungsverbot nicht weiterhilft. Er ist nicht Beschuldigter und wird – nachdem seine Daten gegebenenfalls rechtswidrig „beschlagnahmt“ wurden – von einem Beweisverwertungsverbot nicht „profitieren“ (dies würden gegebenenfalls nur S und G).

D. Zwischenergebnis:

Die gesetzlichen Vorschriften über die Sicherstellung und Beschlagnahme stellen nach der Auslegung des BVerfG eine verfassungsgemäße Ermächtigungsgrundlage für den strafprozessualen Zugriff auf E-Mails dar, die auf dem Mailserver des Providers gespeichert sind.

Teil 3: Verfassungsmäßigkeit der Sicherstellung, Durchsicht und Beschlagnahme der beim Provider befindlichen E-Mail-Daten des B (konkret)

An die Prüfung der Verfassungsmäßigkeit der gesetzlichen Ermächtigungsgrundlagen (abstrakt) schließt sich die weitere Prüfung an, ob der konkrete Zugriff auf die Daten des B ebenfalls verfassungsmäßig war.

FEX: Prüfungsstruktur
Die Rechtmäßigkeit einer konkreten informationstechnologischen Maßnahme setzt also immer zweierlei voraus:
1. zum einen die Verfassungsmäßigkeit der gesetzlichen Ermächtigungsgrundlagen (§§ 94ff. StPO) und
2. zum anderen die Verfassungsmäßigkeit des konkreten Zugriffs.
Hinsichtlich der Eröffnung des Geltungsbereichs eines Grundrechts kann regelmäßig bei der konkreten Prüfung auf die abstrakte Prüfung verwiesen werden.

BVerfG:

„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 […] - 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.“ (Rn. 102)

A. Recht- (R)

Der Geltungsbereich des Art. 10 Abs. 1 GG ist nach der Rechtsprechung des BVerfG eröffnet (siehe Teil 2 A).

B. Eingriff – (E)

Der Eingriff liegt in der vorläufigen Sicherstellung beim Provider (Verfahrensschritt 2) und der Durchsicht (Verfahrensschritt 3). Eine Entscheidung über die endgültige Beschlagnahme ist noch nicht getroffen (Verfahrensschritt 4).

BVerfG:

„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.**“[102]

C. Rechtfertigung – (R)

I. Spezielle Schranke (Art. 10 Abs. 2 S. 1 GG: Gesetz)

Das BVerfG ist der Auffassung, dass die §§ 94 ff StPO eine formell und materiell verfassungsmäßige, gesetzliche Grundlage für die „Beschlagnahme“ darstellen (siehe Teil 2). Problematisch ist allerdings, dass die vorbefassten Richter eine falsche Terminologie zugrundelegten, und die „Beschlagnahme“ prüfen, obwohl es sich nach Auffassung des BVerfG um eine „vorläufige Sicherstellung“ zum „Zwecke der Durchsicht“ handelt. Diese Verwendung falscher Terminologie durch Juristen sei aber unschädlich:

BVerfG:

„**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**. […]

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 klarge-

[102] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 106.

stellt, 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 […].“[103]

II. Verhältnismäßigkeit im weiteren Sinne

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Schwere des Eingriffs in das Eingriffsrechtsgut darf nicht außer Verhältnis zur Qualität der Förderung des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

1. Geeignetheit

Grundsätzlich geht das BVerfG von der Geeignetheit als Unterfall der „Angemessenheit“ aus.

BVerfG:

„[…] **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. Erforderlichkeit

Auch den Grundsätzen der Datensparsamkeit war genügt, weil eine Filterung beim Provider für diesen belastend gewesen wäre (Schutz seiner Geschäftsräume durch Art. 13 GG) und deswegen die Mitnahme aller E-Mails in grundrechtlicher Betrachtung der geringste, für die Förderung des Rechtfertigungsguts geeignete Eingriff war.

[103] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn.105ff.
[104] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 104.

BVerfG:

„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.** […]“[105]

3. Verhältnismäßigkeit im engeren Sinne

Wie oben unter II 1 präsentiert, geht das BVerfG von der Geeignetheit und Verhältnismäßigkeit im engeren Sinne (FEX: Terminologie des BVerfG: Angemessenheit) aus.

III. Grundrechtsschutz durch Verfahren

Wie oben bereits dargestellt, verlangt das BVerfG eine am effektiven Grundrechtsschutz ausgerichtet Gestaltung des Verfahrens:

1. Unterrichtungspflicht

BVerfG:

„[…] In verfahrensrechtlicher Hinsicht wurde der verfassungsrechtlichen Anforderung Genüge getan, den Beschwerdeführer vor dem Zugriff auf die auf dem Mailserver seines Providers gespeicherten E-Mails hierüber zu unterrichten.“[106]

2. Teilnahmerecht

Das BVerfG verlangt nicht, dass der B und sein Rechtsanwalt an der Durchsicht teilnehmen dürfen (Verfahrensschritt 3).

„[…] **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 Nicht-

[105] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 108.
[106] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 111.

verdächtiger ist, folgt kein verfassungsunmittelbares Teilnahmerecht an der Durchsicht der sichergestellten E-Mails.“[107]

3. Löschungspflicht

BVerfG:

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.“[108]

4. Absolut geschützter Kernbereich privater Lebensgestaltung

Weder in den gesetzlichen Vorschriften (§§ 94ff StPO i.V.m Art. 10 Abs. 2 S. 1 GG) noch in der konkreten richterlichen „Beschlagnahme“-Anordnung ist die Einschränkung in grammatikalischer Auslegung enthalten, dass in den absolut geschützten Kernbereich privater Lebensgestaltung nicht eingegriffen werden dürfe. Dennoch beanstandet das BVerfG dieses Defizit weder bei den gesetzlichen Grundlagen (abstrakt) noch bei der Anordnung gegenüber B bzw. P (konkret):

BVerfG:

„[…] 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.“[109]

Das BVerfG erklärt also diese Schutzprinzipien zum vorausgesetzten Wissen - Domänenwissen - der Juristen.

D. Ergebnis:

Die Verfassungsbeschwerde wird vom BVerfG (mangels Begründetheit) zurückgewiesen. Auch die konkrete Vorgehensweise der Ermittlungsbehörden bei der vorläufigen Sicherstellung und der sich jetzt anschließenden Durchsicht wird verfassungsrechtlich nicht beanstandet.

[107] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 112.
[108] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 107.
[109] BVerfG, Beschluss vom 16.06.2009, Az. 2 BvR 902/06, Rn. 110.

Teil 4: Schlussfolgerungen aus dem Beschluss des BVerfG

- Das Fernmeldegeheimnis (Art. 10 GG) umfasst bei der E-Mail-Korrespondenz auch die Phasen außerhalb des dynamischen Übertragungsvorgangs (Zwischen- und Endspeicherung; Verfahrensstadien 2 und 4), in denen sich die E-Mails außerhalb des absoluten Herrschaftsbereichs der Kommunikationsteilnehmer auf dem Mailserver des Providers befinden.
- Auf der Grundlage der gesetzlichen Regelungen der StPO über die Sicherstellung und Beschlagnahme (§§ 94ff. StPO) kann in das Fernmeldegeheimnis dergestalt eingegriffen werden, dass die Strafverfolgungsbehörden im Ermittlungsverfahren auf die auf dem Mailserver des Providers gespeicherten E-Mails der Kommunikationsteilnehmer Zugriff nehmen.

Teil 5: Art. 10 GG bei informationstechnologischem „Mitgewahrsam“ von Arbeitgeber und Arbeitnehmer

Zwei hessische Entscheidungen, die vor der BVerfG-Entscheidung ergingen, veranlassen zur Präsentation der Frage, ob auch in anderen Fällen der „Mitgewahrsam“ eines anderen als dem bezeichneten Kommunikationsteilnehmer die Eröffnung des Geltungsbereichs des Art. 10 GG begründet. Handelt es sich beim BVerfG-Sachverhalt noch vielleicht um einen Einzelfall, so haben die hessischen Entscheidungen einen Alltagssachverhalt zum Gegenstand: nämlich die Datensicherung und die Zugriffsoptionen von Arbeitgebern auf die E-Mails und Rechner der Arbeitnehmer.

A. Sachverhalt

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) unterstützt die us-amerikanische Wertpapieraufsichtsbehörde (SEC) bei deren Ermittlungen gegen Mitarbeiter der Gesellschaft G wegen verbotenen Insiderhandels. Bei zwei Unternehmsübernahmen durch G besteht der Verdacht, dass bestimmte informierte Mitarbeiter ihr Wissen für Wertpapierhandelsgeschäfte ausgenutzt hätten (Insiderhandel).

Etwa: § 38 Gesetz über den Wertpapierhandel (WpHG) [Strafvorschriften][110]

(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer […]

2. […]

c)auf Grund seines Berufs oder seiner Tätigkeit oder seiner Aufgabe bestimmungsgemäß oder

d)auf Grund der Vorbereitung oder Begehung einer Straftat

über eine Insiderinformation verfügt und unter Verwendung dieser Insiderinformation eine in § 39 Abs. 2 Nr. 3 oder 4 bezeichnete vorsätzliche Handlung begeht.

[110] Hervorhebungen von der Verfasserin.

§ 39 WpHG [Bußgeldvorschriften]

(1) Ordnungswidrig handelt, wer […]

3. entgegen § 14 Abs. 1 Nr. 2 **eine Insiderinformation mitteilt oder zugänglich macht,**

4. entgegen § 14 Abs. 1 Nr. 3 den Erwerb oder die Veräußerung eines Insiderpapiers empfiehlt oder auf sonstige Weise dazu verleitet, […]

Dem Ersuchen der US-amerikanischen Wertpapieraufsichtsbehörde entsprechend fordert die BaFin die G zur Vorlage von E-Mails auf,

- die bestimmte Mitarbeiter der G im Zeitraum zwischen 01.05.2005 und 30.09.2006 an ihrem Arbeitsplatz empfangen (Eingang)
- oder von dort gesendet haben (Ausgang) und
- die bestimmte Schlüsselwörter enthalten.

Als Rechtsgrundlage für die Anforderung dieser E-Mails beruft sich die BaFin in einen Verwaltungsakt auf § 4 Abs. 3 i.V.m. § 7 Abs. 7 WpHG.

§ 4 Abs. 3 WpHG [Aufgaben und Befugnisse]

(3) Die Bundesanstalt kann von jedermann **Auskünfte, die Vorlage von Unterlagen und die Überlassung von Kopien** verlangen sowie Personen laden und vernehmen, soweit dies auf Grund von Anhaltspunkten für die Überwachung der Einhaltung eines Verbots oder Gebots dieses Gesetzes erforderlich ist. […] **Gesetzliche Auskunfts- oder Aussageverweigerungsrechte sowie gesetzliche Verschwiegenheitspflichten bleiben unberührt**.

§ 7 Abs. 7 WpHG [Zusammenarbeit mit zuständigen Stellen im Ausland]

(7) Die **Bundesanstalt kann mit den zuständigen Stellen** anderer als der in Absatz 1 genannten Staaten entsprechend den Absätzen 1 bis 6 z**usammenarbeiten und Vereinbarungen über den Informationsaustausch abschließen.** Absatz 4 Satz 5 und 6 findet mit der Maßgabe Anwendung, dass Informationen, die von diesen Stellen übermittelt werden, nur unter Beachtung einer Zweckbestimmung der übermittelnden Stelle verwendet und nur mit ausdrücklicher Zustimmung der übermittelnden Stelle der Deutschen Bundesbank oder dem Bundeskartellamt mitgeteilt werden dürfen, sofern dies für die Erfüllung ihrer Aufgaben erforderlich ist. Absatz 4 Satz 8 findet keine Anwendung. **Für die Übermittlung personenbezogener Daten gilt § 4b des Bundesdatenschutzgesetzes**.

§ 35 VwVfG [Begriff des Verwaltungsakts]

Verwaltungsakt ist jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist. […]

G, die ihren Mitarbeitern auch die Privatnutzung der geschäftlichen E-Mail-Adressen gestattet hat, sieht sich als Telekommunikationsdiensteanbieter an und ist der Auffassung, sie verstieße gegen das Fernmeldegeheimnis (§ 88 Abs. 2, 3 TKG i.V.m. § 4 Abs. 3 S. 3 WpHG), wenn sie der Aufforderung der BaFin entspreche.

§ 3 TKG [Begriffsbestimmungen]

Im Sinne dieses Gesetzes ist oder sind […]

6.**„Diensteanbieter"** jeder, der ganz oder teilweise **geschäftsmäßig**

a)Telekommunikationsdienste erbringt oder

b)an der Erbringung solcher Dienste mitwirkt; […]

10.„**geschäftsmäßiges Erbringen** von Telekommunikationsdiensten" das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht; […]

§ 88 TKG [Fernmeldegeheimnis]

[…]

(2) **Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet**. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. **Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.**

Darüber hinaus mache sich ihr Systemadministrator strafbar, wenn er die E-Mails filtere und vorlege (§ 206 StGB).[111]

§ 206 StGB [Verletzung des Post- oder Fernmeldegeheimnisses]

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

[…]

(5) […] Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Ein Verwaltungsakt, der von ihr – G – die Begehung einer Straftat verlange, sei nichtig.

[111] FINT (Für Interessierte): Zur Strafbarkeit des Systemadministrators bei der Unterdrückung von E-Mails siehe bereits CyLaw-Report IV: „E-Mail Filter I" (18.11.2005).

§ 44 VwVfG [Nichtigkeit des Verwaltungsaktes]

[…]

(2) Ohne Rücksicht auf das Vorliegen der Voraussetzungen des Absatzes 1 ist ein Verwaltungsakt nichtig, […]

5. der die Begehung einer rechtswidrigen Tat verlangt, die einen Straf- oder Bußgeldtatbestand verwirklicht; […].

G klagt deswegen vor dem Verwaltungsgericht Frankfurt gegen den Verwaltungsakt der BaFin. Die BaFin argumentiert in dem Verfahren mit zwei „Säulen“:

- zum einen bestünde kein Schutz des Fernmeldegeheimnisses, weil die E-Mails, die durch die Rechner des Arbeitgebers abgerufen werden könnten, sich im Herrschaftsbereich der Arbeitnehmer befänden (die dynamische Telekommunikation sei damit abgeschlossen);
- zum anderen bestünde – selbst wenn der Geltungsbereich des Fernmeldegeheimnisses (Art. 10 GG, § 88 TKG) eröffnet sei – kein Schutz, weil das Fernmeldegeheimnis nicht die Strafverfolgung behindern dürfe (klassisches Argument**: Datenschutz dürfe nicht Tatenschutz sein**).

Das Vorbringen der BaFin, wie es im Urteil des VG Frankfurt[112] wiedergegeben ist:

„Insbesondere sei das Auskunftsersuchen nicht nichtig im Sinne des § 44 Abs 2 Nr. 5 VwVfG, weil nicht die Begehung einer rechtswidrigen Tat verlangt werde. Es sei fraglich, ob ein Arbeitgeber, der seinen Beschäftigten die private Nutzung der geschäftlichen E-Mail-Adressen gestattet habe, geschäftsmäßig Telekommunikationsdienste erbringe. Zudem entspreche es der Rechtsprechung des Bundesverfassungsgerichts, dass gespeicherte Verbindungsdaten nach Abschluss eines Übertragungsvorganges im Herrschaftsbereich eines Telekommunikationsteilnehmers nicht durch Art 10 Abs 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art 2 Abs 1 i. V. m. Art 1 Abs 1 GG) geschützt würden. **Jedenfalls könne aber ein Arbeitgeber, der die private Nutzung geschäftlicher E-Mail-Adressen gestattet habe, bei einem Verdacht von Straftaten auch private E-Mails von Arbeitnehmern kontrollieren. Ein Einverständnis des Arbeitgebers zur privaten Nutzung geschäftlicher E-Mail-Adressen umfasse nicht die Begehung offensichtlich rechtswidriger Taten. Dies gelte auch dann, wenn der Verdacht einer Straftat wie Insiderhandel (§ 38 Abs 1 WpHG) im Raum stehe, bei der sich der Arbeitnehmer neben dem strafrechtlichen Vorwurf auch gegen die Interessen seines Arbeitgebers stelle. Im vorliegenden Fall bestehe der dringende Verdacht, dass Verstöße gegen das Verbot des Insiderhandels erfolgt seien**.“

Weil G vor dem Verwaltungsgericht im Ergebnis keinen Erfolg hat, beantragt G die Zulassung der Berufung vor dem Verwaltungsgerichtshof (VGH) Kassel.

[112] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 6 (zitiert nach juris).

§ 124a Verwaltungsgerichtsordnung (VwGO) [Zulassung und Begründung der Berufung]

(1) Das Verwaltungsgericht lässt die Berufung in dem Urteil zu, wenn die Gründe des § 124 Abs. 2 Nr. 3 oder Nr. 4 vorliegen. Das Oberverwaltungsgericht ist an die Zulassung gebunden. […]

(4) Wird die Berufung nicht in dem Urteil des Verwaltungsgerichts zugelassen, so ist die Zulassung innerhalb eines Monats nach Zustellung des vollständigen Urteils zu beantragen. Der Antrag ist bei dem Verwaltungsgericht zu stellen. […] Die Stellung des Antrags hemmt die Rechtskraft des Urteils.

(5) Über den Antrag entscheidet das Oberverwaltungsgericht durch Beschluss. Die Berufung ist zuzulassen, wenn einer der Gründe des § 124 Abs. 2 dargelegt ist und vorliegt. Der Beschluss soll kurz begründet werden. Mit der Ablehnung des Antrags wird das Urteil rechtskräftig. Lässt das Oberverwaltungsgericht die Berufung zu, wird das Antragsverfahren als Berufungsverfahren fortgesetzt; der Einlegung einer Berufung bedarf es nicht.

[…]

§ 124 VwGO [Zulässigkeit der Berufung]

[…]

2) Die Berufung ist nur zuzulassen,

1.wenn ernstliche Zweifel an der Richtigkeit des Urteils bestehen,

2.wenn die Rechtssache besondere tatsächliche oder rechtliche Schwierigkeiten aufweist,

3.wenn die Rechtssache grundsätzliche Bedeutung hat,

4.wenn das Urteil von einer Entscheidung des Oberverwaltungsgerichts, des Bundesverwaltungsgerichts, des gemeinsamen Senats der obersten Gerichtshöfe des Bundes oder des Bundesverfassungsgerichts abweicht und auf dieser Abweichung beruht oder

5.wenn ein der Beurteilung des Berufungsgerichts unterliegender Verfahrensmangel geltend gemacht wird und vorliegt, auf dem die Entscheidung beruhen kann.

B. Fernmeldegeheimnis (§ 88 TKG i.V.m. Art. 10 Abs. 1 GG) oder Schutz nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG?

I. Bedeutung der Eröffnung unterschiedlicher Geltungsbereiche für die Prüfungsreihenfolge und den effektiven Garantiebereich für „Datenschutz“

FINT (Für Interessierte): „effektiver Garantiebereich“
Die FÖR-Perspektive des legal realism interessiert sich dafür, welches Ergebnis für das tatsächliche Schutzniveau durch die Bejahung der Eröffnung des Geltungsbereichs eines Grundrechts konturiert wird. Der Schutz, der am Ende der Prüfung für die Privatsphäre bejaht wird, wird als „effektiver Garantiebereich“ bezeichnet. [113]

[113] Grundlegend zu dieser Terminologie Lübbe-Wolf: „Die Grundrechte als Eingriffsabwehrrechte“, 1988.

FEX: Bedeutung der Eröffnung des Geltungsbereichs von Art. 10 Abs. 1GG, § 88 TKG: § 88 Abs. 3 S. 3 TKG und Art. 19 Abs. 1 S. 2 GG

Der vorliegende Sachverhalt verdeutlicht noch einmal die Bedeutung, die die Eröffnung des Geltungsbereichs des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) gegenüber der Eröffnung der Rechte auf informationelle Selbstbestimmung bzw. auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) hat.

- **Wenn Art. 10 Abs. 1 GG eröffnet ist, dann bedarf es nach Art. 10 Abs. 2 GG und seiner Konkretisierung in § 88 Abs. 3 S. 3 TKG einer gesetzlichen Ermächtigungsgrundlage zur Weitergabe der Daten. Darüber hinaus muss diese gesetzliche Grundlage sich in grammatischer Auslegung ausdrücklich auf Telekommunikationsvorgänge erstrecken oder bei den Gesetzgebungsberatungen muss das Fernmeldegeheimnis berücksichtigt worden sein.** Daran fehlt es im vorliegenden Fall in den wertpapierhandelsrechtlichen Befugnisnormen mit der Konsequenz, dass nach Auffassung der G das Übermittlungsverlangen abschlägig zu bescheiden ist.

Vorbringen der G, wie es im Urteil des VG Frankfurt wiedergegeben ist:
„§ 4 Abs 3 WpHG sei keine Rechtsgrundlage für einen Eingriff in den Schutzbereich des § 88 TKG i. V. m. Art 10 Abs 1 GG. Eine Verwendung entsprechender Erkenntnisse sei nur zulässig, wenn dies durch eine gesetzliche Vorschrift vorgesehen sei und diese Vorschrift sich dabei ausdrücklich auf Telekommunikationsvorgänge beziehe (§ 88 Abs 3 Satz 3 TKG).“ [114]

- Wenn die Verkehrsdaten und Inhalte nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG geschützt sind, **dann soll § 88 Abs. 3 S. 3 TKG in seiner spezialgesetzlichen Konturierung des Zitiergebots und auch Art. 19 Abs. S. 2 GG[115] nicht gelten** – mit der Konsequenz, dass eine verfassungsrechtliche Abwägung im Rahmen der RER-Prüfung („verfassungsmäßige Ordnung“) nicht ausgeschlossen ist. Hier wäre dann insbesondere in der „Verhältnismäßigkeit im engeren Sinne“ abzuwägen, zwischen Daten- und Tatenschutz. **Eine solche Prüfung wäre bei der Eröffnung des Geltungsbereichs des Art. 10 GG, § 88 TKG bereits aus formellen Gründen – Nichterfüllung des Zitiergebots durch die Befugnisnormen, die eben nicht auf die Telekommunikation Bezug nehmen (§ 88 Abs. 3 S. 3 TKG) - nicht rechtmäßig.**

In einer technologieorientierten Perspektive scheint maßgeblich für die Entscheidung der Eröffnung des Geltungsbereichs welche Informationstechnologie eingesetzt wird.

II. Qualität der Informationstechnologie

Nach dem Vortrag der G vor dem Verwaltungsgericht setzt sie ein übliches Mailsystem ein:

[114] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 10 (zitiert nach juris).

[115] Dazu, dass nach angeblich h.M. bei der Schrankenbestimmung des Art. 2 Abs. 1 GG Art. 19 Abs. 1 S. 2 GG nicht gilt Huber, Art. 19 Abs. 1 Rn 77 in v. Mangoldt/Klein/Starck, GG, 2005, m.w.N..

Vorbringen der G, wie es im Urteil des VG Frankfurt[116] wiedergegeben ist:

„Die Klägerin setze ein herkömmliches Mailsystem ein. Ein- und ausgehende Mails würden auf einem zentralen Rechner gespeichert. Die Nachrichten auf dem Server würden jede Nacht und sodann wöchentlich gesichert. Die Wochensicherung würde 6 Wochen aufbewahrt und dann gelöscht. Im Übrigen hätten die Mitarbeiter die Möglichkeit, Mails auf ihren Arbeitsplatzrechner zu kopieren bzw. zu archivieren."

FÖR-Terminologie: „Datenorganisation"
In der FÖR-Terminologie ist Datenorganisation ein Oberbegriff für das Erheben, Verarbeiten und Nutzen von Daten (§ 3 Abs. 3 bis 5 BDSG).

Festzuhalten ist, dass zwei „Organisationsstrukturen" zunächst zu unterscheiden sind:

- Die Speicherung auf dem Zentralserver der G mit einer theoretisch zugrundegelegten Speicherzeit von 6 Wochen (originäre Arbeitgebersphäre) und weiteren Zentralspeicherungstrategien.
- Die „Organisationsentscheidung" des Arbeitnehmers darüber, ob er die E-Mails auf seinem lokalen Rechner speichert, auf einem Medium (USB-Stick) mitnimmt, löscht, die E-Mails verschlüsselt …(originäre Arbeitnehmersphäre[117]).

1. Speicherung und Wiederherstellung der E-Mails auf dem Zentralserver (originäre Arbeitgebersphäre)

Strittig war vor beiden Gerichten, inwieweit die Arbeitgeberin G auch nach Ablauf von 6 Wochen noch die Möglichkeit hatte, auf die E-Mails (auf dem Zentralserver) zuzugreifen.

a) VG Frankfurt

Das VG Frankfurt argumentierte hier **juristisch:** Wenn die Daten nach der „Gesellschaftspolicy" gelöscht sein sollten, dann wären sie nicht mehr existent und seien nicht Gegenstand eines Vorlageanspruchs.

VG Frankfurt:

„Nach den Angaben der Klägerin steht (bzw. stand) bei ihr für die ein- und ausgehenden Mails ein zentraler Server zur Verfügung, auf dem die Mails zunächst verbleiben (bzw. verblieben), aber nach sechs Wochen gelöscht werden (bzw. wurden). Alle auf diesem zentralen Server am 30.9.2006 vorhandenen Mails waren also schon am 12.11.2006 gelöscht mit der Konsequenz, dass diese Mails aufgrund des Vorlageersuchens der Bundesanstalt vom 18.4.2007 nicht mehr vorgelegt werden konnten und nicht mehr vorgelegt werden brauchten und folglich eine Verletzung des Fernmeldegeheimnisses insoweit auch nicht mehr in Betracht kommen konnte."[118]

[116] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 9 (zitiert nach juris).
[117] Zu Definitionen des Arbeitnehmers siehe etwa § 5 Betriebsverfassungsgesetz.
[118] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 30 (zitiert nach juris).

b) VGH Kassel

Diese juristische Argumentation des VG Frankfurt hat den VGH Kassel aus zwei Gründen nicht überzeugt.

- Erstes juristisches Contraargument des VGH Kassel: Nichtigkeit des Verwaltungsakts

Wenn man dem VG Frankfurt folgte, dann wäre der Verwaltungsakt auf eine unmögliche Leistung gerichtet gewesen mit der Folge, dass der Verwaltungsakt insoweit nichtig und die Klage erfolgreich hätte sein müssen.

§ 44 VwVfG [Nichtigkeit des Verwaltungsakts] […]

(2) Ohne Rücksicht auf das Vorliegen der Voraussetzungen des Absatzes 1 ist ein Verwaltungsakt nichtig, […]

4.den aus tatsächlichen Gründen niemand ausführen kann; […].

VGH Kassel:

„[…] Wäre dem Erlass des Bescheides vom 18. April 2007 tatsächlich eine nicht wiederherstellbare Löschung sämtlicher von der Beklagten angeforderten E- Mails im innerbetrieblichen Netz der Klägerin vorangegangen, hätte die Klägerin der geforderten Leistung aus tatsächlichen Gründen mit der Rechtsfolge der Rechtswidrigkeit oder sogar Nichtigkeit des Verwaltungsakts (vgl. § 44 Abs. 2 Nr. 4 VwVfG) nicht nachkommen können, so dass der Klage unter diesen Voraussetzungen hätte stattgegeben werden müssen.[…]“[119]

Der VGH Kassel folgt so dem informationstechnologischen Vortrag der G, die ausführt, dass eben nicht gesichert sei, dass die Daten auf dem Server gelöscht seien bzw. wiederherstellbar sein bzw. irgendwo gespeichert seien:

- Informationstechnologisches Contraargument des VGH Kassel

Vorbringen der G, wie es im Beschluss des VGH Kassel[120] wiedergegeben ist:

„Die Klägerin trägt in der Begründung des Zulassungsantrags vor, **die Löschung einer E-Mail in der Datensicherung nach maximal sechs Wochen bedeute keineswegs, dass diese Mail endgültig aus dem System verschwunden sei. Die "E-Maildaten" (gemeint sind offenbar die im Eingangs- oder Ausgangspostfach abgelegten E-Mails) seien grundsätzlich dauerhaft auf dem Server gespeichert und würden erst durch entsprechenden Befehl des Nutzers im Postfach gelöscht. Gerade bei ausgehenden Mails sei den Mitarbeitern oft gar nicht mehr bewusst, welche E-Mails noch in ihrem Postfach existierten. Überdies sei die Löschung nicht mit einer unwiederbringlichen physikalischen Vernichtung der Daten gleichzusetzen.** Diese erfolge erst mit Überschreibung durch andere Daten auf dem Sicherungsband, was auch erst nach Ablauf von sechs Wochen der Fall sein könne **und letztlich von Zufällen abhängig sei**.“

[119] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 10 (zitiert nach juris).
[120] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 10 (zitiert nach juris).

Aufgrund dieser Argumentation und weil es unter diesen Umständen nicht einsehbar ist, warum G sich vor Gerichten gegen das Vorlageverlangen wehrt, wenn es nicht erfüllbar ist, geht das VGH Kassel von einer Zugriffsmöglichkeit der G auf die E-Mails der Arbeitnehmer aus. Es konzediert damit, dass die Arbeitnehmer nicht originären und exklusiven Zugang zu den E-Mail Daten haben – sie sich also nicht im alleinigen Herrschaftsbereich der Empfänger und Sender befinden.

VGH Kassel:

„[…] Unter Berücksichtigung dieses Vortrags konnte die Klägerin die Aufforderung der Beklagten zur Vorlage der gewünschten E-Mails auch nach Ablauf der Frist zur Aufbewahrung des gesicherten Datenbestandes auf dem Server noch befolgen, so dass der Bescheid der Beklagten vom 18. April 2007 in der Gestalt ihres Widerspruchsbescheides vom 18. Februar 2008 nicht auf eine aus tatsächlichen Gründen unmögliche Leistung gerichtet war.“[121]

Mit dieser informationstechnologischen Argumentation hätte die auf das BVerfG[122] gestützte Behauptung, dass das Fernmeldegeheimnis deswegen nicht durch Art. 10 GG, § 88 TKG geschützt sei, weil die Daten sich im exklusiven Herrschaftsbereich der Arbeitnehmer befänden, **scheitern müssen**.

So auch VG Frankfurt:

„Es ist zwar richtig, dass sich Mail-Dokumente nach einer Transaktion oder Speicherung innerhalb des betrieblichen Telekommunikationssystems durch den Berechtigten **auch weiterhin in gewisser Weise im Herrschaftsbereich des Arbeitgebers** befinden. […]“[123]

In dem Moment, in dem eine Kopie der Daten (oder die Daten) **auch** für G verfügbar ist, ist der exklusive Herrschaftsbereich des Arbeitnehmers über die Daten **nach hier vertretener Meinung nicht mehr zu bejahen** (hier so genannte **Duplizitätsratio**). Umso mehr als nach dem Vortrag der G nicht nur die Daten über die Zentralspeicherung potentiell auffindbar sind, sondern sich durch die Zugriffsmöglichkeiten der Systemadministratoren der G auf die Rechner der Arbeitnehmer eine Teilung des Herrschaftsbereichs zu bejahen ist.

FINT (Für Interessierte): Andere Literaturstimmen

Anders als die hier vertretene Duplizitätsratio will eine Literaturstimme je nach informationstechnologischer Organisation des E-Mails Systems unterscheiden:

„Je nach Art der E-Mail-Verwaltung im Unternehmen sind Sachverhalte denkbar, die Parallelen zu der Beschlagnahme beim Provider aufweisen. So ist es möglich, dass auf einem zentralen Server eine Zwischenspeicherung von Mails erfolgt, bevor die Mails in den Account des Mitarbeiters gelangen. Nach den Maßgaben des BVerfG stellt der Zugriff auf Mails, die auf einem zentralen Server zwischengespeichert sind, einen Eingriff in das

[121] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 10 (zitiert nach juris).
[122] Vgl. BVerfG, Urteil vom 02.03.2006, Az. 2 BvR 2099/04
[123] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 33 (zitiert nach juris) – das - nach hier vertretener Auffassung widersprüchlich – im Ergebnis Art. 10 GG ablehnt.

Fernmeldegeheimnis dar. Letztlich richtet sich damit die Rechtsnatur der E-Mail nach dem Zugriffsort: Die beim Provider (oder beim Arbeitgeber auf einem zentralen E-Mail-Server) zwischen- oder endgespeicherten Mails unterliegen dem Fernmeldegeheimnis; dieselben E-Mails, die sich im Mail-Account und /oder auf dem Endgerät des Nutzers/Arbeitnehmers befinden, stammen aus einem abgeschlossenen Kommunikationsvorgang und unterfallen daher dem Telekommunikationsgeheimnis nicht mehr.“[124]

Dagegen ist einzuwenden, dass – wenn man dem BVerfG zu Art. 10 GG folgen will - so nicht berücksichtigt wird, dass von vornherein oder im Nachhinein bei Arbeitnehmer-E-Mails nie Alleingewahrsam bestanden hat. Eine weitere Literaturstimme scheint auch die Eröffnung des Geltungsbereichs des Art. 10 GG zu bejahen:

„Sie (Anmerkung der Verfasserin: die den Entscheidungen VG Frankfurt und VGH Kassel zugrunde liegende Konstellation) unterscheidet sich jedoch insoweit, als es – im Gegensatz etwa zu einer Verwaltung der E-Mails auf dem Server eines Mailproviders – nicht in der Hand des Empfängers lag, die E-Mail zu löschen, denn der Arbeitgeber archivierte sie hier automatisch für einen gewissen Zeitraum. Bereits nach den vom BVerfG zur Abgrenzung des Fernmeldegeheimnisses entwickelten Grundsätzen würde ein Zugriff auf diese Daten einen Eingriff in Art. 10 Abs. 1 GG darstellen, denn die Kommunikationsinhalte erreichen aufgrund der konkreten Ausgestaltung des Netzwerks auch den Empfänger, bleiben aber zugleich auch in der Herrschaftsgewalt eines Dritten, des Arbeitgebers, der zuvor durch Bereitstellung des E-Mail-Systems zur privaten Nutzung an der Übermittlung mitwirkt. Hierfür spricht ebenfalls, dass die Aufzeichnung von Verbindungsdaten durch einen Dritten, der an der Kommunikationsübermittlung mitwirkt, in den Schutzbereich des Fernmeldegeheimnisses fällt; dies muss aber erst recht für eine Aufzeichnung der Kommunikationsinhalte gelten.“ [125]

2. Speicherung, Wiederherstellung der und Zugriff auf die E-Mails in der „originären Arbeitnehmersphäre“

Die G behauptet, dass sie Zugriff auf die Daten unter anderem der Arbeitsplatzrechner habe, und zwar räumlich wie technisch.

Vorbringen der G, wie es im Urteil des VGH Kassel wiedergegeben ist:

„Dem von der Klägerin als bedeutsam herausgehobenen Umstand, dass sich die von ihr herauszugebenden, auf den betrieblichen Arbeitsplatzrechnern und Servern gespeicherten E-Mails (auch) in ihrem technischen und räumlichen Herrschaftsbereich befinden, kommt keine maßgebliche Bedeutung zu. […]“[126]

Hier setzt der VGH Kassel mit seiner zweiten juristischen Argumentation an. Er stellt die gewagte These auf, dass die Arbeitnehmer über die Daten auf im Intranet vernetzten und durch vom bezeichneten Kommunikationsteilnehmer personenverschiedene Systemadministratoren organisierte, gesicherten Firmenrechnern absolut herrschen wie über ihre lokalen Rechner im häuslichen Bereich.

[124] Härting, in: CR 2009, S. 581, 584.
[125] Schantz: „Der Zugriff auf E-Mails durch die BaFin“, in: WM 2009, S. 2112, 2116
[126] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn.17 (zitiert nach juris).

VGH Kassel:

„[…] Es handelt sich insoweit nicht um den dem Fernmeldegeheimnis unterliegenden Herrschaftsbereich der Klägerin in ihrer (möglichen) Eigenschaft als Diensteanbieterin nach dem Telekommunikationsgesetz, sondern um den Herrschaftsbereich der Klägerin als Arbeitgeberin, die ihren Mitarbeitern die betrieblichen IT-Einrichtungen zur Speicherung von Kommunikationsdaten zur Verfügung stellt. Diese elektronischen Dokumente unterscheiden sich bezüglich der Reichweite des Fernmeldegeheimnisses letztlich nicht von solchen **Kommunikationsinhalten oder Verbindungsdaten, die der Kommunikationsteilnehmer auf seinem häuslichen Rechner empfängt, versendet und speichert**. […]“[127]

Dementsprechend schützen Art. 10 GG, § 88 TKG die Arbeitnehmer selbst dann nicht, wenn es keine originäre Arbeitnehmersphäre gibt und die Daten noch physisch im Kommunikationssystem des Unternehmens vorhanden sind.

VGH Kassel:

„Die von der Klägerin aufgeworfene Frage

"Schützt das Fernmeldegeheimnis die Mitarbeiter eines Unternehmens nur während der Übermittlung oder greift der Schutz bzw. die Verpflichtung des Unternehmens zur Wahrung des Fernmeldegeheimnisses auch nach Abschluss der Übermittlung ein, soweit sich die Daten noch physisch innerhalb des Kommunikationssystems des Unternehmens befinden?"

ist auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts im ersteren Sinne zu beantworten, ohne dass Besonderheiten des vorliegenden Falles Anlass zu einer weitergehenden Klärung geben würden.“[128]

Hervorzuheben ist, dass der VGH Kassel sich der Dupliziätsratio durchaus bewusst ist. So erkennt er, dass im Sachverhalt der oben präsentierten Entscheidung des BVerfG jedenfalls beim Provider eine Kopie der eingegangenen und versandten Mails verbleibt und deswegen der Herrschaftsbereich des Empfängers begrenzt ist:

VGH Kassel:

„Ein weiterer Klärungsbedarf besteht entgegen der Ansicht der Klägerin (…) auch nicht in Bezug auf die von dem Bundesverfassungsgericht in seinem Kammerbeschluss vom 29. Juni 2006 - 2 BvR 902/06 - als noch nicht abschließend geklärt bezeichnete Rechtsfrage, ob der Zugriff auf beim Diensteanbieter gespeicherte E-Mails in den Schutzbereich des Fernmeldegeheimnisses fallen. Bei der dieser Entscheidung zu Grunde liegenden Verfassungsbeschwerde geht es um den Zugriff von Ermittlungsbehörden auf E-Mails, die auf dem Server eines Kommunikationsunternehmens bzw. Serviceproviders (noch) gespeichert sind. **Damit sind Kommunikationsinhalte betroffen, die entweder den Herrschaftsbereich des Empfängers nicht oder noch nicht erreicht haben oder die auf den Zentralrechnern des Kommunikationsunternehmens bzw. Serviceproviders ohne**

[127] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn.17 (zitiert nach juris).
[128] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 20-22 (zitiert nach juris).

Zutun und Einwirkungsmöglichkeit des Empfängers nach der Übertragung als Duplikate verbleiben. […]“[129]

Der VGH sieht also, dass die „Arbeitnehmerdaten“ auch für den Arbeitgeber verfügbar sind (Duplizitätsratio). Dennoch soll sich der Sachverhalt der beim Provider zwischen- und endgespeicherten Mails (BVerfG-Fall) vom Arbeitgeberzugriff auf an die Arbeitnehmer gerichteten und von ihnen gesendete Mails (VGH-Fall) unterscheiden, weil dieser Zugriff immer nach Abschluss (des ersten) Übertragungsvorgangs erfolgt.

VGH Kassel:

„[…] Die auf Auswertung dieser Daten gerichteten Maßnahmen haben (noch) einen Bezug zu dem durch Art. 10 Abs. 1 GG geschützten Kommunikationsvorgang, betreffen also nicht, wie das hier der Fall ist, Inhalte von Daten, die erst in Folge der Speicherung durch den Empfänger nach Beendigung des Übertragungsvorgangs angefallen sind. […]“[130]

FÖR-Kritik:
Der VGH Kassel wählt so knapp einen Monat vor dem BVerfG einen Weg, der sich **hinsichtlich der Eröffnung des Geltungsbereichs von Art. 10 GG** unterscheidet. Auch bei E-Mails in Verfahrensphase 4 (nach der Endspeicherung beim Provider) ist der Übermittlungsvorgang abgeschlossen. **Hinsichtlich des Ergebnisses** ist die VGH-Entscheidung mit dem BVerfG vereinbar: auch es verlangt keine Einhaltung von § 88 Abs. 3 S. 3 TKG.

- Zweites juristisches Argument des VGH Kassel: E-Mails in der originären Arbeitnehmersphäre

Nachdem festgestellt ist, dass die E-Mail-Daten für die G nicht unauffindbar sind, bleibt dem VGH Kassel nur, den Herrschaftsbereich der Arbeitnehmer juristisch zu behaupten und die Eröffnung des Geltungsbereichs des Grundrechts auf informationelle Selbstbestimmung und Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (FÖR-Terminologie: Grundrecht auf „IT-Sicherheit“) (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) festzustellen.

So bereits VG Frankfurt:

„Die Klägerin hat weiterhin mitgeteilt, dass ihre Mitarbeiter die Möglichkeit haben (bzw. hatten), die Mails an eine andere Stelle zu kopieren und sie dort zu speichern oder zu archivieren, so etwa auf einem Rechner am Arbeitsplatz. Dies bedeutet jedoch, dass die Mitarbeiter hierzu ausdrücklich selbst aktiv werden müssen (bzw. mussten). Sobald aber Mail-Empfänger oder Mail-Versender ihre E-Mails aus dem eigentlichen Übertragungsvorgang herauslösen und sie selbst platzieren, speichern oder in anderer Weise verarbeiten, ist das Fernmeldegeheimnis nicht mehr betroffen. […]“[131]

„[…] Wenn der Berechtigte jedenfalls die eigene Entscheidung trifft, das Mail-Dokument an einer selbst gewählten Stelle im betrieblichen Telekommunikationssystem verbleiben zu

[129] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 23 (zitiert nach juris).
[130] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 23 (zitiert nach juris).
[131] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 31 (zitiert nach juris).

lassen, steht ihm dafür ein unbefristeter Schutz durch das Fernmeldegeheimnis nicht mehr zur Seite."[132]

VGH Kassel:

„[…] **Möglichen Rechtsbeeinträchtigungen, die den Mitarbeitern durch Datenverlust auf denZentralrechnern oder durch unberechtigten Zugriff der Klägerin selbst oder unbefugter Dritter auf den dort abgelegten Datenbestand drohen, wird nicht durch die Grundrechtsgewährleistung des Art. 10 Abs. 1 GG, sondern durch andere Grundrechte, wie das Recht auf informationelle Selbstbestimmung oder das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme begegnet** (vgl. BVerfG, Urteil vom 27. Februar 2008, a.a.O., Seite 302 ff.)."[133]

Ohne weitere Abwägung (RER-Prüfung) geht der VGH Kassel davon aus, dass Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dem Vorlageverlangen nicht entgegenstehen. Es berücksichtigt in seiner Entscheidung auch nicht einen möglichen wertpapierhandelsrechtlichen Wertungswiderspruch, der den in Teil 2 geschilderten Wertungswiderspruch der unangemessenen Behandlung von Inhalts- gegenüber Verkehrsdaten widerspiegelt.

III. Wertpapierhandelsrechtlicher Wertungswiderspruch?

1. Generalklausel und Spezialnorm für die „Organisation" von Verkehrsdaten

Das Wertpapierhandelsgesetz verfügt zum einen über die Generalklausel des hier ausgelegten § 4 Abs. 3 S. 1 WpHG und zum anderen über eine spezielle Ermächtigungsgrundlage zur Erhebung und Speicherung der Verkehrsdaten in § 16b Abs. 1 S. 1 WpHG. Hervorzuheben ist, dass nach der Kommentarliteratur[134] in § 16b Abs. 1 WpHG geschützte Verkehrsdaten nur dann **ausgewertet werden dürfen**, wenn die BaFin einen Staatsanwalt beizieht (FÖR-Interessenschema: Qualität des Verfahrens).

§ 4 Abs. 3 S. 1 WpHG [Aufgaben und Befugnisse]

(3) Die Bundesanstalt kann von jedermann Auskünfte, die Vorlage von Unterlagen und die Überlassung von Kopien verlangen sowie Personen laden und vernehmen, soweit dies auf Grund von Anhaltspunkten für die Überwachung der Einhaltung eines Verbots oder Gebots dieses Gesetzes erforderlich ist.

§ 16b WphG [Aufbewahrung von Verbindungsdaten]

(1) Die Bundesanstalt kann von einem Wertpapierdienstleistungsunternehmen sowie von einem Unternehmen mit Sitz im Inland, die an einer inländischen Börse zur Teilnahme am Handel zugelassen sind, und von einem Emittenten von Insiderpapieren sowie mit diesem verbundenen Unternehmen, die ihren Sitz im Inland haben oder deren Wertpapiere an einer inländischen Börse zum Handel zugelassen oder in den regulierten Markt oder Freiverkehr einbezogen sind, für einen bestimmten Personenkreis schriftlich die **Aufbewahrung**

[132] VG Frankfurt, Urteil vom 06.11.2008 Az.: 1 K 628/08.F, Rn. 33 (zitiert nach juris).
[133] VGH Kassel, Beschluss vom 19.05.2009, Az. 6 A 2672/08.Z, Rn. 17 (zitiert nach juris).
[134] Dreyling, in: Assmann/Schneider, WpHG, 2009, § 16b Rn. 4.

von bereits existierenden Verbindungsdaten über den Fernmeldeverkehr verlangen, sofern bezüglich dieser Personen des konkreten Unternehmens Anhaltspunkte für einen Verstoß gegen § 14 oder § 20a bestehen. **Das Grundrecht des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt.** Die Betroffenen sind entsprechend § 101 Abs. 4 und 5 der Strafprozessordnung zu benachrichtigen. Die Bundesanstalt kann auf der Grundlage von Satz 1 nicht die Aufbewahrung von erst zukünftig zu erhebenden Verbindungsdaten verlangen.

(2) Die **Frist zur Aufbewahrung** der bereits existierenden Daten beträgt vom Tage des Zugangs der Aufforderung an **höchstens sechs Monate**. Ist die Aufbewahrung der Verbindungsdaten über den Fernmeldeverkehr zur Prüfung des Verdachts eines Verstoßes gegen ein Verbot nach § 14 oder § 20a nicht mehr erforderlich, hat die Bundesanstalt den Aufbewahrungspflichtigen hiervon unverzüglich in Kenntnis zu setzen und die dazu vorhandenen Unterlagen unverzüglich zu vernichten. Die Pflicht zur unverzüglichen Vernichtung der vorhandenen Daten gilt auch für den Aufbewahrungspflichtigen.

Wie in der StPO in der „Auslegung" des BVerfG existiert also im WpHG in der „Auslegung" der hessischen Rechtsprechung ein ausdrücklich (grammatische Auslegung)

- **spezieller und**
- **höherer Schutz**

der Verkehrsdaten (andere Terminologie „Verbindungsdaten) gegenüber den Inhaltsdaten. Dies ist umso weniger überzeugend als E-Mails auch Verkehrsdaten (Zeitpunkt…) enthalten. Diesem Zwischenbefund ist allerdings in einer normenhierarchischen Betrachtung entgegenzuhalten, dass vielleicht das Europarecht zu der von VGH und VG gewählten Auslegung zwingen könnte.

2. Europarechtskonforme Auslegung von § 4 Abs. 3 S. 1 WpHG?

§ 4 Abs. 3 S. 1 WpHG dient ausweislich der Gesetzesbegründung (historische Auslegung)[135] der Umsetzung einer europäischen Richtlinie.

Art. 249 Abs. 3 EG (Vertrag zur Gründung der Europäischen Gemeinschaft)

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Zieles verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

Art. 12 Abs.- 2 lit d RL 2003/6 EG („Marktmissbrauchsrichtlinie")

(2) Unbeschadet des Artikels 6 Absatz 7 werden die in Absatz 1 des vorliegenden Artikels genannten Befugnisse im Einklang mit dem innerstaatlichen Recht ausgeübt und beinhalten zumindest das Recht,

[…]

d) bereits existierende Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern, […].

[135] Bundestagsdrucksache 15/3174 vom 24.05.2004, S. 30.

Grundsätzlich ist damit zu fragen, ob nicht höherrangiges Recht verlangt, dass § 4 Abs. 3 S. 1 WpHG extensiv ausgelegt wird. Von der Aufsatzliteratur wird dem entgegengehalten, dass der Gesetzgeber bei der Umsetzung europäischer Richtlinien nicht von der Beachtung deutschen Verfassungsrechts dispensiert sei.[136]

FINT (Für Interessierte): FÖR-Pragmatik
Die Aufarbeitung der grundrechtlichen Spielräume bei der Umsetzung von europäischen Richtlinienrecht bzw. die Konsequenzen der Verfassungswidrigkeit sogenannter ausbrechender Rechtsakte (unter anderem in der Lissabon-Entscheidung[137]) ist Gegenstand eines weitern in Vorbereitung befindlichen CyLaw-Reports zur Vorratsdatenspeicherung. Ganz grundsätzlich ist nur die Information zu geben, dass die deutsche Verfassung in Art. 23 Abs. 1 S. 1 GG keinen identischen Grundrechtsschutz im deutschen wie im europäischen Recht verlangt – sondern einen „nur" im wesentlichen vergleichbaren.

Art. 23 Abs. 1 S. 1 GG [Verwirklichung der Europäischen Union; Beteiligung des Bundesrates, der Bundesregierung]
(1) Zur Verwirklichung eines vereinten Europas wirkt die Bundesrepublik Deutschland bei der Entwicklung der Europäischen Union mit, die demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiarität verpflichtet ist und einen diesem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet.

3. Generalklausel und Spezialnorm – Zitiergebot

Festzuhalten ist des Weiteren, dass sich § 16b Abs. 1 S. 2 WpHG und § 4 Abs. 3 WpHG hinsichtlich der Wahrung des Zitiergebots (Art. 19 Abs. 1 S. 2 GG und § 88 Abs. 3 S. 3 TKG) unterscheiden. Evident ist, dass der Gesetzgeber gesehen hat, dass **bereits die Aufbewahrung** von Verkehrsdaten Bezug zu Art. 10 Abs. 1GG hat. Warum darüber hinaus der gleiche Gesetzgeber bei der Aufbewahrung und Herausgabe **von Verkehrs- und Inhaltsdaten** (E-Mails) keinen Bezug zu Art. 10 Abs. 1 GG haben soll, bleibt ohne Erklärung durch die hessischen Gerichte.

IV. Fazit

VG Frankfurt und VGH Kassel haben sich mit einem höchst praxisrelevanten Fall – nämlich der Frage des Zugriffs der Arbeitgeber auf Arbeitnehmer E-Mails – befasst. Nach im Schrifttum bisher überwiegend vertretener Auffassung[138] wird der Arbeitgeber, der die Privatnutzung von dienstlichen E-Mail-Adressen gestattet, zum Diensteanbieter (§ 3 Nr. 6 TKG) und muss das Fernmeldegeheimnis wahren (Art. 10 GG, § 88 TKG). Nach der Rechtsprechung des VGH Kassel endet dieses Fernmeldegeheimnis mit der Kenntnisnahme des Arbeitneh-

[136] Schantz, in: WM 2009, 2112, 2117 m.w.N.
[137] BVerfG, Urteil vom 30.06.2009, Az.: 2 BvE 2/08 – 2 BvE 5/08 – BvR 1010/08 – 2 BvR 1022/08 – 2 BvR 1259/08 – 2 BvR 1259/09, Rn. 240.
[138] Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, Kommentar 2008, § 88 TKG, Rn. 18; Robert, in: Beck'scher TKG-Kommentar, 3. Auflage 2006, § 91 TKG, Rn. 9; Mengel: „ Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz", in: BB 2004, S. 2014, 2017.

mers. Der Schutz der Arbeitnehmer vor Zugriffen des Arbeitgebers soll durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleisten werden. Diese neue Verortung des Schutzes der privaten E-Mails, die bei jedem Zugriff des Arbeitgebers auf den E-Mailaccount bzw. die Daten der Arbeitnehmer involviert sein könnte, hat zur Konsequenz, dass das spezialgesetzliche Zitiergebot des § 88 Abs. 3 S. 3 TKG bzw. Art. 10 Abs. 1 S. 2 GG hinsichtlich der Ermächtigungsgrundlage nicht mehr zu beachten ist. Dieses Ergebnis vereint die Rechtsprechung des BVerfG wie des VGH – wenn sie zu diesem Ergebnis auch auf unterschiedlichem Wege kommen: das BVerfG trotz der Anwendung von Art. 10 GG und der VGH wegen der Anwendung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Teil 6: Anhang - Dynamik der Gesetzgebung zur Surveillance am Beispiel von § 100a StPO

FÖR-Hintergrund: Dynamik der Gesetzgebung bei der Telekommunikationsüberwachung – ein Beleg für die Notwendigkeit der Aktualisierung der Rechtsgrundlagen im Cyberlaw

Die Ermächtigungsgrundlage für die Telekommunikationsüberwachung ist **allein** in den Jahren 2005 bis 2009 sechsmal geändert worden. Im Wesentlichen wurde der Katalog der Straftaten, bei deren Verfolgung Telekommunikationsüberwachung eingesetzt werden darf, erweitert und verändert Darüber hinaus trug der Gesetzgeber auch dem vom BVerfG in der Entscheidung zur akustischen Wohnraumüberwachung (CyLAW-Report XVI) geforderten Schutz des absolut geschützten Kernbereichs privater Lebensgestaltung Rechnung (1.1.2008). Insgesamt sind bereits diese Änderungen Beleg für die FÖR-These, dass im Cyberlaw Aktualität der Recherche zu fordern ist.

Änderungen von § 100a StPO: Zeitraum 1.1.2005 bis 04.08.2009

I. Geltungszeitraum 19.02.2005 bis 29.11.2007 (BGBl. I S. 239)

- Änderung in S. 1 Nr. 2: bisheriger § 181 Abs. 1 Nr. 2, 3 StGB (schwerer Menschenhandel) wird mit seiner Aufhebung aus dem Straftatenkatalog herausgenommen; dafür Einfügung der neuen §§ 232 Abs. 3, 4, 5, 233 Abs. 3 StGB (Menschenhandel zum Zweck der sexuellen Ausbeutung bzw. zur Ausbeutung der Arbeitskraft), soweit es sich um Verbrechen handelt

II. Geltungszeitraum 30.11.2007 bis 31.12.2007 (BGBl. I S. 2614)

- Änderung von S. 1 Nr. 1e): Straftaten gegen die Sicherheit der im Land Berlin anwesenden Truppen einer der Drei Mächte werden aus dem Straftatenkatalog herausgenommen; Änderung des Klammerzusatzes in S. 1 Nr. 1e): anstatt bisher §§ 16, 17 des Wehrstrafgesetzes in Verbindung mit Art. 7 des Vierten Strafrechtsänderungsgesetzes, jetzt §§ 16, 17 des Wehrstrafgesetzes in Verbindung mit § 1 des NATO-Truppen-Schutzgesetzes.

III. Geltungszeitraum 01.01.2008 bis 18.03.2008 (BGBl. I S. 3198)

Neuer Abs. 1 :

- Einfügung der Voraussetzung in Abs. 1 Nr. 2: „Tat auch im Einzelfall schwer wiegt“,
- jetziger Abs. 1 Nr.3) vorher: S. 1 letzter HS..

Neuer Abs. 2 enthält die Katalogtaten:

- **neue Katalogtat** in Abs. 2 Nr. 1b): Abgeordnetenbestechung,
- **neue Katalogtat** aus dem Bereich der Sexualdelikte in Abs. 2 Nr. 1f): „Straftaten gegen die sexuelle Selbstbestimmung in Fällen von §§ 176a, 176b, 177 Abs.2 Nr. 2 StGB“, vorher in S. 1 Nr. 1a) als Katalogtaten nur: § 176 a I-III, 176 b StGB (sexueller Missbrauch von Kindern ohne/mit Todesfolge,
- **neue Katalogtat** in Abs. 2 Nr. 1g): Verbreitung, Erwerb und Besitz von kinderpornografischen Schriften nach § 184 b Abs.1 bis 3 StGB,
- **neue Katalogtaten** in Abs. 2 Nr. 1n): Betrug und Computerbetrug unter den in § 263 Abs. 3 S. 2 StGB genannten Vss (Regelbeispiele für besonders schwere Fälle) und im Fall des § 263 V StGB (gewerbsmäßiger Bandenbetrug),
- **neue Katalogtaten** in Abs. 2 Nr. 1o): Regelbeispiele für Subventionsbetrug in besonders schwerem Fall und gewerbsmäßiger Bandensubventionsbetrug,
- **neue Katalogtaten** in Abs.2 Nr. 1p): bestimmte Urkundenfälschungsdelikte,
- **neue Katalogtat** in Abs. 2 Nr. 1q): Regelbeispiele für Bankrott in besonders schwerem Fall,
- **neue Katalogtat** in Abs. 2 Nr. 1s): bestimmte Straftaten gegen den Wettbewerb,
- gemeingefährliche Straftaten jetzt in Abs. 2 Nr.1s), vorher: S.1 Nr.2,
- **neue Katalogtaten** in Abs. 2 Nr. 1t): Bestechlichkeit und Bestechung,
- **neue Katalogtaten** in Abs. 2 Nr. 2 a) bis c): bestimmte Straftaten aus der Abgabeordnung,
- **neue Katalogtaten** in Abs. 2 Nr. 3: bestimmte Straftaten aus dem Arzneimittelgesetz,
- Straftaten aus dem Asylverfahrensgesetz jetzt in Abs. 2 Nr. 4a) – b), vorher: S. 1 Nr.5,
- Straftaten aus dem Aufenthaltsgesetz jetzt in Abs. 2 Nr. 5, vorher S. 1 Nr. 5,
- Straftaten aus dem Außenwirtschaftsgesetz jetzt in Abs. 2 Nr. 6, vorher S. 1 Nr. 3,
- Straftaten aus dem Betäubungsmittelgesetz jetzt in Abs. 2 Nr. 7, , vorher S. 1 Nr. 4,
- **neue Katalogtat:** Straftat nach § 29 Abs. 1 Grundstoffüberwachungsgesetz unter den Vss von § 29 Abs. 3 S. 2 Grundstoffüberwachungsgesetz,
- Straftaten aus dem Gesetz über die Kontrolle von Kriegswaffen jetzt in Abs. 2 Nr. 9a) – b), vorher: S. 1 Nr. 3,
- **neue Katalogtaten**: Straftaten aus dem Völkerstrafgesetzbuch in Abs. 2 Nr. 10 a) – c),
- Straftaten aus dem Waffengesetz jetzt in Abs. 2 Nr. 11 a) – b), vorher S. 1 Nr. 3.

Neuer Abs. 3 (Adressaten der Maßnahme) vorher § 100a S.2.

Neuer Abs. 4: Regelung zum Kernbereich privater Lebensgestaltung.

Mit diesem Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007, das zum 01.01.2008 in Kraft getreten ist, ist § 100a StPO inhaltlich und strukturell stark verändert worden.

§100a StPO [Überwachung der Telekommunikation]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1.bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2.die Tat auch im Einzelfall schwer wiegt und
3.die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.
(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:
1.aus dem Strafgesetzbuch:
[…]
(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.
(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

Zu den schon bisher geltenden Eingriffsvoraussetzungen kommt nach § 100a Abs. 1, Nr.2 StPO hinzu, dass die Tat im (konkreten) Einzelfall schwer wiegen muss. Inhaltlich geändert wurde auch der Straftatenkatalog.

IV. Geltungszeitraum 19.03.2008 – 04.11.2008 (BGBl. I S. 306)

- Änderung in Abs. 2 Nr. 8: jetzt: Straftaten nach § 19 Abs. 1 Grundstoffüberwachungsgesetz unter den Vss. des § 19 Abs.3 S.2 Grundstoffüberwachungsgesetz.

V. Geltungszeitraum 05.11.2008 – 03.08.2009 (BGBl. I S. 2149)

- **neue Katalogtaten** in Abs. 2 Nr. 1g): vorher Verbreitung, Erwerb und Besitz kinderpornografischer Schriften, jetzt auch § 184 c Abs. 3 StGB: gewerbsmäßige(r) oder bandenmäßige(r) Verbreitung, Erwerb und Besitz jugendpornografischer Schriften.

VI. Geltungszeitraum ab 04.08.2009 (BGBl. I S. 2437)

- **neue Katalogtat** in Abs. 2 Nr. 1a) mit § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat)