



Universität Hannover  
Sommersemester 2001 / Wintersemester 2001/2002

## **Abschlußarbeit**

### **Rechtliche Fragen der Überwachung der modernen elektronischen Kommunikation**

Dargestellt am Beispiel der Kommunikation  
per Electronic Mail

von

**Harald Schoen**

## Inhaltsverzeichnis

<b>Literaturverzeichnis</b>	<b>V</b>
<b>Einführung</b>	<b>1</b>
I. Problemstellung	1
II. Eingrenzung der Untersuchung	2
III. Konzept und Aufbau der Arbeit	3
<b>A. Charakteristik und Technik der Kommunikation per E-Mail</b>	<b>4</b>
I. Kennzeichen des E-Mail-Dienstes	4
II. Technische Grundlagen	5
1. Datenübertragung im Internet	5
2. Die Basisprotokolle TCP und IP	6
3. Domain-Namen	8
4. Die Technik des E-Mail-Dienstes	8
5. Der Zugang zum Internet	10
6. Logdateien	11
III. Rollen in der E-Mail-Kommunikation	12
<b>B. Ansatzpunkte für die Überwachung</b>	<b>13</b>
I. Ziele und Vorgehensweisen bei Ermittlungen	14
II. Zugriff auf Inhalte von E-Mails	15
III. Identifizierung der Kommunikationsteilnehmer	16
1. Informationsquellen	16
2. Umsetzung der IP-Adresse in Personendaten	17
<b>C. Der Schutz der E-Mail-Kommunikation durch die Grundrechte</b>	<b>18</b>
I. Art. 10 Abs. 1 GG	20
1. Schutzbereich	20
2. Medium E-Mail	22
3. Schutz der Inhalte von E-Mails	23
4. Schutz von Verbindungsdaten	27
5. Eingriffscharakter strafprozessualer Maßnahmen	29

II.	Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG	30
	1. Schutzbereich	30
	2. Eingriffscharakter strafprozessualer Maßnahmen	31
III.	Art. 5 Abs. 1 GG	32
IV.	Art. 13 Abs. 1 GG	33
	1. Schutzbereich	33
	2. Eingriffscharakter strafprozessualer Maßnahmen	35
V.	Weitere Grundrechte	38
	1. Art. 12 Abs. 1 GG	38
	2. Art. 14 Abs. 1 GG	39
	3. Art. 2 Abs. 1 GG	39
VI.	Verhältnis der beeinträchtigten Grundrechte	40
	1. Verschaffen der Zugriffsmöglichkeit	40
	2. Zugriff auf E-Mail-Inhalte, Verbindungs- und Bestandsdaten	41
VII.	Zusammenfassung	42
<b>D.</b>	<b>Die Zulässigkeit staatlichen Hackings</b>	<b>43</b>
I.	Prüfungsmaßstab Art. 13 GG	44
II.	Durchsuchung (§§ 102, 103 StPO)	45
III.	Beobachtung (§ 100c StPO)	46
IV.	Verdeckter Ermittler (§ 110a, 110c StPO)	47
V.	Überwachung der Telekommunikation (§§ 100a, 100b StPO)	48
VI.	Beschlagnahme und Postbeschlagnahme (§§ 94, 99 StPO)	50
VII.	Zusammenfassung	51
<b>E.</b>	<b>Der Zugriff auf Inhalte von E-Mails</b>	<b>52</b>
I.	Gesetzesvorbehalte	52
II.	Überwachung der Telekommunikation (§§ 100a, 100b StPO)	53
III.	Beschlagnahme (§ 94 StPO)	54
IV.	Postbeschlagnahme (§ 99 StPO)	55
V.	Durchsuchung (§§ 102, 103 StPO)	57
VI.	Beobachtung (§ 100c StPO)	58
VII.	Verdeckter Ermittler (§§ 110a, 110c StPO)	58
VIII.	Zusammenfassung	59

<b>F.</b>	<b>Der Zugriff in den einzelnen Phasen der Übermittlung</b>	<b>60</b>
I.	E-Mails auf dem PC des Absenders	60
	1. Zugriff nach § 100a StPO	61
	2. Zugriff nach § 94 StPO	61
II.	Übertragung der E-Mails zum Mail-Server des Empfängers	65
	1. Zugriff nach § 100a StPO	65
	2. Zugriff nach § 94 StPO	66
III.	Nachrichten auf dem Mail-Server des Empfängers	66
	1. Zugriff nach § 100a StPO	66
	2. Zugriff nach § 94 StPO	77
IV.	Abrufen der E-Mails vom Mail-Server durch den Empfänger	82
V.	Nachrichten auf dem PC des Empfängers	82
VI.	Zusammenfassung	83
<b>G.</b>	<b>Die Identifizierung der Kommunikationsteilnehmer</b>	<b>84</b>
I.	Kommunikationsdaten und ihre Grundrechtsrelevanz	84
	1. Arten von Kommunikationsdaten	84
	2. Quellen für Verbindungs- und Bestandsdaten	86
II.	Vorbemerkung zu den Eingriffsbefugnissen	87
	1. Relevante Normen	87
	2. Verschaffen der Zugriffsmöglichkeit	88
	3. Gesetzesvorbehalte	89
III.	E-Mails auf dem PC des Empfängers	89
	1. Zugriff nach § 94 StPO	89
	2. Sonstige Eingriffsbefugnisse	90
IV.	E-Mails auf dem Mail-Server des Empfängers	90
	1. Zugriff nach § 100a StPO	90
	2. Zugriff nach § 94 StPO	91
	3. Auskunftsanspruch nach § 100g Abs. 1 StPO	91
	4. Auskunftsanspruch nach § 89 Abs. 6 TKG	92
V.	Logdateien der Diensteanbieter	93
	1. Zugriff nach § 100a StPO	93
	2. Zugriff nach § 94 StPO	94
	3. Auskunftsanspruch nach § 100g Abs. 1 StPO	94
	4. Auskunftsansprüche nach §§ 89 Abs. 6 und 90 TKG	95

VI.	Kundendateien der Diensteanbieter	95
	1. Zugriff nach § 100a StPO	95
	2. Auskunftsanspruch nach § 100g Abs. 1 StPO	96
	3. Auskunftsanspruch nach § 89 Abs. 6 TKG	96
	4. Auskunftsanspruch nach § 90 TKG	98
	5. Zugriff nach § 94 StPO	98
VII.	Zusammenfassung	99
<b>H.</b>	<b>Zusammenfassung und Ausblick</b>	<b>101</b>
I.	Ergebnisse der Untersuchung	101
II.	Die Notwendigkeit einer gesetzlichen Neuregelung	102

## Literaturverzeichnis

- Bär*, Der Zugriff auf Computerdaten im Strafverfahren, Köln 1992  
– zitiert: *Bär*, Computerdaten –
- , Strafverfahrensrechtliche Aspekte der Online-Kommunikation, in: *Kröger/Gimmy* (Hg.), Handbuch zum Internetrecht: Electronic Commerce – Informations-, Kommunikations- und Mediendienste, Berlin 2000  
– zitiert: *Bär*, Online-Kommunikation –
- , Anmerkung zum Beschluß des LG Hanau vom 23. September 1999, in: MMR 2000, 176  
– zitiert: *Bär*, Anmerkung –
- Germann*, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000
- Gundermann*, Polizeilicher Zugriff auf Telekommunikationsdaten. Rechtsgrundlagen – Problembereiche – Entwicklungen, in: DuD 1999, 681
- Irlbeck*, Computer-Lexikon. Das Nachschlagewerk zum Thema EDV, München 3. Aufl. 1998
- Jarass/Pieroth*, Grundgesetz für die Bundesrepublik Deutschland. Kommentar, München 5. Aufl. 2000
- Kleine-Voßbeck*, electronic mail und Verfassungsrecht, Marburg 2000
- Kleinknecht/Meyer-Goßner*, Strafprozeßordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, München 45. Aufl. 2001
- Köhntopp/Köhntopp*, Datenspuren im Internet, in: CR 2000, 248
- Kudlich*, Der heimliche Zugriff auf Daten in einer Mailbox: Ein Fall der Überwachung des Fernmeldeverkehrs? – BGH, NJW 1997, 1934, in: JuS 1998, 209  
– zitiert: *Kudlich*, Mailbox –
- , Strafprozessuale Probleme des Internet. Rechtliche Probleme der Beweisgewinnung in Computernetzen, in: JA 2000, 227  
– zitiert: *Kudlich*, Strafprozessuale Probleme –
- Lemcke*, Die Sicherstellung nach § 94 StPO und deren Förderung durch die Inpflichtnahme Dritter als Mittel des Zugriffs auf elektronisch gespeicherte Daten, Frankfurt a.M. 1995

- Lindemann/Immler/Harms*, Internet intern. Technik – Trends – Programmierung, Düsseldorf 2. Aufl. 2000
- Meseke*, Ermittlungen im Internet – Positionen und Dissonanzen, in: *Kriminalistik* 2000, 245
- von *Münch/Kunig* (Hg.), Grundgesetz-Kommentar, Band 1, München 5. Aufl. 2000  
– zitiert: von *Münch/Kunig-Bearbeiter* –
- Palm/Roy*, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, in: *NJW* 1996, 1791  
– zitiert: *Palm/Roy*, Mailboxen –
- , Der BGH und der Zugriff auf Mailboxen [Besprechung von BGH CR 1996, 488], in: *NJW* 1997, 1904  
– zitiert: *Palm/Roy*, Anmerkung –
- Pieroth/Schlink*, Grundrechte. Staatsrecht II, Heidelberg 16. Aufl. 2000
- Rachor*, Kapitel F. Das Polizeihandeln, in: *Lisken/Denninger* (Hg.), Handbuch des Polizeirechts, München 2. Aufl. 1996
- Scheller/Boden/Geenen/Kampermann*, Internet: Werkzeuge und Dienste. Von “Archie” bis “World Wide Web”, Berlin 1994
- Sieber*, Teil 19. Strafrecht und Strafprozeßrecht, in: *Hoeren/Sieber* (Hg.), Handbuch Multimedia-Recht, München Loseblatt (Stand Februar 2000)
- Wuermeling/Felixberger*, Staatliche Überwachung der Telekommunikation, in: *CR* 1997, 555

## Einführung

### I. Problemstellung

Schon bei einer flüchtigen Betrachtung von Technik und Verfahren der Kommunikation wird deutlich, wie sehr sich diese in den letzten Jahrzehnten gewandelt haben. Standen als Kommunikationsmittel noch Anfang der 80er Jahre hauptsächlich nur Brief und stationäres Telefon zur Verfügung, so sind heute Dialog und Übermittlung von Nachrichten auf vielfältigen Wegen möglich, die teils auf der Weiterentwicklung bestehender, teils auf der Einführung neuartiger Techniken beruhen. So ist spätestens seit Anfang der 90er Jahre die Übermittlung schriftlicher Dokumente per Telefax eine übliche Kommunikationsform geworden. Ähnliches gilt für den Mobilfunk, der es erlaubt, von praktisch jedem beliebigen Ort Telefongespräche zu führen und Daten zu übertragen.

Herausragende Entwicklung der heutigen Zeit ist die Verbreitung des Internet mit seinem breiten Angebot an Kommunikationsmöglichkeiten. Eine der Grundfunktionen des Internet ist dabei die schnelle Übermittlung von elektronischen Nachrichten an einen bestimmten Empfänger (E-Mail), die wesentlich zu seiner Popularität beiträgt. Heute haben mehr als 40% der deutschen Bevölkerung geschäftlich oder privat Zugang zum Internet.<sup>1</sup> Da ein Internet-Zugang in der Regel auch zum Versand von E-Mail verwendet wird,<sup>2</sup> bedeutet dies, daß Millionen Bundesbürger bereits über ein elektronisches Postfach verfügen.

---

<sup>1</sup>“27 Millionen Deutsche nutzen das Internet”, Frankfurter Allgemeine Zeitung vom 21. August 2001, S. 15.

<sup>2</sup>Nach *Kleine-Voßbeck*, S. 12, benutzen etwa 96% aller Internet-Nutzer den E-Mail-Dienst.

Angesichts der enormen Bedeutung, die diese moderne Art der Kommunikation damit inzwischen erlangt hat, stellt sich die Frage, wie der Staat darauf reagiert. Auf staatlicher Seite bestehen verschiedene Interessen, Inhalt und Teilnehmer der Kommunikation zu überwachen. Zum einen sollen die Geheimdienste zur Erfüllung ihrer Aufgaben, insbesondere zum Schutz der staatlichen Ordnung, Zugriff auf diese Daten haben. Vor allem aber wird die Überwachung von Kommunikation als Mittel zur Aufklärung und Verfolgung von Straftaten eingesetzt.

Die naheliegenden gesetzlichen Grundlagen, die staatliches Handeln im Bereich der E-Mail-Kommunikation ermöglichen könnten, sind allerdings zum großen Teil schon vor Jahrzehnten formuliert worden.<sup>3</sup> Daher soll im folgenden untersucht werden, ob und wieweit diese Regelungen auf die moderne Kommunikationsform E-Mail überhaupt angewendet werden können und inwiefern sich Parallelen zu den herkömmlichen Kommunikationsformen Brief und Telefon ziehen lassen.

## **II. Eingrenzung der Untersuchung**

Die vorliegende Arbeit wird sich dabei auf den Aspekt des Zugriffs zu strafprozessualen Zwecken beschränken. Außer Betracht bleiben damit Eingriffsbefugnisse zu präventiven Zwecken, wie sie im Artikel 10-Gesetz und im Außenwirtschaftsgesetz vorgesehen sind. Hinsichtlich des betroffenen Personenkreises stehen Privatpersonen als Absender und Empfänger von Nachrichten im Vordergrund. Anbieter von Internet-Diensten, insbesondere Betreiber von Mail-Servern, werden behandelt, soweit es um die Befugnis der Strafverfolgungsbehörden geht, ohne deren Kenntnis in Compu-

---

<sup>3</sup> Beispielsweise wurden die §§ 100a und 100b StPO zur Regelung der Telefonüberwachung bereits 1968 durch das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (BGBl 1968 I, 949) eingeführt.

tersysteme einzudringen oder von ihnen Auskünfte über Umstände der Telekommunikation und Kundendaten zu verlangen.

Im wesentlichen nicht erörtert wird dagegen die rechtliche Stellung der Diensteanbieter bei der Durchführung der Maßnahmen, insbesondere die Verpflichtung nach § 88 TKG, die erforderlichen technischen Einrichtungen zu gestalten und vorzuhalten; ihre Erörterung würde den Rahmen der Arbeit sprengen. Gleiches gilt für Fragen der Zuständigkeit bei Ermittlungen im Internet sowie den Rechtsschutz gegen Maßnahmen.

Die rechtlichen Probleme, die aus der Verwendung moderner Kommunikationstechniken wie E-Mail erwachsen, hängen sehr eng mit deren Technik zusammen. Dabei sind im Laufe der Zeit verschiedene technische Varianten entstanden, die zum Teil zu unterschiedlichen rechtlichen Fragestellungen und Lösungsansätzen führen können. Im Rahmen dieser Arbeit kann nicht auf alle diese technischen Entwicklungen eingegangen werden. Den rechtlichen Erörterungen werden vielmehr die heute typischerweise verwendeten Konstellationen zugrunde gelegt, wie sie im Abschnitt A. beschrieben sind.

### **III. Konzept und Aufbau der Arbeit**

Bevor auf Rechtsfragen eingegangen wird, soll zunächst ein Überblick über Charakteristika und technischen Ablauf der E-Mail-Kommunikation gegeben werden (Abschnitt A.). Daran schließt sich eine Beschreibung der naheliegenden Ermittlungsansätze im Bereich des E-Mail-Verkehrs an (B.).

Ausgangspunkt für die juristischen Fragestellungen ist der Gedanke, daß strafprozessuale Maßnahmen grundrechtsdogmatisch nicht anders zu behandeln sind als staatliches Handeln auf dem

Gebiet des öffentlichen Rechts, etwa des Polizeirechts. In Kapitel C. werden daher die Schutzbereiche verschiedener Grundrechte in bezug auf das Medium E-Mail bestimmt und die Eingriffsqualität naheliegender Maßnahmen untersucht. Dabei geht es zum einen um den Zugriff auf E-Mails selbst, zum anderen um das Verschaffen der Zugriffsmöglichkeit, insbesondere durch “staatliches Hacking”, also das Eindringen in Computersysteme ohne Zustimmung des Berechtigten.

Die Abschnitte D. bis G. behandeln diejenigen Bestimmungen, die zur Rechtfertigung der festgestellten Grundrechtseingriffe dienen können. Zunächst geht es dabei um das “staatliche Hacking” (D.). Rechtsnormen zum Zugriff auf Inhalte von E-Mails beschreibt überblicksartig Abschnitt E.; im Abschnitt F. werden einzelne Normen im Detail untersucht. Daran schließt sich die Erörterung der Identifizierung der Kommunikationsteilnehmer durch Zugriff auf Verbindungs- und Bestandsdaten an (G.).

Den Abschluß bilden eine Zusammenfassung der Ergebnisse sowie eine Begründung, warum eine gesetzliche Neuregelung erforderlich erscheint (H.).

## **A. Charakteristik und Technik der Kommunikation per E-Mail**

### **I. Kennzeichen des E-Mail-Dienstes**

Die Übermittlung elektronischer Post ist eine der ältesten Dienstleistungen des Internet, die bereits 1972 entwickelt wurde.<sup>4</sup> Mit diesem Dienst kann eine einzelne Person Mitteilungen an eine

---

<sup>4</sup>Lindemann/Immler/Harms, S. 99.

oder mehrere bestimmte andere Personen senden, wobei die Mitteilung im Prinzip nur den jeweiligen Empfängern zugänglich ist. E-Mail ist damit, anders als z.B. der Dienst des World Wide Web, dem Bereich der Individualkommunikation zuzuordnen.<sup>5</sup> Dies gilt selbst dann, wenn eine E-Mail an eine sehr große Zahl von Empfängern verschickt wird, da auch in diesem Fall noch ein abgrenzbarer Kreis von Personen existiert.<sup>6</sup>

## **II. Technische Grundlagen**

Für das Bewußtsein und das Verständnis von rechtlichen Problemen, die sich bei der Überwachung der E-Mail-Kommunikation im Internet ergeben können, ist es äußerst bedeutsam, die technischen Abläufe beim Versand von E-Mails zu kennen. Da E-Mail jedoch nur einer der Kommunikationsdienste des Internet ist, baut er auf allgemein im Internet verwendeten Techniken auf. Auch diese sollen daher in groben Zügen dargestellt werden, bevor auf die Spezifika des E-Mail-Dienstes eingegangen wird.<sup>7</sup>

### **1. Datenübertragung im Internet**

Wie in jedem Netzwerk erfolgt auch im Internet die Übermittlung von Daten auf der Basis von sog. Protokollen. Unter einem Protokoll versteht man die Regeln, die Rechner im Netz einhalten müssen, um eine funktionsfähige Verbindung untereinander herzustellen. Sie werden meist in Form von Software realisiert und

---

<sup>5</sup> *Kleine-Voßbeck*, S. 18.

<sup>6</sup> Abgrenzungsschwierigkeiten zu den Massenmedien könnten sich allerdings bei den sog. Mailinglisten ergeben. Bei diesen Systemen wird die von einem Mitglied der Liste eintreffende E-Mail automatisch an die anderen Mitglieder der Liste weitergeleitet. Dabei ist es u.U. jedem möglich, sich in eine solche Liste einzutragen. Zum Teil werden die einzelnen Beiträge auch in einem Archiv über das World Wide Web öffentlich zugänglich gemacht. In dieser Form ist E-Mail kein privates Kommunikationsmedium mehr. Auf die möglichen rechtlichen Folgen dieser Einordnung kann hier allerdings nicht eingegangen werden.

<sup>7</sup> Die Erläuterungen müssen sich aus Platzgründen auf das Wesentliche beschränken. Detaillierte Beschreibungen z.B. bei *Lindemann/Immler/Harms*, S. 947 ff. oder, speziell für die juristische Arbeit, bei *Germann*, S. 56 ff.

haben die Aufgabe, für den Aufbau von Verbindungen zu anderen Computern im Netz, für die reibungslose Übertragung der Daten sowie eine evtl. notwendige Korrektur fehlerhaft übermittelter Daten zu sorgen.<sup>8</sup>

Man kann dabei die im Internet verwendeten Protokolle in zwei Gruppen einteilen: Zum einen gibt es Basisprotokolle, die der Übermittlung von Daten jedweder Art dienen; zum anderen aber verfügt auch jeder der einzelnen Internet-Dienste noch über ein eigenes Protokoll, das komplexere Aufgaben übernimmt (im folgenden Anwendungsprotokoll genannt).<sup>9</sup> Die Anwendungsprotokolle bauen auf den Basisprotokollen auf und nutzen die von diesen zur Verfügung gestellten Funktionen.

## **2. Die Basisprotokolle TCP und IP**

Die grundlegende Funktion, eine fehlerfreie Übermittlung von Daten an einen beliebigen Rechner im Internet zu ermöglichen, erfüllen gemeinsam das Internet Protocol (IP) und das Transmission Control Protocol (TCP). Charakteristisch ist dabei die Aufteilung der zu übermittelnden Daten in kleinere Einheiten durch das IP die sog. Datagramme.<sup>10</sup> Die anschließende Übertragung ist dabei nicht auf einen eindeutigen, vorgebenen Weg festgelegt; vielmehr wird der Weg für jedes Datagramm vom Absender zum Empfänger erst im Moment der Übermittlung durch spezielle Vermittlungsrechner (sog. Router) bestimmt,<sup>11</sup> wobei es für die Auswahl der Route auf deren Stabilität und Geschwindig-

---

<sup>8</sup> Irlbeck, Stichwort "Übertragungsprotokoll".

<sup>9</sup> Diese Unterscheidung erfolgt in Anlehnung an das sog. OSI-Schichtenmodell bzw. an das Modell des "Internet Protocol Stack", dazu Lindemann/Immler/Harms, S. 947 ff. und Germann, S. 57 Fn. 73.

<sup>10</sup> Scheller/Boden/Geenen/Kampermann, S. 25.

<sup>11</sup> Lindemann/Immler/Harms, S. 963.

keit ankommt.<sup>12</sup>

Für die Funktion der Datenübermittlung per TCP und IP unerläßlich sind eindeutige, d.h. innerhalb des Internet nur ein einziges Mal vorkommende Absender- und Zieladressen. Diese Adressen sind quasi die Identität der Rechner im Internet. Sie bestehen aus einer Zahl mit 32 Binärstellen (Bits), in der üblichen Schreibweise angegeben als vier durch Punkte getrennte Dezimalzahlen mit Werten von 0 bis 255; beispielsweise hat der zentrale WWW-Server der Universität Hannover die Adresse 130.75.2.17.

Einem Rechner kann eine solche Adresse auf zwei Arten zugewiesen werden:

- Möglich ist, daß ein Rechner eine Adresse permanent, d.h. für jede Verbindung mit dem Internet, erhält. Dies ist häufig in größeren Netzwerken, etwa bei Unternehmen, der Fall. Die Vergabe einer solchen sog. statischen IP-Adresse erfolgt durch die Network Information Center (NIC),<sup>13</sup> spezielle Einrichtungen, die mit der Organisation des Internet befaßt sind.
- Die Alternative besteht darin, einem Rechner eine Adresse erst dann zuzuordnen, wenn er tatsächlich mit dem Internet in Kontakt tritt; die konkrete Adresse wird dann aus einem Pool von möglichen Adressen ausgewählt. Dieses Prinzip der sog. dynamischen Adreßzuweisung verwenden in der Regel Internet-Provider, bei denen sich der Benutzer nur zeitweise, z.B. per Modem, einwählt.

In jedem Fall wird die einem Rechner zugewiesene IP-Adresse bei einer Kommunikation mit einem anderen Rechner zusammen mit dem IP-Datagramm übertragen.

---

<sup>12</sup>A.a.O., S. 981.

<sup>13</sup>Köhntopp/Köhntopp, in: CR 2000, 248 (248).

### **3. Domain-Namen**

Da die beschriebenen numerischen Adressen für Menschen nur schwer zu merken sind, wurde ein weiterer Internet-Dienst, der Domain Name Service (DNS) aufgebaut. Dieser hat die Aufgabe, Rechnernamen in die numerischen IP-Adressen zu übersetzen.<sup>14</sup> Realisiert ist der DNS durch eine Anzahl über das Internet verteilter speziell konfigurierter Rechnersysteme, die sog. Name Server. Die Name Server erhalten Anfragen von Programmen, die auf den an das Internet angeschlossenen Rechnern laufen. Beispielsweise kontaktiert ein Programm zum Versenden von E-Mail den Name Server, um die numerische IP-Adresse des Rechners "t-online.de" zu erfahren, weil er nur mit dieser die E-Mail übertragen kann.

### **4. Die Technik des E-Mail-Dienstes**

Wie bereits erwähnt, bilden die Protokolle TCP und IP nur die Grundlage, auf der sich die einzelnen Dienste entwickelt haben und auch heute noch neue Dienste entstehen.<sup>15</sup> Jeder Dienst, wie z.B. E-Mail, verfügt dabei über ein weiteres Protokoll, das speziell auf seine Aufgaben zugeschnitten ist und in der Regel aus bestimmten englischsprachigen Schlüsselwörtern besteht, mit denen der Ablauf gesteuert wird. Diese Schlüsselwörter werden zusammen mit den notwendigen Daten mit Hilfe von TCP und IP übertragen. Daraus folgt, daß die beteiligten Rechner auch die IP-Adresse der jeweiligen Gegenstelle kennen. Dies hat Konsequenzen für die technischen Möglichkeiten der Überwachung. Bevor hierauf eingegangen wird, soll jedoch zunächst der technische Ablauf bei der Benutzung von E-Mail dargestellt werden.

Auch wenn elektronische Nachrichten sehr schnell erstellt und

---

<sup>14</sup> Scheller/Boden/Geenen/Kampermann, S. 27.

<sup>15</sup> Z.B. arbeiten die Musiktauschbörse Napster und das Chat-System ICQ ebenfalls mit TCP/IP.

versendet werden können, durchlaufen sie eine ganze Reihe von Stationen.<sup>16</sup>

Zunächst verfaßt der Absender die Mitteilung auf seinem PC mit Hilfe des entsprechenden Anwendungsprogramms (sog. Mail User Agent, z.B. Microsoft Outlook). Ist der Rechner nicht dauerhaft mit dem Internet verbunden, wird die Mitteilung dort zunächst auf der Festplatte in einer Datei zwischengespeichert, die oft als "Ausgangskorb" bezeichnet wird. Erst wenn die Verbindung hergestellt ist, erfolgt die Weitergabe an den für den Absender zuständigen<sup>17</sup> sog. Mail-Server mit Hilfe eines Anwendungsprotokolls.<sup>18</sup> Der Server ermittelt anhand der Adresse des Empfängers den für den Empfänger zuständigen Mail-Server.

Anschließend wird die E-Mail über das Internet an den so ermittelten Mail-Server des Empfängers übermittelt. Ob sie dort zwischengespeichert wird, hängt wiederum davon ab, ob der PC des Empfängers dauerhaft mit dem Internet verbunden ist. Eine dauerhafte Verbindung ist für sehr viele Benutzer heute noch nicht erschwinglich oder sinnvoll, so daß in sehr vielen Fällen eine Zwischenspeicherung stattfindet. In diesem Fall wird die E-Mail zunächst in einem für den Empfänger vorgesehenen "elektronischen Postfach" in Form einer Datei abgelegt, die der Empfänger später ebenfalls mit seinem Mail User Agent auf seinen PC übertragen ("herunterladen") und dort dauerhaft speichern und ver-

---

<sup>16</sup>Vgl. detailliert *Köhntopp/Köhntopp*, in: CR 2000, 248 (254 f.).

<sup>17</sup>Als zuständig werden die Server bezeichnet, die von Absender und Empfänger für das Senden oder Empfangen von Nachrichten aufgrund von vertraglichen Vereinbarungen mit den Server-Betreibern genutzt werden können. Auch wenn im folgenden aus Gründen der sprachlichen Vereinfachung vom Mail-Server "des Absenders" oder "des Empfängers" die Rede ist, ist damit stets der jeweils zuständige Rechner gemeint. Mail-Server befinden sich üblicherweise nicht im Besitz von Absender oder Empfänger, sondern eines Unternehmens, das den Server betreibt und entsprechende Mail-Dienstleistungen anbietet.

<sup>18</sup>SMTP (Simple Mail Transport Protocol).

walten kann; hier kommt ein weiteres Anwendungsprotokoll<sup>19</sup> zum Einsatz.

Da die Übertragung der Daten im einzelnen über TCP und IP abgewickelt wird, fallen hier eine Vielzahl von IP-Adressen an, die üblicherweise in einem Vorspann der Nachricht (sog. Header) festgehalten werden. In dieser Kette sind alle am Transport beteiligten Mail-Server vom Absender bis zum Empfänger ersichtlich, außerdem die E-Mail-Adressen von Absender und Empfänger sowie Datum und Zeit der Absendung.

## **5. Der Zugang zum Internet**

Das Internet legt für den Zugang eines einzelnen Rechners kein bestimmtes technisches Verfahren fest, sondern ist für verschiedene Standards offen, solange der anzubindende Rechner nur mit den Basisprotokollen TCP und IP arbeitet.

Möglich ist daher einerseits, daß ein Benutzer per Netzwerk dauerhaft an das Internet angeschlossen ist, wie dies z.B. bei Universitäten, Behörden und größeren Unternehmen der Fall ist. Für Privatpersonen ist eine solche Verbindung dagegen gegenwärtig noch zu teuer. In diesem Fall wird der Zugang daher üblicherweise mittels eines Modems oder per ISDN über das Telefonnetz realisiert. Der Benutzer benötigt dazu einen Zugangsvermittler (Access Provider), der ihm die Verbindung zum Internet zur Verfügung stellt. Technisch läuft die Kontaktaufnahme dann in der Weise ab, daß der Benutzer mit Modem oder ISDN die Rufnummer eines sog. Terminal-Servers beim Zugangsvermittler anwählt und sich dort mit seiner Benutzerkennung (sog. Login-Name) und seinem Paßwort ausweist;<sup>20</sup> an dieser Stelle erfolgt auch die dyna-

---

<sup>19</sup> In der Regel POP3 (Post Office Protocol Version 3).

<sup>20</sup> *Köhntopp/Köhntopp*, in: CR 2000, 248 (250).

mische Zuweisung einer noch nicht belegten IP-Adresse an den Rechner des Benutzers. Über diese Schnittstelle kann der Benutzer sodann die Dienste des Internet nutzen, also etwa E-Mails versenden oder auf seinen Rechner herunterladen.

## **6. Logdateien**

Viele Informationen im Zusammenhang mit der Benutzung von E-Mail und dem Aufbau einer Verbindung zum Internet gehen nach Abwicklung des Dienstes nicht verloren, sondern werden an den beteiligten Servern in sog. Logdateien für eine bestimmte Zeit festgehalten. Die Gründe für die Speicherung sind vielfältig. Beispielsweise können die Daten der Abrechnung von Dienstleistungen dienen. Weiterhin läßt sich aus den Logdateien u.U. der Versuch eines unbefugten Eindringens in das System erkennen. Schließlich können die Informationen auch zu Zwecken des Marketings ausgewertet werden.<sup>21</sup>

Im einzelnen werden typischerweise die folgenden Daten erfaßt:

### **a) Zugangsvermittlung**

Sofern ein Computer, wie bei Privatpersonen heute noch üblich, nicht dauerhaft mit dem Internet verbunden ist, fallen beim Aufbau der Verbindung, der typischerweise über das Telefonnetz erfolgt, zum einen Verbindungsdaten beim Betreiber des Telefonnetzes, zum anderen Verbindungsdaten beim Zugangsvermittler an.

Der Betreiber des Telefonnetzes speichert vor allem Beginn und Ende der Verbindung mit Datum und Uhrzeit, um diese Leistung

---

<sup>21</sup> Dieser Aspekt spielt vor allem beim World Wide Web eine Rolle. Praktiziert wird aber auch das Sammeln von E-Mail-Adressen (sog. Harvesting), um diesen Personen E-Mails mit Werbung zukommen zu lassen (sog. Spamming).

später abrechnen zu können. Gleiches gilt in der Regel für den Zugangsvermittler. Der Zugangsvermittler protokolliert außerdem meist auch, welche dynamische IP-Adresse dem Benutzer zugewiesen wurde.<sup>22</sup> Nur über seine Aufzeichnungen ist also die Zuordnung zum Benutzer möglich.

### **b) Verwendung des E-Mail-Dienstes**

Beim Versand von E-Mails wird zwar nicht deren Inhalt protokolliert. Über Logdateien nachweisbar sind aber in der Regel der Zeitpunkt der Übermittlung von E-Mail an den Mail-Server des Absenders sowie der Abruf der Mitteilungen vom Mail-Server des Empfängers.<sup>23</sup> Da die Übertragung der Daten in beiden Fällen mit den Basisprotokollen TCP und IP erfolgt, wird die den jeweiligen Rechnern zugewiesene IP-Adresse registriert.

## **III. Rollen in der E-Mail-Kommunikation**

Abschließend sollen die verschiedenen an der Kommunikation per E-Mail beteiligten Personen und ihre Funktionen zusammengefaßt werden.

Absender und Empfänger sind Privatpersonen. Praktisch wird es nicht vorkommen, daß eine Person ausschließlich E-Mails versendet oder empfängt; vielmehr ist jeder Absender auch Empfänger und umgekehrt. Für die Betrachtung der technischen Aspekte und der rechtlichen Fragestellungen ist es aber notwendig, diese beiden Funktionen zu unterscheiden.

Sowohl Absender als auch Empfänger stellen ihre Verbindung zum Internet üblicherweise über das Telefonnetz mit Hilfe eines

---

<sup>22</sup> Köhntopp/Köhntopp, in: CR 2000, 248 (250).

<sup>23</sup> A.a.O., S. 254.

Modems oder per ISDN her; beteiligt ist also auch der Betreiber des Telefonnetzes. Die eigentliche Schnittstelle zum Internet bietet dagegen der Zugangsvermittler. Aufgabe des Betreibers des Telefonnetzes ist es lediglich, die Verbindung zum Zugangsvermittler bereitzustellen. Sowohl der Betreiber des Telefonnetzes als auch der Zugangsvermittler sind in der Regel Unternehmen.

Für den Transport der E-Mails unabdingbar sind Mail-Server. Deren Betreiber können, müssen aber nicht, mit den Zugangsvermittlern identisch sein. Hierbei handelt es sich typischerweise ebenfalls um Unternehmen.

Die Betreiber des Telefonnetzes, die Zugangsvermittler und die Betreiber der Mail-Server werden im folgenden auch als Diensteanbieter bezeichnet.

## **B. Ansatzpunkte für die Überwachung**

Aus den technischen Merkmalen folgen die Ansatzpunkte für die Überwachung, die in diesem Abschnitt beschrieben werden sollen. Diese Maßnahmen bilden auch den Rahmen für die anschließende rechtliche Untersuchung. Leider stehen kaum Informationen darüber zur Verfügung, welche Methoden die Strafverfolgungsbehörden bei Ermittlungen im Internet tatsächlich einsetzen.<sup>24</sup> Dargestellt werden deswegen Vorgehensweisen, die ganz allgemein aufgrund der technischen Gegebenheiten plausibel erscheinen.

---

<sup>24</sup>Hinweise zur Praxis finden sich allerdings bei *Meseke*, in: *Kriminalistik* 2000, 245 ff. und *Gundermann*, in: *DuD* 1999, 681 ff.

## I. Ziele und Vorgehensweisen bei Ermittlungen

Generell können Überwachungsmaßnahmen zwei Ziele haben. Zum einen können sie dazu dienen, Kommunikationsinhalte zu erlangen, z.B. den Inhalt einer E-Mail. Zum anderen können sie die Identifizierung der Kommunikationsteilnehmer bezwecken. In beiden Richtungen werden Ermittlungen dadurch erschwert, daß es technische Möglichkeiten gibt, Inhalt und Identität geheim zu halten. So können E-Mails vor dem Versand verschlüsselt und dadurch dem staatlichen Einblick effektiv entzogen werden.<sup>25</sup> Herkunft und Ziel von Daten lassen sich sowohl auf der Ebene des IP-Protokolls als auch auf der höheren Ebene des E-Mail-Dienstes verschleiern.<sup>26</sup> Diese Probleme betreffen aber in der Regel nur die tatsächlichen Erfolgsaussichten der Überwachung, nicht jedoch rechtliche Fragen.<sup>27</sup>

Neben den Daten, auf die es den Strafverfolgungsbehörden ankommt, muß auch nach den verschiedenen Methoden differenziert werden, wie sich die Strafverfolgungsbehörden den Zugang hierzu verschaffen. Denkbar ist ein offenes Vorgehen, etwa im Rahmen einer Durchsuchung. In Betracht kommt aber auch eine "virtuelle Durchsuchung", indem die staatlichen Organe in einen Rechner ohne Wissen des Betreibers von außen über eine Internet-Verbindung eindringen und dabei die Sperren überwinden, die vom Betreiber eingebaut wurden, um die auf dem Rechner befindlichen Daten vor dem Zugriff durch Unbefugte zu schützen. Typischerweise handelt es sich dabei um einen Paßwortschutz,

---

<sup>25</sup> Zur Wirksamkeit der Verschlüsselung *Germann*, S. 94 ff. Selbst das amerikanische FBI war jedenfalls im Januar 1999 nicht in der Lage, eine mit dem verbreiteten Programm PGP hergestellte Verschlüsselung zu brechen, vgl. "Das Ohr des FBI – am Keyboard", <http://www.heise.de/newsticker/data/thd-30.07.01-002>.

<sup>26</sup> Detailliert *Germann*, S. 272 ff., 276.

<sup>27</sup> Rechtliche Bedeutung erlangt Verschlüsselungstechnik allerdings, wenn ihr Einsatz, wie in manchen Staaten, bestimmten Einschränkungen unterliegt.

d.h. der Zugriff z.B. auf die bereitliegenden E-Mails wird erst nach Übermittlung eines Paßworts eröffnet. Wenn im folgenden von “staatlichem Hacking” die Rede ist, ist damit einerseits die Überwindung der Sperren mittels eines fremden, den Behörden aber bekanntgewordenen Paßworts gemeint; zum anderen soll der Begriff aber auch den Einsatz spezieller Hacking-Techniken<sup>28</sup> erfassen.

## **II. Zugriff auf Inhalte von E-Mails**

Am einfachsten ist der Zugriff auf Inhalte von E-Mails möglich, wenn sich der Benutzer bei einem Zugangsvermittler einwählen muß; dann kann in der Art der klassischen Fernmeldeüberwachung der Telefonanschluß des Benutzers “abgehört” und der gesamte Datenverkehr aufgezeichnet werden. Dies betrifft insbesondere E-Mails, die vom Absender zum Versand an den für ihn zuständigen Mail-Server übermittelt oder als Empfänger von seinem Mail-Server abgeholt werden.

Eine Überwachung der Vermittlungsrechner (Router) im Internet verspricht dagegen wenig Erfolg, da in der Regel nicht vorhergesagt werden kann, über welche Router die für die Strafverfolgungsbehörden interessanten Daten laufen. Diese Methode wird daher nicht weiter untersucht.

Ein wichtiger Ansatzpunkt für den Zugriff auf E-Mails ist dagegen der Mail-Server des Empfängers. Wie dargestellt, werden eingehende E-Mails dort sehr häufig für längere Zeit gespeichert. Deswegen liegt es für die Ermittlungsbehörden nahe, während dieses Zeitraums Einsicht in diese Nachrichten zu nehmen.

---

<sup>28</sup>Denkbar erscheint hier der Einsatz spezieller Software, die mögliche Paßwörter ausprobiert, aber auch eine Umgehung des Paßwortschutzes insgesamt, z.B. durch Ausnutzen von Sicherheitslücken im System.

Außerdem ist es selbstverständlich möglich, E-Mails zu untersuchen, die sich auf den persönlichen Rechnern von Absender und Empfänger befinden. Auf dem PC des Absenders bleiben abzuschickende E-Mails zumindest solange im Ausgangskorb gespeichert, bis sie tatsächlich zu dem für den Absender zuständigen Mail-Server übertragen werden. Auf dem PC des Empfängers befinden sich die E-Mails, die dieser von seinem Mail-Server heruntergeladen hat. Da alle gängigen Mail User Agents, z.B. Microsoft Outlook, Archivierungsfunktionen für abgeschickte und empfangene E-Mails bieten, können die Strafverfolgungsbehörden sogar damit rechnen, auch noch ältere Nachrichten vorzufinden.

### **III. Identifizierung der Kommunikationsteilnehmer**

#### **1. Informationsquellen**

Bei E-Mails kann die Person des Absenders wie des Empfängers gleichermaßen interessant sein. Deren Identität ergibt sich nicht zwangsläufig schon aus den E-Mail-Adressen von Absender und Empfänger, die im Vorspann der Nachricht enthalten sind. Diese Bezeichnungen können nämlich bei vielen Anbietern von E-Mail-Diensten frei gewählt werden. Zur Identifizierung sind zwei Wege denkbar:

- Über den Anbieter des E-Mail-Dienstes kann versucht werden, mit Hilfe der jeweiligen Adresse die persönlichen Daten des Absenders bzw. Empfängers in Erfahrung zu bringen. Eine Reihe von Unternehmen, z.B. GMX, bieten für die Öffentlichkeit allerdings auch Dienste an, für deren Nutzung die Angabe persönlicher Daten nicht erforderlich ist oder bei denen die Richtigkeit angegebener Daten nicht überprüft wird.
- In diesen Fällen kann über die Logdateien der Mail-Server die IP-Adresse des einsendenden bzw. abrufenden Rechners ermittelt werden; dabei kann auch die Auswertung des im Vorspann

der E-Mails üblicherweise aufgezeichneten Übertragungswegs hilfreich sein. Die erhaltene IP-Adresse muß allerdings noch einer Person zugeordnet werden.

## **2. Umsetzung der IP-Adresse in Personendaten**

### **a) Vorgehensweise**

Wie gezeigt, kann man ganz allgemein bei den Diensten des Internet, und daher auch bei E-Mail, vor allem mit Hilfe der Logdateien die beteiligten Rechner, d.h. ihre IP-Adressen, relativ einfach feststellen. Dies hat seinen Grund in der Verwendung des Internet Protocol, für das eine jedem Rechner zugewiesene eindeutige Adresse, gewissermaßen eine "Internet-Identität", charakteristisch ist. Schwieriger ist dagegen der Schluß von dieser "Internet-Identität" auf die Identität desjenigen, der einen Rechner zur Kommunikation per E-Mail benutzt hat.

Handelt es sich bei der IP-Adresse um eine statische Adresse, so kann über eine im Internet verfügbare Datenbank der IP-Adressen der Betreiber des zugehörigen Rechners abgefragt werden.<sup>29</sup>

Bei einer dynamischen IP-Adresse läßt sich diese Verknüpfung dagegen nur mittels der Unterlagen des Zugangsvermittlers herstellen; dazu muß die Logdatei des Terminal-Servers ausgewertet werden, in der die Anrufe der Benutzer und die ihnen jeweils zugewiesene IP-Adresse verzeichnet sind. Auch insoweit kann sich allerdings das Problem stellen, daß der Zugang "anonym" von einem sog. Internet-by-call-Dienst vermittelt wurde, der seine Leistungen über die Telefonrechnung des Anrufers abrechnet. In diesem Fall ist aber zwangsläufig beim Zugangsvermittler die Telefonnummer des Internet-Nutzers bekannt, so daß dessen

---

<sup>29</sup> Abfrage der sog. WHO IS-Datenbank, z.B. über <http://www.ripe.net> .

Personalien mit Hilfe der Unterlagen des Betreibers des Telefonnetzes ermittelt werden können.

#### **b) Aussagekraft der erlangten Daten**

In beiden Fällen kann die IP-Adresse – unabhängig von den Möglichkeiten ihrer Fälschung – im Rahmen von Ermittlungen allerdings keinen vollständigen Beweis für die Aktivität einer bestimmten Person im Internet erbringen. Zum einen muß die IP-Adresse nicht zwangsläufig auf einen einzigen Rechner hinweisen; vielmehr kann hinter einem Rechner mit einer einzigen IP-Adresse ein größeres Netzwerk stehen. Zum anderen ist nicht unbedingt nachvollziehbar, welche Person einen bestimmten Rechner zur Kommunikation per E-Mail benutzt hat, wenn mehrere Personen zu dem Rechner Zugang hatten. Bei dynamischer Adreßzuweisung muß außerdem berücksichtigt werden, daß eine IP-Adresse zu verschiedenen Zeitpunkten verschiedenen Rechnern und damit verschiedenen Benutzern zugewiesen sein kann. Gleichwohl kann die Adresse aber im Zusammenhang mit anderen Anhaltspunkten ein wichtiges Indiz bilden.

### **C. Der Schutz der E-Mail-Kommunikation durch die Grundrechte**

Nach Art. 1 Abs. 3 GG sind Gesetzgebung, vollziehende Gewalt und Rechtsprechung an die Grundrechte gebunden. Da die Strafverfolgungsbehörden der vollziehenden Gewalt zuzuordnen sind, müssen auch sie diese Verpflichtung bei ihrer Tätigkeit beachten. Dies wirft gerade im Bereich von Ermittlungen mit Bezug zur EDV-Technik besondere Schwierigkeiten auf, da die Bestimmungen des Grundgesetzes zu einer Zeit verfaßt wurden, als Computersysteme und Internet noch unbekannt waren.

Gleichwohl können und müssen die Grundrechte weiterhin Geltung beanspruchen. Aufgabe dieses Abschnitts ist es daher, die Schutzbereiche verschiedener Grundrechte im Zusammenhang mit der Verwendung des Kommunikationsmediums E-Mail und dem Einsatz von Rechnersystemen zu bestimmen. Außerdem soll der Eingriffscharakter möglicher Ermittlungsmaßnahmen untersucht werden. Soweit sich dabei ergibt, daß eine Maßnahme in ein Grundrecht eingreift, bedeutet dies, daß den Strafverfolgungsbehörden eine entsprechende gesetzliche Ermächtigungsgrundlage zur Verfügung stehen muß, um den Eingriff zu rechtfertigen. In diesem Punkt besteht zwischen den Maßnahmen einer Verwaltungsbehörde, die nach den Vorschriften des öffentlichen Rechts handelt, und denen einer Strafverfolgungsbehörde, die nach der StPO verfährt, kein dogmatischer Unterschied.<sup>30</sup>

Die Prüfung des Eingriffscharakters von Maßnahmen der Strafverfolgungsbehörden geht dabei von einer doppelten Fragestellung aus. Zum einen ist der eigentliche Zugriff auf die relevanten Daten zu beurteilen, z.B. die Beschlagnahme eines Datenträgers. Zum anderen ist aber auch die – in der Praxis vorgelagerte – Frage von Bedeutung, wie sich die Behörden die *Möglichkeit des Zugriffs* verschaffen können. Beide Maßnahmen müssen klar getrennt werden, weil sie unterschiedliche Grundrechte verschiedener Personen betreffen können.

---

<sup>30</sup>Daß bei der Beurteilung strafprozessualer Maßnahmen nicht nur das einfache Recht der StPO, sondern vor allem auch die Grundrechte eine wesentliche Rolle spielen, wird freilich in Rechtsprechung und Literatur nicht immer berücksichtigt. So widerspricht die "Mailbox"-Entscheidung BGH CR 1996, 488 allgemein anerkannten Regeln der Grundrechtsdogmatik (dazu unten VII.); dieser Umstand wird aber z.B. von Kudlich, Mailbox, nicht einmal kurz angesprochen. Einzig Sieber, in: Hoeren/Sieber (Hg.), Rn. 703 f., bemerkt, daß die Entscheidung bereits aus *verfassungsrechtlichen* Gründen (Art. 13 GG) nicht haltbar sei. Kudlich geht auf diesen Kritikpunkt erst in Strafprozessuale Probleme, S. 233 ein.

Möglichkeiten zum Zugriff auf Daten stehen den Ermittlungsbehörden offen, wenn sie im Rahmen einer Durchsuchung in die Wohnung von Absender oder Empfänger eindringen; dann können sie die auf deren PC's befindlichen Mails untersuchen. Ebenso erscheint z.B. eine Durchsuchung beim Betreiber des für den Empfänger zuständigen Mail-Servers naheliegend, um Zugriff auf die auf diesem Server für den Empfänger bereitliegenden E-Mails zu erhalten. Das gleiche gilt für die Einsicht in Log- und Kundendateien bei den verschiedenen Diensteanbietern.

Zum anderen erscheint es denkbar, sich den Zugriff auf die auf den Rechnern von Privatpersonen und Betreibern gespeicherten Dateien nicht im Rahmen einer "körperlichen Durchsuchung" zu verschaffen, sondern durch "Anzapfen" der Rechner von außen über das Internet.<sup>31</sup> Der Einsatz von "staatlichem Hacking" bietet sich insbesondere auf dem Mail-Server des Empfängers zum Abruf der für ihn gespeicherten Nachrichten an, weil dieser Rechner ständig mit dem Internet verbunden ist, während dies bei den PC's von Privatpersonen in der Regel heute noch nicht der Fall ist.

## **I. Art. 10 Abs. 1 GG**

### **1. Schutzbereich**

Art. 10 Abs. 1 GG schützt das Brief-, Post- und Fernmeldegeheimnis. Allgemeiner gesprochen soll die Vertraulichkeit bei Verwendung der genannten Medien gewährleistet werden, die eine räumlich distanzierte Kommunikation ermöglichen.<sup>32</sup> Eine genaue Abgrenzung der drei Gewährleistungen ist entbehrlich, weil der

---

<sup>31</sup>Ein solches Vorgehen der Strafverfolgungsbehörden kann in Zukunft durchaus realistisch sein. So entwickelt das FBI gegenwärtig eine spezielle Software, die per E-Mail auf dem PC des Betroffenen installiert werden kann und dann Daten an das FBI sendet, vgl. "Laterne für den Fleischfresser", <http://www.heise.de/newsticker/data/wst-21.11.01-004> .

<sup>32</sup>Von Münch/Kunig-Löwer, Art. 10 Rn. 11, *Jarass/Pieroth*, Art. 10 Rn. 1.

Schutzumfang in jedem Fall der gleiche ist. Alle Schutzgüter stehen unter dem einheitlichen Gesetzesvorbehalt des Art. 10 Abs. 2 Satz 1 GG. Die Dreiteilung des Schutzes beruht auf der historischen Entwicklung,<sup>33</sup> wobei heute insbesondere die Bedeutung des Grundrechts angesichts der Privatisierung des Post- und Telekommunikationswesens umstritten ist.<sup>34</sup> Entscheidend ist jedoch der allen Varianten des Art. 10 Abs. 1 GG zugrunde liegende Gedanke, die Übermittlung von Informationen über eine Distanz besonders zu schützen, weil insoweit die verstärkte Gefahr eines Eindringens in die Privatsphäre der Kommunikationspartner besteht.<sup>35</sup>

Der von Art. 10 Abs. 1 GG gewährte Schutz gegenüber staatlichen Behörden erstreckt sich dabei auf zwei Aspekte:<sup>36</sup>

- Zum einen ist es der öffentlichen Gewalt verwehrt, den *Inhalt* der Kommunikation mitzulesen oder mitzuhören.
- Zum anderen dürfen aber auch die Umstände der Kommunikation, z.B. Datum und Dauer eines Telefongesprächs oder Absender und Empfänger eines Briefes, nicht aufgezeichnet werden. Diese Umstände werden auch *Verbindungsdaten* genannt.

Nicht von Art. 10 Abs. 1 GG geschützt sind dagegen die sog. *Bestandsdaten*. Darunter werden diejenigen persönlichen Daten, z.B. Name und Anschrift, verstanden, die unabhängig von einem konkreten Kommunikationsvorgang der Durchführung eines Vertragsverhältnisses über die Inanspruchnahme von Kommunikations-

---

<sup>33</sup> *Pieroth/Schlink*, Rn. 762, *Kleine-Voßbeck*, S. 32 ff.

<sup>34</sup> Näher von *Münch/Kunig-Löwer*, Art. 10 Rn. 9. Im Rahmen der vorliegenden Arbeit spielt dieser Streit keine Rolle, da jedenfalls die staatlichen Strafverfolgungsbehörden als Träger öffentlicher Gewalt auch weiterhin an Art. 10 Abs. 1 GG gebunden sind.

<sup>35</sup> *Kleine-Voßbeck*, S. 37.

<sup>36</sup> Von *Münch/Kunig-Löwer*, Art. 10 Rn. 11, *Pieroth/Schlink*, Rn. 767, 775.

dienstleistungen dienen.<sup>37</sup> Daß diese Daten für die Nutzung von Kommunikation erforderlich sind, macht sie noch nicht zu einem Schutzgut des Art. 10 Abs. 1 GG.

Ob auch der E-Mail-Verkehr von Art. 10 Abs. 1 GG erfaßt wird, hängt von der generellen Anwendbarkeit auf dieses Medium sowie davon ab, inwieweit beim Senden und Empfangen einer konkreten Nachricht Inhalte übermittelt werden. Außerdem ist der Schutz von Verbindungsdaten näher zu untersuchen.

## **2. Medium E-Mail**

Es versteht sich von selbst, daß die Kommunikationstechnik E-Mail bei der Formulierung des Art. 10 Abs. 1 GG nicht ausdrücklich bedacht werden konnte. Allgemein sind Bezugnahmen auf technische Sachverhalte dem Grundgesetz aber nicht fremd. So verweist Art. 10 Abs. 1 GG selbst auf den technischen Begriff des "Fernmeldens". Er ähnelt in dieser Beziehung Art. 5 Abs. 1 Satz 2 GG, der die Berichterstattung durch Rundfunk betrifft. Für den Begriff des Rundfunks ist eine Entwicklungsoffenheit allgemein anerkannt; einbezogen werden auch neuartige Angebote, solange es sich noch um Massenkommunikation handelt.<sup>38</sup> Es liegt nahe, dies im Fall von Art. 10 Abs. 1 GG ähnlich zu sehen. Hier wie dort bestehen keine Anhaltspunkte, daß der Verfassungsgeber den Schutzbereich auf eine bestimmte Technologie beschränken wollte. Der Grundrechtsschutz muß daher hinsichtlich der technischen Entwicklung dynamisch sein.<sup>39</sup> Demnach schützt das Fernmeldegeheimnis nicht nur den klassischen Telefon-, Telegramm- und Funkverkehr, sondern auch moderne Kommunikationsformen

---

<sup>37</sup> Zum Begriff der Bestands- und Verbindungsdaten vgl. etwa § 2 Nr. 3 und 4 der Telekommunikations-Datenschutzverordnung (TDSV), BGBl 2000 I, 1740.

<sup>38</sup> Jarass/Pieroth, Art. 5 Rn. 36.

<sup>39</sup> Von Münch/Kunig-Löwer, Art. 10 Rn. 11.

wie Mobilfunk oder die Kommunikation per Internet.<sup>40</sup>

In ähnlicher Weise könnte man auch den Begriff des Briefes in einem aktualisierten Sinn verstehen und eine E-Mail hierunter subsumieren. Zwar wurde der Brief bei der Abfassung des Grundgesetzes sicherlich als verkörperte Mitteilung verstanden;<sup>41</sup> dem stünde jedoch eine den modernen Gegebenheiten angepaßte Interpretation nicht entgegen, die nicht auf die Körperlichkeit der Nachricht, sondern auf den praktischen Eindruck abstellt. In diesem Sinne ähnelt eine E-Mail dem Brief, weil sie Informationen in Schriftzeichen lesbar vermittelt.

Ohne daß hier eine exakte Einordnung der E-Mail als Brief oder Objekt einer Telekommunikation erforderlich ist, kann jedenfalls festgestellt werden, daß die E-Mail bei der gebotenen modernen Interpretation des Verfassungstextes dem Schutzbereich des Art. 10 Abs. 1 GG unterfällt. Hierfür spricht auch der Zweck dieses Grundrechts, allgemein die ungestörte räumlich distanzierte Kommunikation zu gewährleisten. Der Schutz des Art. 10 Abs. 1 GG erstreckt sich damit grundsätzlich auf den Inhalt von E-Mails sowie die im Zusammenhang mit der Kommunikation per E-Mail anfallenden Verbindungsdaten.

### **3. Schutz der Inhalte von E-Mails**

Mit der grundsätzlichen Anwendbarkeit von Art. 10 Abs. 1 GG auf die moderne Kommunikationstechnik E-Mail ist allerdings noch nichts über seine Reichweite in bezug auf die einzelnen Kommunikationsvorgänge gesagt. Wie bereits dargestellt,<sup>42</sup> verläuft der E-Mail-Verkehr in mehreren Phasen. Daher ist zu untersuchen, wäh-

---

<sup>40</sup> So auch *Pieroth/Schlink*, Rn. 773.

<sup>41</sup> *Kleine-Voßbeck*, S. 38.

<sup>42</sup> Oben A.II.4.

rend welcher Aktionen im einzelnen Art. 10 Abs. 1 GG gelten kann.

Charakteristisch für alle Gewährleistungen des Art. 10 Abs. 1 GG ist das Merkmal der Übermittlung von Inhalten, sei es in körperlicher oder unkörperlicher Form. Nur insoweit besteht daher ein Schutz. Für E-Mails bedeutet dies:

**a) Nachrichten auf dem PC des Absenders**

Solange die Nachricht noch auf dem persönlichen Rechner des Absenders im Ausgangskorb gespeichert ist, greift Art. 10 Abs. 1 GG nicht ein. Auch wenn das Zwischenspeichern bis zum nächsten Aufbau einer Verbindung mit dem Internet aus Sicht des Absenders den ersten Schritt des Versendens darstellt, hat dennoch keine Übermittlung von Inhalten stattgefunden. Die zu versendende Nachricht kann daher keinen anderen Status haben als jede andere auf dem Rechner gespeicherte Datei. Die Situation ist vergleichbar mit einem bereitgelegten, aber noch nicht in den Briefkasten eingeworfenen Brief.<sup>43</sup>

**b) Übertragung der E-Mail zum Mail-Server des Empfängers**

Dagegen ist Art. 10 Abs. 1 GG zweifellos einschlägig, sobald eine E-Mail vom PC des Absenders zu dem für ihn zuständigen Mail-Server und von dort zum Mail-Server des Empfängers übertragen wird. Insoweit findet offensichtlich eine Übermittlung von Inhalten statt. Dies gilt auch dann, wenn die Nachricht auf dem Transportweg aus technischen Gründen kurzzeitig zwischengespeichert wird; diese aus Sicht der Benutzer des E-Mail-Dienstes zufällige

---

<sup>43</sup> A.A. *Kleine-Voßbeck*, S. 36 ff., der allerdings von dem andersartigen technischen Sachverhalt ausgeht, daß die zu versendende Nachricht über längere Zeit nicht auf dem PC des Absenders, sondern auf dem für diesen zuständigen Mail-Server gespeichert bleibt. Diese Situation ist für den E-Mail-Versand per Internet untypisch.

Unterbrechung kann nicht zu einer Lücke im grundrechtlichen Schutz führen.

### **c) Nachrichten auf dem Mail-Server des Empfängers**

Schwierigkeiten bereitet dagegen die Einordnung der Nachricht, sobald sie das dem Empfänger zugeordnete Postfach auf dem für ihn zuständigen Mail-Server erreicht hat, von ihm aber noch nicht auf seinen PC heruntergeladen wurde.

Einerseits könnte man hier argumentieren, daß der Vorgang des Übermitteln von Inhalten beendet sei, weil es nun lediglich in der Hand des Empfängers liege, wann dieser die E-Mail abrufe; anders als im oben genannten Fall erfolge die Zwischenspeicherung nicht zufällig und kurzzeitig aus technischen Gründen, sondern vom Empfänger gewollt und u.U. über längere Zeit, weil eine dauerhafte Verbindung zum Internet wirtschaftlich nicht sinnvoll sei.

Diese Sichtweise vernachlässigt aber, daß sich eine E-Mail, auch wenn der Empfänger sie jederzeit von seinem Mail-Server herunterladen kann, solange noch nicht in seinem Machtbereich befindet, bis er dies tatsächlich tut. In einem weiteren, von den technischen Merkmalen losgelösten Sinn ist die Übermittlung daher noch nicht abgeschlossen. Die Situation ist vergleichbar mit einem bei der Post lagernden Brief, den der Empfänger ebenfalls jederzeit abholen kann; in diesem Fall endet der Schutz des Art. 10 Abs. 1 GG aber erst in dem Zeitpunkt, in dem der Brief tatsächlich abgeholt wird.<sup>44</sup> Erst mit dem Herunterladen ist die der Übermittlung innewohnende Gefahr des Einbruchs fremder Personen in den Kommunikationsvorgang, den Art. 10 Abs. 1 GG verhindern will, gebannt.

---

<sup>44</sup>Von Münch/Kunig-Löwer, Art. 10 Rn. 17.

Gegen eine Ausklammerung der auf dem Mail-Server für den Empfänger bereitliegenden E-Mail spricht außerdem, daß die E-Mail später, wenn sie vom Empfänger heruntergeladen wird, während dieses Zeitraums wiederum dem Schutz des Art. 10 Abs. 1 GG unterliegt, weil insoweit zweifellos Inhalte übermittelt werden. Der Ausschluß würde damit zu dem paradoxen Ergebnis führen, daß eine Nachricht auf dem Weg zum Empfänger zunächst geschützt, später nicht geschützt und in der letzten Phase des Übermittlungsvorgangs schließlich wieder geschützt<sup>45</sup> wäre. Die Anwendbarkeit von Art. 10 Abs. 1 GG würde dann auch von der Zufälligkeit abhängen, wann der Empfänger die Nachricht herunterlädt. Dies widerspricht dem Sinn und Zweck von Art. 10 Abs. 1 GG, die Nachrichtenübermittlung umfassend vom Absenden bis zum Empfang zu schützen.<sup>46</sup>

Art. 10 Abs. 1 GG gilt daher auch für Nachrichten, die auf dem Mail-Server des Empfängers lagern, bis diese heruntergeladen werden.<sup>47</sup>

#### **d) Abrufen von E-Mails vom Mail-Server durch den Empfänger**

Auch während der Übertragung vom Mail-Server des Empfängers auf dessen PC sind die E-Mails vom Schutz des Art. 10 Abs. 1 GG erfaßt. Die Situation ähnelt sehr stark der Übertragung der E-Mails beim Versenden. Auf diese Ausführungen wird daher verwiesen.

---

<sup>45</sup> Dazu unten d.

<sup>46</sup> Vgl. *Kleine-Voßbeck*, S. 37 f. zu der nach seinen Annahmen ähnlichen Situation von Nachrichten in der Mailbox des Absenders.

<sup>47</sup> So im Ergebnis auch *Kudlich*, Mailbox, S. 213. Auch die Rechtsprechung geht von einem eindeutigen Schutz durch Art. 10 Abs. 1 GG aus; BGH CR 1996, 488 (489) und LG Hanau MMR 2000, 175 (175) nehmen die Geltung von Art. 10 Abs. 1 GG ohne weitere Begründung an.

#### **e) Nachrichten auf dem PC des Empfängers**

Nach diesem Zeitpunkt, wenn sich die E-Mail auf dem persönlichen Rechner des Empfängers befindet, scheidet ein Schutz durch Art. 10 Abs. 1 GG aus, denn die Übermittlung ist mit dem Herunterladen abgeschlossen. Die Nachricht hat dann grundsätzlich keinen anderen Status als jede andere Datei auf dem PC. Der Sachverhalt erscheint vergleichbar mit Briefen, die der Empfänger von der Post abgeholt hat und nun in seiner Wohnung aufbewahrt. Hier kann auf die Ausführungen zu Mitteilungen auf dem PC des Absenders verwiesen werden.

#### **4. Schutz von Verbindungsdaten**

Wie dargestellt, sind die Daten, die beim Versand von E-Mails entstehen, ebenfalls vom Schutz des Art. 10 Abs. 1 GG erfaßt. Dies gilt vor allem für die E-Mail-Adressen von Absender und Empfänger und Datum und Zeit der Absendung. Für IP-Adressen ist umstritten, ob diese den von Art. 10 Abs. 1 GG geschützten Verbindungs- oder den nicht geschützten Bestandsdaten zuzuordnen sind.<sup>48</sup> Da die IP-Adressen der Identifizierung der Kommunikationspartner dienen können, soll auf diese Problematik erst später näher eingegangen werden.<sup>49</sup>

Weiterhin stellt sich die Frage, ob zwischen den Personen unterschieden werden muß, bei denen Verbindungsdaten entstehen. Wie sich aus dem technischen Ablauf ergibt, werden Daten zum einen in den verschiedenen Logdateien beim Betreiber des Telefonnetzes, beim Zugangsvermittler und bei den Betreibern der Mail-Server aufgezeichnet;<sup>50</sup> zum anderen sind Verbindungsdaten

---

<sup>48</sup> *Gundermann*, in: DuD 1999, 681 (686), *Meseke*, in: *Kriminalistik* 2000, 245 (249).

<sup>49</sup> Unten G.I.1.

<sup>50</sup> Oben A.II.6.

aber auch in den E-Mails enthalten, die der Empfänger auf seinen PC herunterlädt.<sup>51</sup>

Während für die Logdateien ein Schutz durch Art. 10 Abs. 1 GG nach dem oben Gesagten grundsätzlich bejaht werden kann, ist die Lage hinsichtlich der in den E-Mails enthaltenen Verbindungsdaten komplizierter. Hier wurde bereits festgestellt, daß der Inhalt der E-Mails nicht mehr geschützt ist, sobald sich die E-Mails auf dem PC des Empfängers befinden. Zu fragen ist, ob sich eine Einschränkung der Zugriffsmöglichkeit nun daraus ergibt, daß jede E-Mail neben dem gedanklichen Inhalt auch Verbindungsdaten enthält. Aus praktischen Gründen müßte ein solcher Schutz die gesamte E-Mail erfassen, weil die Verbindungsdaten mit dem Inhalt in einer Datei verbunden sind und es in der Praxis kaum möglich sein dürfte, diese beiden Elemente zu trennen.

Im Ergebnis ist ein Schutz der gesamten E-Mail unter dem Aspekt des Schutzes der in ihr enthaltenen Verbindungsdaten aber abzulehnen. Dafür spricht, daß auch konventionelle Briefe regelmäßig eine Vielzahl von Verbindungsdaten enthalten. Meistens sind Absender und Empfänger sowie zumindest der Zeitpunkt ersichtlich, zu dem der Brief erstellt wurde. Dies führt gleichwohl nicht dazu, einen Schutz durch Art. 10 Abs. 1 GG anzunehmen. Nichts anderes kann auch für E-Mails gelten. Hier sind die Verbindungsdaten zwar durch ihre automatische Erfassung und Einfügung in den Nachrichtenkopf präziser und umfangreicher als bei einem konventionellen Brief, in ihrer Qualität unterscheiden sie sich dadurch aber nicht.

---

<sup>51</sup> Oben A.II.4.

## **5. Eingriffscharakter strafprozessualer Maßnahmen**

### **a) Verschaffen der Zugriffsmöglichkeit**

Wie beschrieben, schützt Art. 10 Abs. 1 GG vor der Kenntnisnahme von Inhalt und Umständen der Kommunikation per E-Mail. Nicht in seinen Regelungsbereich fällt dagegen die Abwehr vorgelagerter staatlicher Aktivitäten, um sich die Möglichkeit zum Einblick zu verschaffen. Das Verschaffen der Zugriffsmöglichkeit auf E-Mail-Inhalte oder Verbindungsdaten in dem oben beschriebenen Sinne berührt somit den Schutzbereich von Art. 10 Abs. 1 GG nicht. Es kann daher weder gegenüber den betroffenen Privatpersonen (Absender und Empfänger) noch gegenüber den sonstigen an der Übermittlung beteiligten Personen (Diensteanbieter) einen Eingriff darstellen.

### **b) Zugriff auf E-Mail-Inhalte und Verbindungsdaten**

Soweit strafprozessuale Maßnahmen dagegen dem eigentlichen Zugriff auf den Inhalt oder Verbindungsdaten der E-Mail-Kommunikation dienen, ist der Schutzbereich von Art. 10 Abs. 1 GG berührt, es sei denn, sie beschränken sich auf E-Mails, die sich auf den PC's von Absender oder Empfänger befinden. Denn gerade eine solche Kenntnisnahme soll der Bürger abwehren können. Hinsichtlich der Frage, ob in das Grundrecht *eingegriffen* wird,<sup>52</sup> sind die Personen von Absender und Empfänger einerseits und die anderen an der erfolgreichen Übertragung der E-Mail beteiligten Diensteanbieter andererseits zu unterscheiden.<sup>53</sup>

#### **aa) Absender und Empfänger**

Ein Eingriff in Art. 10 Abs. 1 GG ist gegeben, wenn die öffentliche Gewalt sich Kenntnisse von Inhalt oder äußeren Umständen der E-

---

<sup>52</sup> Zur Unterscheidung von Berührung des Schutzbereichs und Eingriff in den Schutzbereich *Pieroth/Schlink*, Rn. 226 ff.

<sup>53</sup> Vgl. die Zusammenstellung oben A.III.

Mail-Kommunikation verschafft.<sup>54</sup> Dies ist bei den nächstliegenden Maßnahmen, dem “Abhören” des gesamten E-Mail-Verkehrs einschließlich des Abrufs von Nachrichten vom Mail-Server des Empfängers und der Ermittlung der Verbindungsdaten, der Fall,<sup>55</sup> ebenso aber auch bei der Beschlagnahme von Datenträgern bei Diensteanbietern, auf denen sich zwischengespeicherte E-Mails oder Verbindungsdaten befinden.

### **bb) Diensteanbieter**

Die anderen Beteiligten, insbesondere die Betreiber der Mail-Server, sind durch eine Überwachungsmaßnahme nicht in Art. 10 Abs. 1 GG beeinträchtigt. Sie haben nämlich nur eine Übermittlungsfunktion, sind dagegen aber nicht eigentliche Teilnehmer der Kommunikation.<sup>56</sup>

## **II. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG**

### **1. Schutzbereich**

Das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung, das aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG abgeleitet wird, schützt generell die Freiheit des einzelnen, frei über seine Daten aus seinem privaten Lebensbereich zu verfügen.<sup>57</sup> Es erfasst daher auch die Kommunikation, die Ausdruck der menschlichen Persönlichkeit ist. Denn jeder einzelne entscheidet im Laufe des Kontakts, welche Informationen aus seinem persönlichen Lebensbereich er preisgeben möchte. Kommunikation betrifft damit einen Kern menschlicher Selbstbestimmung.<sup>58</sup>

---

<sup>54</sup> *Pieroth/Schlink*, Rn. 775.

<sup>55</sup> A.a.O., Rn. 781.

<sup>56</sup> Von Münch/Kunig-Löwer, Art. 10 Rn. 20. Diese Auffassung ist allerdings nicht unumstritten, zum Meinungsstand siehe a.a.O.

<sup>57</sup> *Jarass/Pieroth*, Art. 2 Rn. 32.

<sup>58</sup> Von Münch/Kunig-Löwer, Art. 10 Rn. 1.

Unter dem Schutz von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG stehen folglich auf jeden Fall die gedanklichen Inhalte von E-Mails. Nichts anderes gilt aber auch für die Verbindungsdaten. Diese werden zwar automatisiert von Computersystemen festgehalten, verlieren dadurch aber nicht ihre Eigenschaft als Informationen, die in engem Zusammenhang mit menschlicher Kommunikation stehen.

Auch die Bestandsdaten unterfallen dem Recht auf informationelle Selbstbestimmung, weil es sich bei diesen Angaben wie Name und Anschrift ebenfalls um Angaben aus dem persönlichen Lebensbereich handelt.

## **2. Eingriffscharakter strafprozessualer Maßnahmen**

Der Eingriffscharakter von Maßnahmen der Strafverfolgungsbehörden ist ähnlich zu beurteilen wie bei Art. 10 Abs. 1 GG.

### **a) Verschaffen der Zugriffsmöglichkeit**

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährt Schutz vor der Offenbarung persönlicher Lebensumstände und kann daher u.U. ihre Kenntnisnahme durch die Strafverfolgungsbehörden verhindern. Dagegen fällt der Schutz vor staatlichen Aktivitäten, die der Verschaffung einer Möglichkeit zum Zugriff dienen, nicht in den Regelungsbereich dieses Grundrechts. Insoweit kann der Schutzbereich daher nicht berührt sein.

### **b) Zugriff auf E-Mail-Inhalte, Verbindungs- und Bestandsdaten**

Da es Inhalt des allgemeinen Persönlichkeitsrechts ist, frei über die Preisgabe persönlicher Daten verfügen zu können, ist der Schutzbereich dieses Grundrechts dagegen berührt, wenn die Strafverfolgungsbehörden auf diese Daten ohne Zustimmung des

Berechtigten zugreifen, etwa durch eine Beschlagnahme. Für den Eingriffscharakter kommt es jedoch wie bei Art. 10 Abs. 1 GG auf die Funktion des Betroffenen an.

#### **aa) Absender und Empfänger**

Absender und Empfänger sind in ihrem allgemeinen Persönlichkeitsrecht beeinträchtigt, soweit die Daten, in die die Behörden Einsicht nehmen, von ihnen herrühren, d.h. aufgrund ihrer Nutzung des E-Mail-Dienstes entstanden sind. Dies gilt einerseits für Nachrichteninhalte, andererseits aber auch für die Daten in Logdateien sowie für die Bestandsdaten.

#### **bb) Diensteanbieter**

Anderen Personen, insbesondere den Betreibern der Mail-Server, steht das allgemeine Persönlichkeitsrecht in bezug auf die Daten ihrer Kunden nicht zu. Maßnahmen der Strafverfolgungsbehörden können sie daher insoweit nicht beeinträchtigen.

### **III. Art. 5 Abs. 1 GG**

Art. 5 Abs. 1 GG schützt als ein Element der "Kommunikationsverfassung"<sup>59</sup> die Freiheit der Meinungsäußerung des einzelnen (Art. 5 Abs. 1 Satz 1 GG) sowie die Massenmedien wie Presse und Rundfunkveranstalter (Art. 5 Abs. 1 Satz 2 GG).

Da in E-Mails auch Meinungen geäußert werden können, könnte der Schutzbereich von Art. 5 Abs. 1 Satz 1 GG durch eine Überwachung des E-Mail-Verkehrs berührt sein. Jedoch geht es beim "Mithören" seitens des Staates nicht eigentlich um die Meinungsäußerung als solche, sondern um die *Kenntnisnahme* von einer Meinungsäußerung. Die Freiheit der Meinungsäußerung ist daher

---

<sup>59</sup> A.a.O.

erst dann berührt und beeinträchtigt, wenn gegen den Absender wegen des Inhalts der geäußerten Meinung Sanktionen ergriffen werden, er z.B. wegen Beleidigung verurteilt wird.<sup>60</sup> Die bloße Kenntnisnahme von der Meinungsäußerung fällt dagegen in den Regelungsbereich von Art. 10 Abs. 1 GG.

Auch der Schutzbereich von Art. 5 Abs. 1 Satz 2 GG ist nicht berührt. Diese Bestimmung schützt den Bestand und die ungehinderte Verbreitung der Massenmedien.<sup>61</sup> Massenmedien sind dadurch gekennzeichnet, daß Nachrichten von einer unbestimmten Vielzahl von Personen empfangen werden. E-Mail ist dagegen ein Medium der Individualkommunikation, mit dem Nachrichten an einen einzigen Empfänger oder jedenfalls an einen abgrenzbaren Kreis von Empfängern übermittelt werden.<sup>62</sup>

Auch soweit es um das Verschaffen einer Zugriffsmöglichkeit geht, ist der Schutzbereich von Art. 5 Abs. 1 GG nicht berührt, weil zumindest Art. 5 Abs. 1 Satz 1 GG insoweit kein Abwehrrecht gewährt; Art. 5 Abs. 1 Satz 2 GG ist auch unter diesem Aspekt ebenfalls nicht berührt, weil er die Massenkommunikation betrifft.

Art. 5 Abs. 1 GG ist daher für Maßnahmen zur Überwachung von E-Mail kein Prüfungsmaßstab.

## **IV. Art. 13 Abs. 1 GG**

### **1. Schutzbereich**

Art. 13 Abs. 1 GG schützt die Wohnung. Hierunter ist der Lebensraum zu verstehen, der dem einzelnen zur Entfaltung seiner Persönlichkeit dient und in dem er in Ruhe gelassen werden will, also

---

<sup>60</sup> *Pieroth/Schlink*, Rn. 246, *Jarass/Pieroth*, Art. 5 Rn. 9.

<sup>61</sup> *Jarass/Pieroth*, Art. 5 Rn. 23, 27 (Presse), 35, 39 (Rundfunk), 49, 51 (Film).

<sup>62</sup> *Kleine-Voßbeck*, S. 16. Siehe auch oben A.I.

insbesondere die Wohnräume im engeren Sinne.<sup>63</sup> Umfaßt sind aber außerdem auch Geschäftsräume, sofern sie nicht der Allgemeinheit zugänglich sind, weil die berufliche Tätigkeit ebenfalls Ausdruck der menschlichen Selbstverwirklichung ist.<sup>64</sup> Geschützt sind damit nicht nur die Wohnräume einer betroffenen Privatperson (Absender und Empfänger), sondern auch der Geschäftsraum eines beteiligten Diensteanbieters, in dem sich ein Server mit relevanten Daten befindet; dieser Raum ist der Öffentlichkeit nicht zugänglich.

Art. 13 Abs. 1 GG schützt gegen das Eindringen von Trägern öffentlicher Gewalt und damit auch der Strafverfolgungsbehörden in zweierlei Weise:

- Zum einen ist grundsätzlich ein körperliches Eindringen untersagt, d.h. das Eindringen z.B. von Polizeibeamten.
- Aber auch ein Eindringen in anderer Weise, ohne unmittelbaren Einsatz von Personen, berührt den Schutzbereich. Dies wird gerade auch durch die Regelungen zum "Lauschangriff" in Art. 13 Abs. 3 bis 5 GG deutlich, die für den Einsatz u.a. akustischer Mittel zur Strafverfolgung eine Einschränkung des Art. 13 Abs. 1 GG vorsehen. Eine solche Einschränkung wäre überflüssig, wenn schon von vornherein der Schutzbereich des Art. 13 Abs. 1 GG auf das Eindringen in körperlicher Form beschränkt wäre.

Vom Schutz des Art. 13 Abs. 1 GG nicht mehr erfaßt sind die Sicherstellung und Beschlagnahme von Gegenständen.<sup>65</sup>

---

<sup>63</sup> *Pieroth/Schlink*, Rn. 872.

<sup>64</sup> A.a.O., Rn. 876.

<sup>65</sup> A.a.O., Rn. 878a.

## **2. Eingriffscharakter strafprozessualer Maßnahmen**

### **a) Verschaffen der Zugriffsmöglichkeit**

An dieser Stelle ist zu fragen, ob in die Unverletzlichkeit der Wohnung durch Maßnahmen der Strafverfolgungsbehörden eingegriffen wird, die dazu dienen, ihnen die Möglichkeit für einen Zugriff auf E-Mails zu verschaffen. Dabei soll die Qualität des Eingriffs noch unberücksichtigt bleiben, weil dieser Aspekt erst für die Rechtfertigung des Eingriffs durch eine entsprechende gesetzliche Grundlage von Bedeutung ist.<sup>66</sup> Betroffener eines Eingriffs können sowohl Absender und Empfänger als auch die Diensteanbieter sein, weil beide Gruppen Träger des Grundrechts sind.

#### **aa) Zugriffsmöglichkeit mittels Durchsuchung**

Wenn die Strafverfolgungsbehörden den eigentlichen Zugriff auf Daten auf der Basis der vorhandenen Hardware und Datenträger durchführen wollen (z.B. durch Beschlagnahme von Datenträgern, die E-Mails oder Verbindungsdaten enthalten), so eröffnet sich ihnen diese Zugriffsmöglichkeit nur, wenn sie die Wohnung der Privatpersonen oder Diensteanbieter durchsuchen. Diese Durchsuchung ist die klassische Form eines Grundrechtseingriffs, wie er in Art. 13 Abs. 2 GG unter bestimmten Voraussetzungen zugelassen wird. Durch die Durchsuchung wird die ansonsten verbürgte Gewährleistung der Privatsphäre erheblich eingeschränkt.

#### **bb) Zugriffsmöglichkeit mittels staatlichen Hackings**

Angesichts der Tatsache, daß es bei den Maßnahmen zur Überwachung allerdings weniger auf konkrete Hardware und Datenträger, sondern auf die auf ihnen verkörperten Informationen als solche ankommt, besteht der zweite denkbare Weg der Strafverfolgungsbehörden darin, sich die Zugriffsmöglichkeit durch Hacking

---

<sup>66</sup> Dazu unten D.

zu verschaffen.<sup>67</sup> Fraglich ist, ob dieses Vorgehen ebenfalls einen Eingriff in die Unverletzlichkeit der Wohnung desjenigen bedeutet, in dessen Räumen sich der angegriffene Rechner befindet.

Einer Bewertung dieses Verhaltens als Eingriff steht nicht entgegen, daß hier keine fremde Person in eine Wohnung eindringt. Denn Eingriff ist jede dem Staat zurechenbare Maßnahme, die zu einer Verkürzung des Grundrechtsschutzes führt, indem sie ihm ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, ganz oder teilweise unmöglich macht.<sup>68</sup> Dementsprechend sind auch die unkörperlichen "Lauschangriffe", bei denen entweder von außen oder durch in der Wohnung installierte technische Mittel<sup>69</sup> das gesprochene Wort aufgezeichnet wird, als Eingriff anerkannt und deshalb in Art. 13 Abs. 3 bis 5 GG gesondert geregelt; denn diese Maßnahmen beeinträchtigen die Möglichkeit des Betroffenen zur ungestörten und unbeobachteten Entfaltung seiner Persönlichkeit.

Ob nach diesen Wertungen aber auch das Eindringen in einen Rechner unter Überwindung von Zugangsbarrieren als Eingriff in Art. 13 Abs. 1 GG anzusehen ist, ist umstritten. Zumindest für den Fall, daß die Strafverfolgungsbehörden sich Zugriffsmöglichkeiten mit einem aufgefundenen Paßwort verschaffen, wird das Vorliegen eines staatlichen Eingriffs teilweise abgelehnt, weil der Betreiber des Rechners den Zutritt unter Verwendung dieses Paßworts generell gestattet habe und es ihm unter dem Gesichtspunkt des Art. 13 GG gleichgültig sei, wer das Paßwort benutze.<sup>70</sup> Ein ande-

---

<sup>67</sup> Zum Begriff des "staatlichen Hackings" oben B.I.

<sup>68</sup> *Pieroth/Schlink*, Rn. 240.

<sup>69</sup> A.a.O., Rn. 879.

<sup>70</sup> *Kudlich*, Strafprozessuale Probleme, S. 233.

rer Teil der Literatur<sup>71</sup> sowie die Rechtsprechung<sup>72</sup> gehen dagegen von einem Eingriff aus.

Die besseren Argumente sprechen dafür, einen Eingriff anzunehmen. Eine Ähnlichkeit zur Durchsuchung besteht insofern, als beim Zugriff auf einen Rechner von außen gezielt auf einen Gegenstand eingewirkt wird, der sich innerhalb des von Art. 13 Abs. 1 GG geschützten Bereichs befindet.<sup>73</sup> Hierdurch wird die ungestörte Entfaltung der Persönlichkeit ebenfalls erheblich beeinträchtigt, weil der Inhaber der Wohnung die alleinige Kontrolle über diesen Gegenstand verliert. Die Situation ist vergleichbar mit dem Betreten einer Wohnung durch Polizeibeamte ohne Wissen des Inhabers.<sup>74</sup> Schließlich läßt sich auch nicht feststellen, daß es dem Betreiber eines Rechners gleichgültig ist, wer ein Paßwort benutzt. So verpflichten z.B. Zugangsvermittler und Betreiber von Mail-Servern üblicherweise ihre Kunden, das Paßwort geheim zuhalten und ein Bekanntwerden des Paßworts unverzüglich mitzuteilen.<sup>75</sup> Diese Klauseln sollen den Unternehmen die Kontrolle darüber ermöglichen, wer sich Zugang zu seinen Rechneranlagen verschaffen kann. Möchte ein solcher Diensteanbieter also schon die Weitergabe des Paßworts unter Privatpersonen verhindern, so kann man erst recht nicht davon ausgehen, daß er die Verwendung des Paßworts durch die staatlichen Strafverfolgungsbehörden billigen würde, zumal aus seiner Sicht die Entdeckung z.B. von E-Mails von verdächtigen Personen auf seinen Rechnern

---

<sup>71</sup> Sieber, in: Hoeren/Sieber (Hg.), Rn. 703 f., erörtert die Bestimmungen des Art. 13 Abs. 2 und 3 GG und macht dadurch deutlich, daß er bei dem gegebenen Sachverhalt einen Eingriff annimmt.

<sup>72</sup> BGH CR 1996, 488 (489).

<sup>73</sup> A.a.O.

<sup>74</sup> Bär, Online-Kommunikation, S. 617, der allerdings nicht von einem Eingriff gerade in Art. 13 Abs. 1 GG ausgeht.

<sup>75</sup> Vgl. etwa Ziff. 7.1 und 7.2 der Nutzungsbedingungen von CompuServe, <http://www.compuserve.de/cso/hilfe/win/nutzungsbedingungen/>.

für ihn die Gefahr birgt, selbst in Ermittlungen hineingezogen zu werden.<sup>76</sup>

### **b) Zugriff auf E-Mail-Inhalte, Verbindungs- und Bestandsdaten**

Art. 13 Abs. 1 GG enthält lediglich ein Abwehrrecht gegen das Eindringen des Staates in die räumliche Privatsphäre, regelt dagegen nicht, unter welchen Bedingungen z.B. Strafverfolgungsbehörden auf Gegenstände zugreifen können, die sie in der Wohnung vorfinden. Dies ist Gegenstand anderer Grundrechte, z.B. von Art. 10 Abs. 1 GG. Die Kenntnisnahme von Inhalten von E-Mails oder Verbindungs- und Bestandsdaten berührt den Schutzbereich von Art. 13 Abs. 1 GG daher nicht. Damit scheidet auch ein Eingriff aus.

## **V. Weitere Grundrechte**

### **1. Art. 12 Abs. 1 GG**

Die beteiligten Diensteanbieter werden von Art. 12 Abs. 1 GG geschützt, sofern sie – wie üblicherweise anzunehmen ist – ihre Tätigkeit längerfristig ausüben wollen und die Erzielung von Gewinn beabsichtigen. In diesem Fall üben sie einen Beruf i.S.d. Art. 12 Abs. 1 GG aus.<sup>77</sup> Das Grundrecht der Berufsfreiheit ist auf juristische Personen entsprechend anwendbar (Art. 19 Abs. 3 GG).

Einen Eingriff in dieses Grundrecht stellen sowohl Maßnahmen dar, mit denen sich die Strafverfolgungsbehörden die Zugriffsmöglichkeit auf Daten verschaffen (z.B. Durchsuchung) als auch der eigentliche Zugriff auf die Daten (z.B. durch Beschlagnahme

---

<sup>76</sup> Wie weit diese Gefahr tatsächlich besteht, kann hier nicht weiter erörtert werden. Es geht an dieser Stelle lediglich darum, die subjektive Sicht des Betreibers eines Rechners darzustellen.

<sup>77</sup> Jarass/Pieroth, Art. 12 Rn. 4.

von Datenträgern). Das gleiche gilt, soweit den Diensteanbietern Mitwirkungs- und Auskunftspflichten auferlegt werden (z.B. nach § 100b Abs. 3 StPO). In allen Fällen wird die berufliche Tätigkeit unmittelbar eingeschränkt. Der Eingriff ist der Stufe der Berufsausübungsregelungen zuzuordnen. Die Auswirkungen der Überwachungstätigkeit der Strafverfolgungsbehörden auf die Berufsfreiheit der Diensteanbieter sind allerdings im wesentlichen nicht Thema dieser Arbeit.<sup>78</sup> Art. 12 Abs. 1 GG wird daher – mit Ausnahme der Konstellation des “staatlichen Hackings” – nicht weiter berücksichtigt.

Absender und Empfänger können mangels Grundrechtsträgerschaft nicht in Art. 12 Abs. 1 GG beeinträchtigt sein.

## **2. Art. 14 Abs. 1 GG**

Die beschriebenen Maßnahmen der Strafverfolgungsbehörden stellen Inhalts- und Schrankenbestimmungen des Eigentums dar, von denen sowohl die Privatpersonen als auch die Diensteanbieter betroffen sein können. Hinsichtlich der Diensteanbieter gilt auch hier, daß die allgemeinen Auswirkungen, die Überwachungsmaßnahmen auf sie haben, nicht Gegenstand dieser Arbeit sein sollen.

## **3. Art. 2 Abs. 1 GG**

Die genannten Maßnahmen beeinträchtigen außerdem das Grundrecht der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG). Betroffen sein können sowohl Absender und Empfänger als auch die Diensteanbieter. Insbesondere ist Art. 2 Abs. 1 GG bei staatlichem Hacking beeinträchtigt. Zugriffe staatlicher Behörden auf einen Rechner über ein Netzwerk greifen erheblich in das Recht

---

<sup>78</sup> Oben Einführung II.

des Betreibers des Rechners ein, damit nach eigenem Belieben zu verfahren.<sup>79</sup>

## **VI. Verhältnis der beeinträchtigten Grundrechte**

Nicht alle der beschriebenen Grundrechte, bei denen ein Eingriff festgestellt wurde, sind für die spätere Untersuchung von Ermächtigungsgrundlagen stets relevant. Zu differenzieren ist nach den jeweiligen Maßnahmen und den jeweils betroffenen Personen.

### **1. Verschaffen der Zugriffsmöglichkeit**

Maßnahmen der Strafverfolgungsbehörden mit dem Ziel, die Möglichkeit zum Zugriff auf relevante Daten zu eröffnen, beeinträchtigen sowohl Absender und Empfänger als auch die Diensteanbieter in ihrem Grundrecht aus Art. 13 Abs. 1 GG, sofern sich die Maßnahme gegen sie richtet; bei den Diensteanbietern ist zusätzlich Art. 12 Abs. 1 GG betroffen. Art. 2 Abs. 1 und Art. 14 Abs. 1 GG treten zurück, weil nach der hier vertretenen Auffassung ein spezielles Grundrecht beeinträchtigt ist.<sup>80</sup>

Bei den Diensteanbietern tritt außerdem Art. 12 Abs. 1 GG hinter Art. 13 Abs. 1 GG ebenfalls wegen Spezialität zurück. Es läßt sich zwar nicht feststellen, daß Art. 13 Abs. 1 GG und Art. 12 Abs. 1 GG generell in einem Verhältnis der Spezialität stehen; ein solches Verhältnis ist aber in dem hier vorliegenden Einzelfall anzunehmen, daß die berufliche Tätigkeit gerade durch Eindringen in die Geschäftsräume beeinträchtigt wird.

Soweit es um das Verschaffen der Zugriffsmöglichkeit geht, ist

---

<sup>79</sup> So im Ergebnis auch *Germann*, S. 542, *Bär*, Online-Kommunikation, S. 617.

<sup>80</sup> *Pieroth/Schlink*, Rn. 339, 340. Art. 2 Abs. 1 GG bleibt dagegen anwendbar, wenn man einen Eingriff in Art. 13 Abs. 1 GG durch staatliches Hacking verneint.

daher insgesamt ausschließlich Art. 13 Abs. 1 GG Prüfungsmaßstab.

## **2. Zugriff auf E-Mail-Inhalte, Verbindungs- und Bestandsdaten**

Im Zusammenhang mit dem Zugriff der Strafverfolgungsbehörden auf die für sie relevanten Daten ist weiter zu unterscheiden:

- Die Bestandsdaten unterliegen zu keiner Zeit dem Schutz des Art. 10 Abs. 1 GG. Sie sind nur durch das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt.
- Ein Zugriff auf Inhalte und Verbindungsdaten bedeutet dagegen einen Eingriff in Art. 10 Abs. 1 GG, es sei denn, der Zugriff erfolgt auf den PC's von Absender und Empfänger. Soweit Art. 10 Abs. 1 GG gilt, kommt dagegen das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) nicht zur Anwendung, sondern tritt wegen Spezialität zurück.<sup>81</sup> Im übrigen, d.h. beim Zugriff auf den PC's, ist es dagegen anwendbar.

Art. 14 Abs. 1 GG ist Prüfungsmaßstab, wenn die Strafverfolgungsbehörden aktiv auf konkrete Sachen zugreifen, z.B. Datenträger beschlagnahmen. Zu Art. 2 Abs. 1 GG gilt das oben Gesagte.

Die Diensteanbieter können sich auf keines der hier noch zu berücksichtigenden<sup>82</sup> Grundrechte berufen. Insbesondere steht ihnen bezüglich der Daten ihrer Kunden weder ein Recht aus Art. 10 Abs. 1 GG noch ein solches aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu.

---

<sup>81</sup> BVerfG NJW 2000, 55 (56).

<sup>82</sup> Vgl. die thematischen Einschränkungen oben V.1 und 2 sowie Einführung II.

## VII. Zusammenfassung

Wie die vorangegangene Betrachtung gezeigt hat, beeinträchtigen Maßnahmen zur Überwachung von E-Mail eine Reihe von Grundrechten.

Wenn sich die Strafverfolgungsbehörden die Zugriffsmöglichkeit auf die für sie relevanten Daten ohne Mitwirkung des Betreibers eines Rechners verschaffen wollen, greifen sie damit in Art. 13 Abs. 1 GG ein. Dies gilt sowohl für eine konventionelle Durchsuchung als auch bei Eindringen in den Rechner mittels Hacking-Methoden. Betroffen sein können sowohl Absender und Empfänger als auch die Diensteanbieter. Aus praktischen Gründen erscheint aber nur ein Vorgehen gegen die Diensteanbieter sinnvoll.

Vom eigentlichen Zugriff auf Daten sind in erster Linie Absender und Empfänger in ihrem Grundrecht aus Art. 10 Abs. 1 GG betroffen. Geht es um die Einsichtnahme in Daten, die sich auf ihren PC's befinden, können sie sich auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG berufen.

Wie wichtig und notwendig es für die Erarbeitung adäquater, den Grundrechtsschutz beachtender Lösungen für neue Problemstellungen ist, die verschiedenen Eingriffe einerseits und die von ihnen betroffenen Personen andererseits auseinanderzuhalten, zeigt sich an der "Mailbox"-Entscheidung des BGH, bei der es sich um eine Leitentscheidung der Rechtsprechung im Bereich von Ermittlungen mit Bezug zu elektronischen Nachrichten handelt.<sup>83</sup> Zu entscheiden war über die Zulässigkeit eines Antrags des Generalbundesanwalts, das Einwählen in Mailboxen unter Verwendung von Paßwörtern zu gestatten, die bei dem Beschuldigten im

---

<sup>83</sup> BGH CR 1996, 488, zum folgenden S. 489.

Rahmen einer konventionellen Durchsuchung aufgefunden worden waren; außerdem sollte der Abruf der für den Beschuldigten bestimmten Nachrichten aus diesen Mailboxen erlaubt werden.

Der BGH führt hier keine klare Trennung der beiden an verschiedenen Grundrechten zu messenden Eingriffe durch, sondern vermengt Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG. Noch schwerer wiegt aber die Tatsache, daß das Gericht auch die betroffenen Personen nicht unterscheidet und meint, Art. 13 Abs. 1 GG trete hinter den schwerpunktmäßig betroffenen Art. 10 Abs. 1 GG zurück; damit entledigt es sich der strengen, nur bestimmte Typen von Eingriffen zulassenden Gesetzesvorbehalte in Art. 13 GG. Eine präzise Betrachtung führt dagegen zu dem eindeutigen Ergebnis, daß hier eine Konkurrenzsituation von Art. 13 Abs. 1 GG und Art. 10 Abs. 1 GG gar nicht vorstellbar ist, weil verschiedene Grundrechtsträger betroffen sind. Folglich kann auch Art. 13 Abs. 1 GG nicht aus Konkurrenzgründen zurücktreten.

Diese Form der Behandlung der Grundrechte wird nicht nur ihrer Bedeutung nicht gerecht, sondern trägt auch wenig zur sicherlich sehr notwendigen Schaffung von Rechtssicherheit bei. Eine rechtsstaatlich einwandfreie Lösung kann aber nur unter Beachtung der betroffenen Grundrechte erzielt werden.

## **D. Die Zulässigkeit staatlichen Hackings**

Im vorangegangenen Abschnitt wurde die Bedeutung der Grundrechte für die Beurteilung von Überwachungsmaßnahmen geklärt. Dort wurde auch bereits dargestellt, in welchen Formen sich die Strafverfolgungsbehörden die Möglichkeit zum Zugriff auf die für sie relevanten Daten verschaffen können. Dies ist zum einen in

der Form einer konventionellen Durchsuchung, zum anderen durch den Einsatz “staatlichen Hackings” denkbar. Relevant kann dieser zweite Weg, der im folgenden näher untersucht werden soll, sowohl in bezug auf die Erlangung von E-Mail-Inhalten als auch von Verbindungs- oder Bestandsdaten sein. Da es einen Eingriff in Art. 13 Abs. 1 GG zu rechtfertigen gilt,<sup>84</sup> ist zu fragen, inwieweit sich dieses Grundrecht überhaupt einschränken läßt. Anschließend muß erörtert werden, ob Gesetze existieren, die einen in Art. 13 GG vorgesehenen Vorbehalt in verfassungskonformer Weise ausfüllen.

## **I. Prüfungsmaßstab Art. 13 GG**

Anders als viele andere Grundrechte enthält Art. 13 GG keinen allgemeinen Gesetzesvorbehalt zugunsten einschränkender Gesetze, sondern sieht in Art. 13 Abs. 2 bis 5 GG nur verschiedene definierte Typen von Eingriffen vor; hinzu kommt ein qualifizierter Gesetzesvorbehalt in Art. 13 Abs. 7 GG. Die Ausnahmen nach Art. 13 Abs. 4 und 7 GG richten sich schon nach ihrem klaren Wortlaut auf die Abwehr von Gefahren und scheiden daher für die Strafverfolgung aus. Gleiches gilt im Ergebnis auch für Art. 13 Abs. 5 GG, weil bei “staatlichem Hacking” gerade keine Personen in einer Wohnung eingesetzt werden sollen. Eine gesetzliche Grundlage kann sich daher nur auf Art. 13 Abs. 2 oder 3 GG stützen.

Auch soweit nach Art. 13 Abs. 2 oder 3 GG eine Einschränkung zulässig ist, muß diese aber von einem einfachen Gesetz zugelassen sein.<sup>85</sup> Es ist deshalb die zweistufige Prüfung erforderlich, ob das Hacking von einer Norm des einfachen Rechts gedeckt ist und

---

<sup>84</sup> Oben C.IV.2.a.bb.

<sup>85</sup> *Jarass/Pieroth*, Art. 13 Rn. 10 (Durchsuchung), 14 (akustische Überwachung).

ob deren Auslegung mit der Verfassung in Einklang steht.

## **II. Durchsuchung (§§ 102, 103 StPO)**

Die Regelungen zur Durchsuchung erlauben den Strafverfolgungsbehörden das ziel- und zweckgerichtete Suchen nach Sachen, um etwas aufzuspüren, was der Inhaber der Wohnung von sich aus nicht offenlegen oder herausgeben will.<sup>86</sup> Diese Definition des verfassungsrechtlichen Begriffs der Durchsuchung (Art. 13 Abs. 2 GG) ist auch für den strafprozessualen Begriff in §§ 102, 103 StPO anerkannt.<sup>87</sup> Damit erübrigt sich hier die oben genannte zweistufige Prüfung, und es reicht zu fragen, ob das Hacking noch als “Durchsuchung” in dem dargestellten Sinn bewertet werden kann.

Im Ergebnis ist dabei festzustellen, daß eine “virtuelle Durchsuchung” von dem Bild einer Durchsuchung, wie es Art. 13 Abs. 2 GG und §§ 102, 103 StPO zugrunde liegt, zu weit entfernt ist, um noch als Durchsuchung im Sinne dieser Vorschriften gelten zu können. Bei der Durchsuchung nach traditionellem Muster handelt es sich um eine gegenüber dem Betroffenen offene Maßnahme, gekennzeichnet durch die körperliche Anwesenheit von Beamten der Strafverfolgungsbehörden.<sup>88</sup> Die virtuelle Durchsuchung würde dagegen von dem Betroffenen weitgehend unbemerkt stattfinden. Hinzu kommt, daß es Ziel der Durchsuchung sein muß, Gegenstände aufzufinden, die beschlagnahmt werden können. Bei einem Eindringen per Netzwerk kann dies aber nie der Fall sein, weil über ein Netzwerk keine körperlichen Gegenstände sichergestellt werden können.<sup>89</sup>

---

<sup>86</sup> *Pieroth/Schlink*, Rn. 878.

<sup>87</sup> Vgl. etwa *Bär*, Online-Kommunikation, S. 621, der die Formel des BVerfG im Zusammenhang mit den §§ 102, 103 StPO zitiert.

<sup>88</sup> A.a.O.

<sup>89</sup> A.a.O.; zur Beschlagnahme unten E.III.

Vom geltenden Verständnis des Begriffs der Durchsuchung ist staatliches Hacking damit nicht gedeckt. Es kommt auch nicht in Betracht, diesen Begriff entsprechend zu aktualisieren, wie dies bei Art. 10 Abs. 1 GG im Hinblick auf die modernen Techniken der Kommunikation getan wurde.<sup>90</sup> Gegen eine solche erweiternde Interpretation spricht bereits, daß es sich bei Art. 13 Abs. 2 GG um eine Ausnahmevorschrift handelt und daher eng auszulegen ist. Zudem würde damit wohl auch die Grenze des Wortsinns überschritten.

### **III. Beobachtung (§ 100c StPO)**

§ 100c Abs. 1 StPO gestattet den Strafverfolgungsbehörden den Einsatz bestimmter technischer Mittel zur Ermittlung des Aufenthaltsortes eines Beschuldigten oder zur Ermittlung des Sachverhalts; mit § 100c Abs. 1 Nr. 3 StPO wird von der in Art. 13 Abs. 3 bis 5 GG vorgesehenen Möglichkeit der akustischen Wohnraumüberwachung Gebrauch gemacht. Allen Maßnahmen nach § 100c Abs. 1 StPO ist gemeinsam, daß sie ohne Wissen des Betroffenen erfolgen.

Das Eindringen in einen Rechner wird durch § 100c Abs. 1 StPO nicht legitimiert. Keine der dort vorgesehenen Maßnahmen läßt sich als "virtuelles Zutrittsrecht" interpretieren; insbesondere beziehen sich § 100c Abs. 1 Nr. 2 und 3 StPO nur auf das gesprochene Wort. Bereits auf der Ebene des einfachen Gesetzes ist somit zweifelhaft, daß eine Grundlage für staatliches Hacking besteht.

Hinzu kommt aber das verfassungsrechtliche Argument, daß eine Auslegung des § 100c Abs. 1 StPO, die ein Eindringen in einen

---

<sup>90</sup> Oben C.I.2.

Rechner erlauben würde, an Art. 13 Abs. 2 und 3 GG gemessen werden muß. Daß das Hacking keine Durchsuchung i.S.d. Art. 13 Abs 2 GG ist, wurde bereits klargelegt. Es wäre aber auch keine akustische Wohnraumüberwachung i.S.d. Art. 13 Abs. 3 GG. Dieser verfassungsrechtliche Begriff ist wie der der Durchsuchung ebenfalls eng auszulegen. Eine Einbeziehung von in einer Wohnung ablaufenden "Datenströmen" o.ä. kommt daher nicht in Betracht. Somit geriete eine erweiternde Auslegung des § 100c Abs. 1 StPO bereits in Konflikt mit Art. 13 GG.<sup>91</sup>

#### **IV. Verdeckter Ermittler (§ 110a, 110c StPO)**

Die §§ 110a, 110c StPO regeln die Befugnis der Strafverfolgungsbehörden zum Einsatz Verdeckter Ermittler sowie die Befugnis des Verdeckten Ermittlers, eine Wohnung zu betreten.

Für die Zulässigkeit von staatlichem Hacking nach den §§ 110a, 110c StPO könnte sprechen, daß es sich hierbei – im Gegensatz zur Durchsuchung – um einen verdeckten Einsatz handelt, den die §§ 110a, 110c StPO gerade legitimieren wollen. Diese Sichtweise würde allerdings die Bedeutung des Begriffs "verdeckt" verkennen. Denn verborgen bleibt bei Einsätzen Verdeckter Ermittler nicht die Person des Verdeckten Ermittlers als solche, sondern nur seine wirkliche Identität und Funktion. Unter seiner Legende, d.h. einer ihm längerfristig verliehenen veränderten Identität, kann und soll der Ermittler dagegen offen auftreten und kann dazu auch Rechtsgeschäfte abschließen (§ 110a Abs. 2 StPO).

Aus dieser Charakteristik des Einsatzes Verdeckter Ermittler ergibt sich die Unzulässigkeit staatlichen Hackings. Möchten die Ermittler bereits die Tatsache ihres Eindringens verbergen, ist dieser Fall

---

<sup>91</sup> Vgl. Sieber, in: Hoeren/Sieber (Hg.), Rn. 704 f.

vergleichbar mit dem heimlichen Betreten einer Wohnung durch den Verdeckten Ermittler. Genau ein solches Recht schließt § 110c Satz 1 StPO aber aus, nach dem in jedem Fall das Einverständnis des Wohnungsinhabers erforderlich ist. Beim Einwählen mit einem fremden Paßwort würden sich die Strafverfolgungsbehörden den Zugang nicht mit einer Legende verschaffen. Ein Ermittler würde dann nämlich nicht unter einer eigenen, für ihn aufgebauten Identität handeln, sondern sich die Identität einer fremden Person zu eigen machen.

Eine entsprechende Befugnis der Strafverfolgungsbehörden scheidet daher bereits nach einfachem Recht aus. Eine verfassungsrechtliche Überprüfung erübrigt sich damit. Für Ermittlungen in Computernetzen erlauben es die §§ 110a, 110c StPO lediglich, daß sich ein Verdeckter Ermittler um einen Zugang zu geschlossenen Benutzergruppen unter seiner Legende bemüht,<sup>92</sup> d.h. daß ihm von diesem Kreis der Zugang *gewährt* wird.<sup>93</sup>

## **V. Überwachung der Telekommunikation (§§ 100a, 100b StPO)**

Von den Vorschriften zur Überwachung der Telekommunikation ist § 100a StPO die Eingriffsgrundlage gegenüber dem Bürger. § 100b StPO trifft ergänzende Regelungen zur Zuständigkeit und Durchführung der Überwachung; nach § 100b Abs. 3 StPO ist jeder, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu verpflichtet, die Überwachung zu ermöglichen.

Um ein Eindringen in einen Rechner zu rechtfertigen, müßte das Hacking als "Überwachung" anzusehen sein. Dieser Begriff ist gesetzlich nicht definiert; die Strafverfolgungsbehörden sind nicht

---

<sup>92</sup> Sieber, in: Hoeren/Sieber (Hg.), Rn. 707.

<sup>93</sup> Kudlich, Strafprozessuale Probleme, S. 229.

auf eine bestimmte Verfahrensart festgelegt, sondern können ihr Vorgehen der technischen Entwicklung anpassen.<sup>94</sup> Gleichwohl kann – entsprechend dem natürlichen Sprachgebrauch – als konstanter Begriffsinhalt festgehalten werden, daß hier der Einbruch des Staates in die zwischen zwei Personen vertraulich geführte Kommunikation gemeint ist. Hiervon unterscheidet sich der Vorgang der Zugangsverschaffung durch die Strafverfolgungsbehörden unter Überwindung von Zugangssperren dadurch, daß eine Kommunikation zwischen zwei Personen insoweit nicht stattfindet, vielmehr ein Beamter selbst erst eine eigene Verbindung aufbaut.<sup>95</sup>

Neben diesem Begriffsinhalt spricht auch die Existenz von § 100b Abs. 3 StPO gegen eine solche Befugnis. Danach ist der Anbieter von Telekommunikationsdiensten verpflichtet, die Überwachung zu ermöglichen. Diese Mitwirkungspflicht kann gem. §§ 100b Abs. 3 Satz 3, 95 Abs. 2 Satz 1, 70 StPO mit Ordnungsgeld und Ordnungshaft durchgesetzt werden. Daraus wird deutlich, daß nach dem Willen des Gesetzgebers eine Weigerung des Diensteanbieters nicht durch vis absoluta, sondern mit vis compulsiva überwunden werden soll. Das Eindringen in einen Rechner ohne Zustimmung des Betreibers ähnelt aber gerade der vis absoluta.

Somit ist eine Befugnis der Strafverfolgungsbehörden bereits nach einfachem Recht zweifelhaft. Hinzu kommt aber wieder das verfassungsrechtliche Argument, daß eine Auslegung des § 100a StPO, die ein Hacking zulassen würde, den Gesetzesvorbehalten des Art. 13 Abs. 2 und 3 GG entsprechen müßte. Es ist jedoch nicht ersichtlich, wie eine Überwachung i.S.d. § 100a StPO als

---

<sup>94</sup> Bär, Computerdaten, S. 326.

<sup>95</sup> Bär, Online-Kommunikation, S. 622 f.

Durchsuchung i.S.d. Art. 13 Abs. 2 GG oder akustische Wohnraumüberwachung i.S.d. Art. 13 Abs. 3 GG eingeordnet werden könnte.

Ein weiterer Konflikt würde sich zudem mit Art. 19 Abs. 1 Satz 2 GG ergeben. Danach muß jedes Gesetz, das ein Grundrecht einschränkt, dieses unter Angabe seines Artikels nennen. Weder im Normtext des § 100a StPO noch in dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses von 1968, durch das die §§ 100a, 100b StPO in ihrer ursprünglichen Fassung eingefügt wurden, noch in den weiteren Änderungsgesetzen ist jedoch ein Hinweis auf Art. 13 Abs. 1 GG enthalten. Da das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG u.a. die Funktion hat, für den Rechtsanwender klarzustellen, in welche Grundrechte eine Vorschrift eingreifen darf,<sup>96</sup> verbietet sich somit eine Auslegung, die zu einem Eingriff in das nicht genannte Grundrecht der Unverletzlichkeit der Wohnung führt.

## **VI. Beschlagnahme und Postbeschlagnahme (§§ 94, 99 StPO)**

§ 94 StPO ermöglicht es den Strafverfolgungsbehörden, Gegenstände, die als Beweismittel von Bedeutung sein können, in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. § 99 StPO dehnt die Möglichkeiten der Sicherstellung auf Postsendungen und Telegramme aus, die sich im Gewahrsam der Post- und Telekommunikationsunternehmen befinden. Die Postbeschlagnahme ist keine Beschlagnahme im engeren Sinn, sondern die Weisung, eine Postsendung bzw. ein Telegramm auszusondern und an die Strafverfolgungsbehörden auszuliefern, die sodann über eine Beschlagnahme nach § 94 StPO entscheiden.<sup>97</sup> Durch die

---

<sup>96</sup> *Pieroth/Schlink*, Rn. 310.

<sup>97</sup> *Kleinknecht/Meyer-Goßner*, § 99 Rn. 5.

Weisung werden die betroffenen Unternehmen vom Post- bzw. Telekommunikationsgeheimnis befreit (§§ 39 PostG, 85 TKG).<sup>98</sup>

Bereits aus dem Wortlaut dieser Bestimmungen ergibt sich kein Anhaltspunkt für eine Befugnis, sich den Zugang zu einem zu beschlagnahmenden Gegenstand mit staatlichem Hacking zu verschaffen. Auch zeigt die Existenz einer Vorlagepflicht nach § 95 Abs. 1 StPO, deren Erfüllung ggf. mit den Zwangsmitteln nach § 95 Abs. 2 StPO durchgesetzt werden kann, daß der Gesetzgeber den Behörden ein Recht zum Einsatz von vis absoluta zur Verschaffung der Zugriffsmöglichkeit nicht auf der Basis von § 94 StPO einräumen wollte. Hierzu hat er sie vielmehr auf die Durchsuchung nach §§ 102, 103 StPO verwiesen. Daß eine "virtuelle Durchsuchung" nach §§ 102, 103 StPO nicht zulässig ist, kann hinsichtlich §§ 94, 99 StPO nicht zu einem anderen Ergebnis führen.

## **VII. Zusammenfassung**

Die Untersuchung möglicher gesetzlicher Ermächtigungsgrundlagen hat gezeigt, daß es den Strafverfolgungsbehörden nicht erlaubt ist, sich den Zugang zu relevanten Informationen durch den Einsatz von Hacking-Methoden zu verschaffen. Zu beachten ist, daß insoweit ein Eingriff in Art. 13 Abs. 1 GG gerechtfertigt werden muß, was durch einfachgesetzliche Normen ohnehin nur in den eng begrenzten Ausnahmefällen der Art. 13 Abs. 2 und 3 GG möglich ist.

In der Regel scheidet eine Zulassung staatlichen Hackings bereits an einer fehlenden Stütze in den einfachgesetzlichen Normen der StPO. Selbst bei Verneinung eines Eingriffs in Art. 13 Abs. 1 GG

---

<sup>98</sup> A.a.O., Rn. 1.

ist diese Ermittlungsmethode daher rechtswidrig. Nach der hier vertretenen Auffassung würde eine entsprechend weite Auslegung zudem gegen Art. 13 Abs. 2 und 3 verstoßen.

## **E. Der Zugriff auf Inhalte von E-Mails**

Entsprechend der Erörterung der Zulässigkeit staatlichen Hackings geht es in diesem Abschnitt und im Abschnitt F. darum, die Normen zu klären, die einen Eingriff in die insoweit beeinträchtigten Grundrechte der Art. 10 Abs. 1 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie Art. 14 GG rechtfertigen können. Auch hier ist zuvor wieder zu fragen, welche Möglichkeiten einer Einschränkung die beeinträchtigten Grundrechte überhaupt vorsehen.

In diesem Abschnitt sollen zunächst – ähnlich den Ausführungen zu Art. 10 Abs. 1 GG – zunächst diejenigen Vorschriften ausgefiltert werden, die offensichtlich generell nicht zum Zugriff auf Inhalte von E-Mails geeignet sind; Abschnitt F. behandelt dann die verbliebenen Normen im Detail unter Berücksichtigung der verschiedenen Phasen der Übermittlung von E-Mails.<sup>99</sup>

### **I. Gesetzesvorbehalte**

Die Prüfung wird dadurch vereinfacht, daß alle hier zu beachtenden Grundrechte nur einem einfachen Gesetzesvorbehalt unterliegen und daher grundsätzlich bis zur Grenze der Wesensgehaltsgarantie eingeschränkt werden dürfen;<sup>100</sup> für Art. 14 Abs. 1 GG, der ohnehin nur bei der Beschlagnahme eine Rolle spielt, ergibt sich diese Konsequenz aus dem allgemeinen Vorbehalt der Inhalts- und Schrankenbestimmung. Auch innerhalb dieses Spielraums

---

<sup>99</sup> Vgl. C.I.2 und 3.

<sup>100</sup> So für Art. 10 von Münch/Kunig-Löwer, Art. 10 Rn. 27.

müssen einschränkende Gesetze aber einige Anforderungen erfüllen. So muß das Gesetz, das den Eingriff zuläßt, Art, Umfang und Voraussetzungen des Eingriffs in den wesentlichen Zügen beschreiben.<sup>101</sup> Weiterhin ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dieses Prinzip fordert, daß der Staat in Grundrechte nicht stärker eingreift als erforderlich; außerdem muß zwischen dem Eingriff und dem Gewicht und der Bedeutung des beeinträchtigten Grundrechts ein angemessenes Verhältnis bestehen.<sup>102</sup>

## **II. Überwachung der Telekommunikation (§§ 100a, 100b StPO)**

Für den Zugriff auf Inhalte von E-Mails ist von entscheidender Bedeutung zunächst der Inhalt des Begriffs "Telekommunikation" in § 100a Abs. 1 Satz 1 StPO. Zu fragen ist, ob dieser auch Computerdaten wie E-Mails erfaßt.

Der Begriff der Telekommunikation wurde in § 100a StPO durch das Begleitgesetz zum Telekommunikationsgesetz (TKG) vom 17. Dezember 1997 eingefügt.<sup>103</sup> Dadurch sollte der Sprachgebrauch der StPO an die Terminologie des TKG angepaßt werden.<sup>104</sup> Telekommunikation im strafprozessualen Sinn erscheint damit durch das TKG, insbesondere § 3 Nr. 16 TKG, definiert als der technische Vorgang des Aussendens, Übermittels oder Empfangens von Nachrichten jeglicher Art. Unter den Begriff der Nachricht fallen zweifellos auch Computerdaten wie E-Mails. Eine Anwendung der §§ 100a, 100b StPO zum Zugriff auf E-Mails zum Zweck ihrer Überwachung erscheint daher generell möglich.

---

<sup>101</sup> *Pieroth/Schlink*, Rn. 264, 266.

<sup>102</sup> *Jarass/Pieroth*, Art. 20 Rn. 86.

<sup>103</sup> BGBl 1997 I, 3108.

<sup>104</sup> *Bär*, Online-Kommunikation, S. 632; dort auch zur Rechtslage nach dem früheren Begriff des "Fernm eldeverkehrs".

### III. Beschlagnahme (§ 94 StPO)

Eine Beschlagnahme von E-Mail-Inhalten setzt voraus, daß es sich dabei um Gegenstände i.S.d. § 94 StPO handelt. Unter Gegenständen als Objekt der Beschlagnahme werden herkömmlich bewegliche und unbewegliche Sachen verstanden.<sup>105</sup> Hieran ist auch im Bereich der modernen Kommunikation festzuhalten; auch insoweit ist eine Beschlagnahme nur möglich, soweit körperliche Gegenstände vorliegen.<sup>106</sup>

Gegen eine erweiternde Auslegung, die auch Computerdaten unabhängig von einer Verkörperung umfaßt, spricht vor allem der allgemeine Sprachgebrauch, der unter dem Begriff Gegenstand ein körperliches Objekt versteht.<sup>107</sup> Darüber hinaus sprechen auch systematische Aspekte für die traditionelle Auslegung, weil in § 103 Abs. 1 Satz 1 StPO neben den "Gegenständen" auch die – für sich betrachtet unkörperlichen – "Spuren" erwähnt werden; dies wäre überflüssig, wenn sich bereits der Begriff des Gegenstandes auf unkörperliche Objekte erstrecken würde.<sup>108</sup> Auch § 97 StPO, der Beschlagnahmeverbote regelt, geht mit dem Begriff des Gewahrsams in § 97 Abs. 2 von körperlichen Objekten aus.<sup>109</sup> Aus diesen Überlegungen folgt, daß E-Mails als gedanklicher Inhalt nicht beschlagnahmefähig, weil unverkörperte Informationen sind.

Eine Beschlagnahme kann aber stattfinden, soweit sie sich auf die Datenträger bezieht, auf denen die Nachrichten gespeichert sind; dann liegen nämlich körperliche Gegenstände vor.<sup>110</sup> Da E-Mails

---

<sup>105</sup> *Kleinknecht/Meyer-Goßner*, § 94 Rn. 4.

<sup>106</sup> BGH CR 488 (489).

<sup>107</sup> *Bär*, Computerdaten, S. 242, 245.

<sup>108</sup> A.a.O., S. 243.

<sup>109</sup> *Lemcke*, S. 21.

<sup>110</sup> *Kleinknecht/Meyer-Goßner*, § 94 Rn. 4.

während des gesamten Übermittlungsvorgangs vom Absender bis zum Empfänger nahezu ständig auf irgendeinem Speichermedium (Festplatte in den PC's von Absender und Empfänger, Festplatte im Mail-Server des Empfängers) festgehalten werden, erscheint eine Anwendung von § 94 StPO auf E-Mails grundsätzlich möglich.

#### **IV. Postbeschlagnahme (§ 99 StPO)**

Auch bei § 99 StPO stellt sich die Frage, ob dem Begriff der Postsendung nur körperliche Gegenstände zuzuordnen sind oder auch die für sich betrachtet unkörperlichen E-Mails darunter fallen können. Für letztere Interpretation könnte der Gedanke sprechen, daß der E-Mail-Dienst inzwischen weithin als Ersatz für konventionelle papiergebundene Briefe verwendet wird. Dies kann jedoch im Ergebnis nicht dazu führen, den Begriff der Postsendung entsprechend zu erweitern.

Dagegen spricht schon der enge Zusammenhang mit § 94 StPO; da dieser nur die Beschlagnahme körperlicher Objekte erlaubt, würde eine Weisung zur Aussonderung unkörperlicher Objekte keinen Sinn machen. Dementsprechend verweist auch § 99 StPO auf den "Gewahrsam" der Post- und Telekommunikationsunternehmen, der nur an körperlichen Gegenständen bestehen kann.<sup>111</sup> Auch geht die nachfolgende Vorschrift des § 100 StPO, die die weitere Behandlung der Postsendungen betrifft, in ihrem Abs. 3 eindeutig von verkörperten Nachrichten aus, indem sie das "Öffnen" der Nachrichten, d.h. die erstmalige Kenntnisnahme, dem Richter vorbehält.<sup>112</sup>

---

<sup>111</sup> Bär, Computerdaten, S. 293.

<sup>112</sup> Kleine-Voßbeck, S. 141.

Schließlich kommt ein historisches Argument hinzu. Der Gesetzgeber hat durch das Begleitgesetz zum TKG in § 99 StPO den Begriff “Briefe und Sendungen” durch “Postsendungen” und die Ausdrücke “auf der Post” bzw. “auf den Telegraphenanstalten” durch das Tatbestandsmerkmal des Gewahrsams eines geschäftsmäßigen Anbieters von Post- oder Telekommunikationsdiensten ersetzt; ansonsten blieb die Vorschrift aber unverändert. Wäre es im Sinne des Gesetzgebers gewesen, auch moderne Kommunikationsformen in § 99 StPO einzubeziehen, hätte man hier eine entsprechende Klarstellung im Wortlaut erwarten dürfen. Im Gegenteil wird aber in den Gesetzesmaterialien ausdrücklich festgestellt, daß mit der Änderung nur die organisatorischen Neuerungen bei der Erbringung von Post- und Telekommunikationsdienstleistungen berücksichtigt, dagegen nicht die Möglichkeiten der Beschlagnahme erweitert werden sollten.<sup>113</sup>

Gegenstand der Postbeschlagnahme nach § 99 StPO können daher nur körperliche Objekte sein. Fraglich ist aber, ob eine solche verkörperte Postsendung stets schon dann vorliegt, wenn die E-Mail in verkörperter Form existiert, d.h. auf einem Datenträger gespeichert ist. Teilweise wird dies ohne weitere Begründung für möglich gehalten.<sup>114</sup> Allerdings besteht zwischen dem konventionellen Brief, für den § 99 StPO anwendbar ist, und dem E-Mail-Versand ein wesentlicher Unterschied: Während beim Brief das Trägermedium, in dem die Informationen, d.h. der Inhalt, verkörpert ist, nämlich das Papier, zur Übermittlung bestimmt ist, ist dies bei einer E-Mail gerade nicht der Fall; hier bleibt der Datenträger stets im Gewahrsam z.B. des Betreibers des Mail-Servers,

---

<sup>113</sup> BT-Drucks. 13/8016, S. 25 f.

<sup>114</sup> Bär, Anmerkung, S. 177.

nur die Informationen, d.h. die E-Mail, werden übermittelt.<sup>115</sup> Eine Subsumtion der auf dem Datenträger verkörperten Nachricht unter den Begriff der Postsendung würde daher letztlich doch wieder das Abstellen auf ein übermitteltes unkörperliches Objekt bedeuten.

Auch eine Subsumtion von E-Mails unter den Begriff des Telegramms scheidet aus. Unter dem Telegramm wird im allgemeinen Sprachgebrauch eine ganz bestimmte Kommunikationsweise verstanden. Einer Auslegung, die die Grenze des Wortsinns beachten muß, sind daher enge Grenzen gesetzt, die mit der Einbeziehung von E-Mails bereits überschritten wären.

Die Anwendung von § 99 StPO auf den E-Mail-Verkehr ist daher nicht möglich.<sup>116</sup>

## **V. Durchsuchung (§§ 102, 103 StPO)**

Hinsichtlich des Zugriffs auf E-Mails, d.h. zur Rechtfertigung eines möglichen Eingriffs in Art. 10 Abs. 1 GG oder Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und ggf. Art. 14 Abs. 1 GG, enthält § 102 StPO keine Regelung. Für die weitere Behandlung aufgefundener Sachen gelten vielmehr die Regeln der Beschlagnahme nach §§ 94 ff. StPO. Auf die nähere Abgrenzung der Objekte, auf die sich eine Durchsuchung richten darf, kommt es daher im vorliegenden Zusammenhang nicht an.

---

<sup>115</sup> Daher besteht auch ein wesentlicher Unterschied zu der Kommunikationsform des "Telebriefs", bei dem eine Postbeschlagnahme nach § 99 StPO für zulässig erachtet wird (*Bär*, Computerdaten, S. 296). Beim Telebrief wird die Nachricht von einem Telefaxgerät zu einer Poststelle übertragen, dort ausgedruckt und dieser Ausdruck sodann dem Empfänger zugestellt. Hier ist Gegenstand der Übermittlung nicht lediglich der Nachrichteninhalt, sondern auch das Trägermedium selbst.

<sup>116</sup> So im Ergebnis auch *Palm/Roy*, Mailboxen, S. 1794, *Bär*, Computerdaten, S. 297; a.A. dagegen *Bär*, Anmerkung, S. 177.

Ein Zugriffsrecht besteht im Rahmen einer Durchsuchung nur insoweit, als der Staatsanwaltschaft nach § 110 StPO die Durchsicht von Papieren gestattet ist, worunter auch Datenträger zu verstehen sind.<sup>117</sup> Ziel darf lediglich sein, die Beweisbedeutung des Inhalts des Datenträgers und damit der E-Mails festzustellen. Ein dauerhafter Zugriff auf E-Mails, wie er hier zur Diskussion steht, ist dagegen auf der Basis dieser Bestimmung nicht möglich.

## **VI. Beobachtung (§ 100c StPO)**

§ 100c Abs. 1 StPO enthält keine Grundlage für einen Zugriff auf E-Mails und damit eine Rechtfertigung für einen Eingriff in die genannten Grundrechte. § 100c Abs. 1 Nr. 2 und 3 StPO beziehen sich ausdrücklich nur auf das gesprochene Wort; eine Einbeziehung von E-Mail scheidet hier eindeutig aus. Auch § 100c Abs. 1 Nr. 1 StPO kann nicht herangezogen werden. In seiner Alternative a beschränkt er sich auf Lichtbilder und Bildaufzeichnungen; unter den besonderen für Observationszwecke bestimmten Mitteln der Alternative b sind Einrichtungen wie Peilsender, Bewegungsmelder oder Nachtsichtgeräte zu verstehen.<sup>118</sup> Eine Anwendung auf den E-Mail-Verkehr ist wegen des klaren Wortlauts auch hier nicht möglich.

## **VII. Verdeckter Ermittler (§§ 110a, 110c StPO)**

Die Regelungen zum Verdeckten Ermittler enthalten keinerlei Bestimmungen, die auf den Zugriff auf Inhalte von E-Mails angewendet werden könnten. Nach § 110a StPO dürfen Verdeckte Ermittler zwar unter bestimmten Voraussetzungen zur Aufklärung von Straftaten eingesetzt werden. Eine Ermächtigung zu weitergehenden Maßnahmen, die in Grundrechte der Betroffenen

---

<sup>117</sup> Sieber, in: Hoeren/Sieber (Hg.), Rn. 692.

<sup>118</sup> Kleinknecht/Meyer-Goßner, § 100c Rn. 2.

eingreifen, ist damit aber nicht verbunden. Auch § 110c StPO sieht lediglich vor, daß ein Verdeckter Ermittler eine Wohnung mit Zustimmung des Inhabers betreten darf. Wie § 110c Satz 3 StPO feststellt, gelten ansonsten die übrigen Normen der StPO. Dies bedeutet, daß es dem Verdeckten Ermittler aufgrund der §§ 110a, 110c StPO nicht gestattet ist, eine strafprozessuale Zwangsmaßnahme, z.B. eine Beschlagnahme, vorzunehmen. Ebenso darf sich ein Verdeckter Ermittler ohne Zustimmung des Berechtigten auch keine Kenntnis von E-Mails verschaffen; dies wäre ein Eingriff in Art. 10 Abs. 1 GG oder Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, für den eine Rechtfertigung in den §§ 110a, 110c StPO fehlt.

### **VIII. Zusammenfassung**

Ziel dieses Abschnitts war es, die generelle Anwendbarkeit von Vorschriften der StPO für den Zugriff auf Inhalte von E-Mails zu untersuchen. Als Ergebnis läßt sich festhalten, daß die §§ 100c, 110a, 110c StPO bereits wegen der in ihnen geregelten speziellen Befugnisse zur Rechtfertigung der hier in Rede stehenden Grundrechtseingriffe nicht herangezogen werden können. Gleiches gilt für die Postbeschlagnahme nach § 99 StPO. Hier kommt zwar eine entsprechende Auslegung des Begriffs der Postsendung in Betracht; letztlich besteht zwischen einer – auch zwischengespeicherten und damit verkörperten – E-Mail und dem klassischen Brief, den § 99 StPO im Blick hatte, aber ein so großer Unterschied, daß eine Anwendung dieser Vorschrift schon auf eine unzulässige Analogie hinauslaufen würde.

Die Regelungen zur Durchsuchung (§§ 102, 103 StPO) dienen in erster Linie dazu, den Strafverfolgungsbehörden den Zugang zu Gegenständen zu ermöglichen, um diese ggf. nach § 94 StPO zu

beschlagnahmen. Im Zusammenhang mit der Durchsuchung erlaubt § 110 StPO vorübergehend die Durchsicht von Datenträgern. Eine echte Befugnis zum dauerhaften Zugriff auf Inhalte von E-Mails ist damit aber nicht verbunden.

Einen Zugriff auf E-Mails unter Überwindung der anfangs genannten Grundrechte könnten dagegen grundsätzlich die §§ 100a und 94 StPO ermöglichen.

## **F. Der Zugriff in den einzelnen Phasen der Übermittlung**

Im vorangegangenen Abschnitt wurde bereits die generelle Anwendbarkeit verschiedener Befugnisnormen zum Zugriff auf Inhalte von E-Mails untersucht. Das gefundene Ergebnis hat allerdings nur vorläufigen Charakter. Berücksichtigt werden muß nämlich auch die Tatsache, daß die E-Mail-Kommunikation in den bereits beschriebenen verschiedenen Phasen abläuft.<sup>119</sup> Wie schon die Erörterung des Art. 10 Abs. 1 GG gezeigt hat, führen diese technischen Gegebenheiten durchaus auch zu unterschiedlichen rechtlichen Konstellationen.<sup>120</sup> Daher muß auch hinsichtlich der Rechtfertigung der Grundrechtseingriffe entsprechend differenziert werden.

### **I. E-Mails auf dem PC des Absenders**

Insoweit geht es darum, einen Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) zu rechtfertigen; Art. 10 Abs. 1 GG ist dagegen nicht betroffen.<sup>121</sup>

---

<sup>119</sup> Oben A.II.4.

<sup>120</sup> Vgl. oben C.I.3.

<sup>121</sup> Zusammenfassend oben C.VI.2.

Je nach Vorgehen der Strafverfolgungsbehörden kann auch ein Eingriff in das Eigentum (Art. 14 Abs. 1 GG) vorliegen,<sup>122</sup> für den eine Ermächtigungsgrundlage notwendig ist.

### **1. Zugriff nach § 100a StPO**

Soweit sich Maßnahmen der Strafverfolgungsbehörden darauf richten, Einsicht in die noch nicht abgesandten E-Mails zu nehmen, können sie ihr Vorgehen nicht auf § 100a StPO stützen. Nach § 100a StPO zulässig ist die Überwachung der Telekommunikation. Ohne den genauen Inhalt dieses Begriffs bereits hier definieren zu müssen, ist ohne weiteres ersichtlich, daß ein Telekommunikationsvorgang noch nicht vorliegt, wenn der Absender die verfaßte Nachricht in seinem Mail User Agent in den "Ausgangskorb" legt.<sup>123</sup>

### **2. Zugriff nach § 94 StPO**

Grundsätzlich möglich ist dagegen eine Beschlagnahme nach § 94 Abs. 1 StPO. Auf dem PC des Absenders gespeicherte E-Mails sind beschlagnahmefähig, weil sie auf einem Datenträger verkörpert sind. Als solche unterfallen sie dem Begriff des Gegenstands i.S.d. § 94 Abs. 1 StPO.<sup>124</sup> Näher zu betrachten sind an dieser Stelle jedoch der Umfang sowie die Art und Weise der Beschlagnahme. Da hier ein Eingriff in Art. 14 Abs. 1 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zur Diskussion steht, fordert der Grundsatz der Verhältnismäßigkeit von den Strafverfolgungsbehörden, möglichst schonend vorzugehen, um diese Grundrechte nicht mehr als nötig zu beeinträchtigen.

---

<sup>122</sup> Oben C.V.2.

<sup>123</sup> Vgl. die parallele Erwägung zu Art. 10 Abs. 1 GG oben C.I.3.a.

<sup>124</sup> Kudlich, Strafprozessuale Probleme, S. 229; oben E.III.

### **a) Umfang der Beschlagnahme**

Gemäß § 94 Abs. 1 StPO darf sich die Beschlagnahme nur auf solche Gegenstände erstrecken, die als Beweismittel in Betracht kommen. Fraglich ist, welche Konsequenzen dies für die Beschlagnahme von Computeranlagen hat.

Sofern E-Mails auf einem von der Zentraleinheit des PC's getrennten Medium, z.B. einer CD-ROM, gespeichert sind, kann dieser Datenträger beschlagnahmt werden. Dies gilt im Prinzip auch dann, wenn sich auf dem Datenträger noch andere, für die Strafverfolgung nicht relevante Daten befinden, denn technisch gesehen ist es nicht möglich, die beweisrelevanten von den nicht relevanten Daten und von dem Gegenstand, auf dem sie verkörpert sind, zu trennen. Die Beweisbedeutung erstreckt sich deshalb stets auf den gesamten Datenträger.<sup>125</sup>

Problematischer ist die Situation dagegen, wenn sich die E-Mails, wie sehr häufig, auf der in der Zentraleinheit eingebauten Festplatte befinden. Dann stellt sich die Frage, ob die Beschlagnahme der gesamten Zentraleinheit zulässig ist. Dies hängt letztlich davon ab, ob man die Zentraleinheit als einheitlichen Gegenstand betrachten kann oder auf die einzelnen darin eingebauten Bestandteile abstellen muß.<sup>126</sup> Da es gerade Zweck des § 94 StPO ist, den staatlichen Strafverfolgungsbehörden Zugriff auf Beweismittel zu verschaffen, kann die Festplatte nur dann isoliert betrachtet werden, wenn sie allein noch einen Beweiswert hat, d.h. weiterhin ein Zugriff auf die auf ihr gespeicherten E-Mails möglich ist.

Dies muß zumindest bei handelsüblichen PC's bejaht werden. Eine Festplatte läßt sich hier relativ einfach durch Lösen einiger

---

<sup>125</sup> Bär, Computerdaten, S. 254.

<sup>126</sup> A.a.O., S. 257.

Schrauben und Ziehen einiger Stecker entfernen, ohne dabei Schaden zu nehmen. Eine Auswertung des Inhalts erscheint ebenfalls ohne größere Schwierigkeiten möglich; dafür sprechen zum einen die jedenfalls im Bereich der Standard-PC's sehr weit vorgeschrittene Standardisierung, zum anderen die inzwischen bei den Strafverfolgungsbehörden vorhandene<sup>127</sup> technische Ausstattung. Für den Regelfall ist daher die restliche Zentraleinheit zum Auslesen der Festplattendaten nicht erforderlich und ihre Beschlagnahme somit unzulässig.<sup>128</sup>

### **b) Art und Weise der Sicherstellung**

Auch wenn nach den dargestellten Grundsätzen die Beschlagnahme der gesamten Festplatte zulässig ist, ist allerdings festzustellen, daß für die Strafverfolgungsbehörden in der Regel nur ein kleiner Teil der auf einem Datenträger gespeicherten Daten relevant ist. Dies gilt zumindest dann, wenn es sich bei dem zu beschlagnehmenden Medium um die Festplatte des PC's handelt. Diese enthält üblicherweise das Betriebssystem und die Anwendungsprogramme. Die vom Benutzer selbst angelegten Verzeichnisse und Dateien machen demgegenüber nur einen Bruchteil aus.

Angesichts dieser Tatsachen könnte die Inverwahrungnahme der Festplatte gegen den Grundsatz der Verhältnismäßigkeit verstoßen, und zwar sowohl hinsichtlich Art. 14 Abs. 1 GG als auch in bezug auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das Eigentum könnte mehr als erforderlich eingeschränkt sein, weil die Inbesitznahme zur Funktionsunfähigkeit des gesamten Rechners führt und dem Betroffenen außerdem die Möglichkeit genommen wird, von den als Eigentum geschützten Nutzungsrechten an der auf der

---

<sup>127</sup> A.a.O., S. 256.

<sup>128</sup> Im Ergebnis mit Blick auf mögliche Veränderungen der Hardware a.A. *Bär*, a.a.O., S. 260.

Festplatte enthaltenen Software Gebrauch zu machen. In das Recht auf informationelle Selbstbestimmung könnte mehr als unvermeidlich eingegriffen werden, wenn sich auf dem Datenträger noch andere persönliche Daten befinden, von denen die Behörden im Zuge ihrer Ermittlungen zwangsläufig Kenntnis nehmen werden.

Bereits § 94 Abs. 1 StPO sieht dem Gedanken der Erforderlichkeit entsprechend vor, daß Gegenstände nicht nur in Verwahrung genommen, sondern auch in anderer Weise sichergestellt werden können. Hinsichtlich der Beschlagnahme von Datenträgern kann dies insbesondere die Anfertigung von Kopien bedeuten.<sup>129</sup> Zu fragen ist daher, ob die Strafverfolgungsbehörden auf Antrag des Betroffenen nicht nur berechtigt, sondern sogar verpflichtet wären, den Datenträger beim Betroffenen zu belassen und statt dessen Kopien der relevanten Daten, im vorliegenden Zusammenhang demnach Kopien der E-Mails, anzufertigen. Dies richtet sich danach, ob der mit der Inverwahrungnahme verfolgte Zweck ebenso gut durch die Anfertigung von Kopien erreicht werden kann; bei Bejahung dieser Voraussetzung wäre der Eingriff der Inverwahrungnahme nicht erforderlich und daher unzulässig.

Da § 94 StPO der Beschaffung von Beweismitteln dient, ist entscheidend, ob die angefertigten Kopien den gleichen Beweiswert wie der originale Datenträger besitzen. Im Hinblick auf praktische Schwierigkeiten<sup>130</sup> und die Möglichkeiten des Betroffenen, den Datenträger zu manipulieren, wenn er weiterhin in seinem Besitz bleibt,<sup>131</sup> wird ein gleicher Beweiswert teilweise abgelehnt.

---

<sup>129</sup> *Kleinknecht/Meyer-Goßner*, § 94 Rn. 16a; a.A. *Lemcke*, S. 100 (lediglich Ersatz für eine Sicherstellung).

<sup>130</sup> *Bär*, Computerdaten, S. 272.

<sup>131</sup> *Lemcke*, S. 98 f.

Letztlich kommt es aber wohl auf die Umstände des Einzelfalls an.<sup>132</sup> Sofern man danach aber die Anfertigung von Kopien als ebenso geeignet wie die Inverwahrnehmung des Original-Datenträgers betrachtet, sind die Strafverfolgungsbehörden auf Antrag des Betroffenen zur Herstellung von Kopien verpflichtet. Denn das Gebot der Verhältnismäßigkeit ist ein zwingender Grundsatz, weil es darum geht, Eingriffe in Grundrechte zu rechtfertigen.

## **II. Übertragung der E-Mails zum Mail-Server des Empfängers**

In dieser Situation ist nur Art. 10 Abs. 1 beeinträchtigt.<sup>133</sup>

### **1. Zugriff nach § 100a StPO**

Eine Überwachung der Internet-Verbindung des Absenders, und damit auch abgesendeter E-Mails, ist durch § 100a StPO gedeckt. Insoweit findet nach einhelliger Ansicht von Rechtsprechung und Literatur eine Telekommunikation i.S.d. § 100a StPO statt, die überwacht werden kann.<sup>134</sup> Der Eingriff in Art. 10 Abs. 1 GG ist damit in diesem Bereich gerechtfertigt, sofern die übrigen Voraussetzungen, insbesondere der Verdacht einer Katalogtat, vorliegen.

Technisch kann die Überwachung wie bei der "klassischen" Fernmeldeüberwachung durch Aufschalten auf den Anschluß des Betroffenen realisiert werden. Ein Ansetzen an den eigentlichen Komponenten des Internet, dem Terminal-Server und den Routern, erscheint dagegen wegen der Vielzahl der anfallenden Daten und der Ungewißheit des Übertragungswegs nicht sinnvoll.<sup>135</sup>

---

<sup>132</sup> So andererseits ebenfalls *Bär*, Computerdaten, S. 271.

<sup>133</sup> Oben C.I.3.b. und VI.

<sup>134</sup> LG Hanau MMR 2000, 175; *Bär*, Anmerkung, S. 176, *Kudlich*, Strafprozessuale Probleme, 230 f., *Palm/Roy*, Mailboxen, S. 1793.

<sup>135</sup> Vgl. oben B.II.

## **2. Zugriff nach § 94 StPO**

Umgekehrt scheidet eine Beschlagnahme gemäß § 94 StPO während der Übermittlungsphase nach ebenso einhelliger Ansicht aus.<sup>136</sup> Es fehlt hier an dem erforderlichen körperlichen Gegenstand,<sup>137</sup> weil die Übertragung in unkörperlicher Form mittels elektromagnetischer oder optischer Signale erfolgt.

## **III. Nachrichten auf dem Mail-Server des Empfängers**

Auch die auf dem Mail-Server des Empfängers für diesen zwischengespeicherten E-Mails sind von Art. 10 Abs. 1 GG geschützt, was zur Verdrängung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG führt.<sup>138</sup> Daher muß ein Eingriff in dieses Grundrecht gerechtfertigt werden.

### **1. Zugriff nach § 100a StPO**

Während in den bisher beschriebenen Konstellationen Einigkeit besteht, wird die Anwendbarkeit von § 100a StPO kontrovers diskutiert für den Fall, daß die Ermittlungsbehörden auf Inhalte von E-Mails zugreifen, die sich auf dem Mail-Server des Empfängers befinden. Ausgangspunkt dürfte die Entscheidung des Ermittlungsrichters des BGH vom 31. Juli 1995 gewesen sein.<sup>139</sup> In dem Beschluß wird es dem Generalbundesanwalt gestattet, auf der Grundlage von § 100a StPO für den Beschuldigten bestimmte Nachrichten aus einer Mailbox abzurufen. Außerdem darf dieser Abruf ohne Wissen des Betreibers der Mailbox erfolgen, indem die Strafverfolgungsbehörden Paßwörter des Beschuldigten übermitteln, die bei ihm bei einer Durchsuchung aufgefunden wurden.

---

<sup>136</sup> Siehe die in Fn. 134 genannten Fundstellen.

<sup>137</sup> Oben E.III.

<sup>138</sup> Oben C.I.3.c und VI.

<sup>139</sup> BGH CR 1996, 488 = NJW 1997, 1934; Darstellung des Sachverhalts bei Kudlich, Mailbox, S. 209.

Daß es den Strafverfolgungsbehörden auch auf der Grundlage von § 100a StPO nicht erlaubt ist, mit einem fremden Paßwort in einen Rechner einzudringen und sich so die Möglichkeit zum Zugriff auf E-Mails zu verschaffen, wurde bereits festgestellt.<sup>140</sup> Hier ist daher nur noch zu erörtern, ob ein Abruf der Nachrichten in Zusammenarbeit mit dem Betreiber des Mail-Servers – die ggf. über § 100b Abs. 3 Satz 3 StPO erzwungen werden könnte – zulässig ist.

### **a) Überblick über den Meinungsstand**

Nach der Rechtsprechung ist auch ein Abruf von Nachrichten von einem Mail-Server eine Überwachung der Telekommunikation i.S.d. § 100a StPO. Sowohl der BGH<sup>141</sup> als auch das LG Hanau<sup>142</sup> ordnen die Maßnahme dieser Norm zu. Der BGH führt sinngemäß aus, es handele sich bei einem Server, der einen Zugriff von außen auf seine Daten erlaube, um einen Teil einer Telekommunikationsanlage; auch die Nachrichtenübermittlung von und zu dieser Anlage sei deshalb Telekommunikation.<sup>143</sup> Nach dem LG Hanau folgt die Anwendung von § 100a StPO daraus, daß eine Aufspaltung des komplexen Übermittlungsvorgangs in mehrere Phasen nicht in Betracht komme. Daher müsse § 100a StPO nicht nur während der eigentlichen Übertragung der E-Mails im Netz, sondern auch während ihrer "Ruhephase" auf einem Server angewen-

---

<sup>140</sup> Oben D., insbesondere V.

<sup>141</sup> BGH CR 1996, 488 (489).

<sup>142</sup> LG Hanau MMR 2000, 175 (175).

<sup>143</sup> Der BGH nennt außerdem den Gesichtspunkt, daß der Gesetzgeber mit § 100a StPO gerade auch ein verdecktes Vorgehen zur Aufklärung von schwerstkrimineller Tätigkeit zulassen wollen und es daher nicht sachgerecht sei, die Strafverfolgungsbehörden auf offene Maßnahmen wie Durchsuchung und Beschlagnahme zu beschränken. Dieser Teil der Begründung betrifft den vom BGH nicht deutlich unterschiedenen Eingriff des Eindringens in ein Computersystem. Nach der hier vertretenen Auffassung kann eine Telekommunikationsüberwachung wohl heimlich gegenüber dem Beschuldigten, nie aber heimlich gegenüber dem Betreiber des Mail-Servers durchgeführt werden. Siehe dazu oben D.V sowie C.VII.

det werden.

In der Literatur sind die Auffassungen zur Anwendung des § 100a StPO geteilt. Die ablehnenden Stimmen sehen in einem Abruf von Nachrichten von einem Mail-Server begrifflich keine Maßnahme zur Überwachung der Telekommunikation.<sup>144</sup> Die Befürworter<sup>145</sup> halten dagegen diese Voraussetzungen für gegeben.<sup>146</sup>

### **b) Begriff der Telekommunikation**

Von vornherein kommt eine Überwachung des E-Mail-Verkehrs durch Abruf von Nachrichten, die auf einem Mail-Server für den Empfänger bereitliegen, auf der Basis von § 100a StPO nur in Betracht, wenn die Speicherung auf dem Mail-Server als Telekommunikation aufzufassen ist. Der Standpunkt der Autoren, die eine Anwendung des § 100a StPO ablehnen, läßt sich diesbezüglich in zwei Thesen zusammenfassen:

(1) Beim Zwischenspeichern der Nachrichten handelt es sich nicht um Telekommunikation i.S.d. § 3 Nr. 16 TKG.<sup>147</sup>

(2) Der Begriff der Telekommunikation nach § 3 Nr. 16 TKG ist für § 100a StPO maßgeblich.<sup>148</sup>

Beide Thesen erweisen sich bei genauerer Betrachtung aber als zweifelhaft.

---

<sup>144</sup> *Palm/Roy*, Mailboxen, S. 1793 und Anmerkung, S. 1905, *Bär*, Anmerkung, S. 176, *Sieber*, in: *Hoeren/Sieber* (Hg.), Rn. 702 f.

<sup>145</sup> *Kudlich*, Strafprozessuale Probleme, S. 232 und Mailbox, S. 213 f., *Ger mann*, S. 555, *Kleine-Voßbeck*, S. 142 f.

<sup>146</sup> *Kleine-Voßbeck*, S. 142 f., argumentiert allerdings wie der BGH sehr stark auf der Basis von Praktikabilitätsabwägungen.

<sup>147</sup> So ausdrücklich etwa *Bär*, Anmerkung, S. 176.

<sup>148</sup> In diesem Sinne etwa *Bär*, Online-Kommunikation, S. 632 f., *Klein-knecht/Meyer-Goßner*, § 100a Rn. 2.

### **aa) Zwischenspeichern keine Telekommunikation?**

Auch wenn sich die Autoren vordergründig mit der Auslegung von § 100a StPO beschäftigen, geht es wegen der gleichzeitig befürworteten strikten Anlehnung an das TKG in Wirklichkeit um die Auslegung von § 3 Nr. 16 TKG. Es erscheint daher notwendig, den Inhalt dieses Begriffs "Telekommunikation" im Telekommunikationsrecht zu untersuchen.

Nach § 3 Nr. 16 TKG ist unter Telekommunikation der technische Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten mittels Telekommunikationsanlagen zu verstehen; Telekommunikationsanlagen sind Systeme, die als Nachrichten identifizierbare Signale senden, übertragen, vermitteln, empfangen oder steuern können (§ 3 Nr. 17 TKG). Auf der Definition der Telekommunikation bauen weitere wichtige Begriffsbestimmungen wie die der Telekommunikationsdienstleistungen (§ 3 Nr. 18 TKG) oder des geschäftsmäßigen Erbringens von Telekommunikationsdiensten (§ 3 Nr. 5 TKG) auf. Insbesondere der Begriff der Telekommunikationsanlage könnte darauf hindeuten, in einer Zwischenspeicherung keine Telekommunikation zu sehen, weil in § 3 Nr. 17 TKG eine *Speicherung* von Signalen nicht erwähnt ist.

Tatsächlich versteht aber der Gesetzgeber selbst den Begriff nicht in diesem engen Sinn. Aus § 89 Abs. 4 TKG, der die Speicherung von Nachrichteninhalten betrifft, wird deutlich, daß dieser Vorgang gerade auch Gegenstand eines *Telekommunikationsdienstes* sein kann. Dementsprechend enthält auch die Telekommunikations-Datenschutzverordnung (TDSV), die auf der Grundlage des § 89 Abs. 1 TKG erlassen wurde und Vorschriften zum Schutz der persönlichen Daten der an der *Telekommunikation* Beteiligten enthalten soll, in ihrem § 16 eine Regelung zu "Nachrichtenübermittlungssystemen mit Zwischenspeicherung". Hiervon sind nicht

nur Daten wie Telefaxe oder Sprache, sondern auch die Zwischenspeicherung von E-Mails auf Mail-Servern im Rahmen eines entsprechenden Internet-Dienstes unproblematisch erfaßt. Wer aus dem Begriff der Telekommunikation die Zwischenspeicherung ausnehmen will, müßte annehmen, daß die Bestimmung des § 16 TDSV mangels Rechtsgrundlage nichtig ist. Diese Konsequenz ziehen aber auch die Kritiker der Rechtsprechung nicht. So stellt etwa *Bär* im Gegenteil – aus seiner Sicht widersprüchlich – ausdrücklich fest, daß es sich beim E-Mail-Transport mit Zwischenspeicherung auf einem Mail-Server um ein Nachrichtenübermittlungssystem mit Zwischenspeicherung i.S.d. § 14 Abs. 2 TDSV a.F.<sup>149</sup> handelt.<sup>150</sup> Zwar ist es aufgrund des Rangverhältnisses der Normen nicht zulässig, den Inhalt der TDSV zur Auslegung von Begriffen des TKG heranzuziehen. Jedoch findet sich der entscheidende Bezugspunkt für § 16 TDSV bereits, wie beschrieben, in § 89 Abs. 4 TKG.

Eine Ausklammerung zwischengespeicherter E-Mails aus dem Begriff der Telekommunikation hätte auch gravierende Auswirkungen auf deren Vertraulichkeit. Da Internet-Dienstleistungen üblicherweise von privaten Unternehmen erbracht werden, sind diese nicht durch Art. 10 Abs. 1 GG daran gehindert, vom Inhalt von E-Mails Kenntnis zu nehmen. Aus diesem Grund sieht § 85 TKG auf der Ebene des einfachen Gesetzes eine in der Sache ähnliche Verpflichtung der Anbieter von Telekommunikationsdiensten vor. Insbesondere ist es ihnen nach § 85 Abs. 3 TKG untersagt, sich von Inhalten und Umständen über das zum Betrieb erforderliche Maß hinaus Kenntnis zu verschaffen, vorausgesetzt es handelt sich um *Telekommunikation*. Nur in diesem Fall ist die unbefugte Kenntnisnahme auch durch § 206 StGB strafbewehrt,

---

<sup>149</sup> Dieser hatte den gleichen Regelungsgegenstand wie der heutige § 16 TDSV.

<sup>150</sup> *Bär*, Anmerkung, S. 176.

während ein strafrechtlicher Schutz nicht in Betracht kommt, falls das Zwischenspeichern nicht der Telekommunikation zugeordnet wird.<sup>151</sup>

Insgesamt ist daher davon auszugehen, daß der Begriff Telekommunikation auch die Zwischenspeicherung von Nachrichten aller Art, und damit auch von E-Mails, umfaßt.

Geht man von einer engen Anlehnung von § 100a StPO an die Definition der Telekommunikation im TKG aus, so ist damit gleichzeitig klar, daß auch zwischengespeicherte E-Mails in den Anwendungsbereich von § 100a StPO fallen. Insofern ist der Rechtsprechung im Ergebnis zuzustimmen. Wenn dagegen angeführt wird, eine Telekommunikation setze Bewegung voraus, die während der längerfristig angelegten Speicherung von E-Mails auf einem Mail-Server nicht gegeben sei,<sup>152</sup> wird der oben herausgearbeitete umfassendere Inhalt, den der Begriff der Telekommunikation nach dem TKG hat, nicht hinreichend berücksichtigt.

### **bb) Definition des TKG maßgeblich?**

Unabhängig von dem konkreten Inhalt des Begriffs der Telekommunikation nach dem TKG stellt sich aber die Frage, ob dieser im Rahmen des § 100a StPO überhaupt maßgeblich sein kann, oder ob für das Strafprozeßrecht eine eigene Definition vorgenommen werden muß.

---

<sup>151</sup> Insbesondere kommt eine Bestrafung nach § 201 oder § 202 StGB nicht in Frage. § 201 StGB bezieht sich ausdrücklich nur auf das gesprochene Wort. § 202 StGB spricht von Briefen oder anderen Schriftstücken und macht dadurch deutlich, daß er nur Briefe im traditionellen Sinn erfaßt. Eine Anwendung auf E-Mails wäre daher bereits eine gemäß Art. 103 Abs. 2 GG, § 1 StGB unzulässige Analogie.

<sup>152</sup> *Palm/Roy*, Mailboxen, S. 1793. Die Autoren beziehen sich hier noch auf den damals in § 100a StPO verwendeten Begriff des "Fernmeldeverkehrs", der durch das Begleitgesetz zum TKG 1997 durch das Wort "Telekommunikation" ersetzt wurde. Dies war aber lediglich eine redaktionelle Anpassung ohne inhaltliche Änderung, vgl. *Bär*, Online-Kommunikation, S. 632 f.

Für einen Gleichlauf von TKG und StPO sprechen vor allem die Gesetzgebungsmaterialien. Diese führen bezüglich der Ersetzung des Begriffs "Fernmeldeverkehr" in § 100a StPO durch "Telekommunikation" aus, es handele sich um eine redaktionelle Anpassung an den Sprachgebrauch des TKG.<sup>153</sup>

Dagegen sind jedoch die unterschiedlichen Zielsetzungen beider Gesetze anzuführen. Die StPO dient der Sicherung einer effektiven Strafverfolgung bei gleichzeitig möglichst großer Schonung der Personen, die in den Blick der Strafverfolgungsbehörden geraten sind; auf dieser Basis läßt § 100a StPO einen intensiven Grundrechtseingriff zu, wobei ein Ausgleich zwischen den Interessen des Betroffenen und dem öffentlichen Interesse an der Strafverfolgung durch die verschiedenen Einschränkungen in § 100a Abs. 1 StPO hergestellt wird.<sup>154</sup> Dagegen ist es Zweck des TKG, den gesamtwirtschaftlichen Rahmen der Erbringung von Telekommunikationsdiensten vorzugeben und die flächendeckende Versorgung der Bevölkerung zu sichern (§ 1 TKG). Aus diesem Grund beschäftigt sich das TKG im Prinzip auch nur mit den Möglichkeiten zur Übermittlung von Nachrichten, nicht dagegen mit den Inhalten der Telekommunikation.<sup>155</sup>

Deutlich wird damit, daß beide Regelungskomplexe höchst unterschiedliche Ziele verfolgen.<sup>156</sup> Daraus folgt, daß auf die Definition des TKG, die eher technisch orientiert ist, nicht ohne weiteres

---

<sup>153</sup> BT-Drucks. 13/8016, S. 26.

<sup>154</sup> Auf diese Voraussetzungen, insbesondere den Straftatenkatalog und die Subsidiaritätsklausel, wird hier nicht eingegangen, da diese Fragen nicht speziell den Zugriff auf E-Mails betreffen. Siehe dazu z.B. *Bär*, Computerdaten, S. 328 ff.

<sup>155</sup> BT-Drucks. 13/3609, S. 37; siehe aber zum Schutz der Nachrichteninhalte oben aa.

<sup>156</sup> Vgl. zur ähnlichen Problemlage unter der Geltung des alten Fernmeldeanlagengesetzes *Bär*, Computerdaten, S. 308.

zurückgegriffen werden kann. Vielmehr ist eine eigenständige Begriffsbestimmung erforderlich, die sich an den genannten Zielen der StPO ausrichtet.

Geht man vom allgemeinen Sprachgebrauch aus, so ergibt sich als Anforderung, daß eine Nachricht, um Telekommunikation zu sein, mit Hilfe technischer Geräte über eine Entfernung übermittelt werden muß. Eine Zwischenspeicherung, auch über längere Zeit, schadet dabei nicht. Auch der E-Mail-Dienst, für den die Zwischenspeicherung von Mitteilungen auf Mail-Servern typisch ist, wird wohl allgemein als Mittel der Telekommunikation bezeichnet, weil für die sprachliche Bezeichnung das Ergebnis dominiert, daß letztendlich eine Nachricht übermittelt wird. Das technische Merkmal der Zwischenspeicherung spielt für die Begriffsbildung dagegen keine Rolle..

Da es ein Ziel der StPO ist, Mittel zu einer möglichst effektiven Ermittlung des Sachverhalts bereitzustellen, ist unter diesem Aspekt der Begriff der Telekommunikation im Rahmen des Wortsinns möglichst weit auszudehnen. Nachdem die Einbeziehung von auf einem Server lagernden E-Mails dem allgemeinen Sprachgebrauch entspricht, ist eine solche Interpretation auch unter dem teleologischen Gesichtspunkt anzustreben.

Schließlich kann auch ein systematisches Argument herangezogen werden. Grundsätzlich sollten – in den Grenzen des Wortlauts der jeweiligen Vorschriften – Nachrichten möglichst gleich behandelt werden, unabhängig von der Art des gewählten Kommunikationsmittels. Unter dieser Prämisse bietet sich ein Vergleich mit der Postbeschlagnahme nach § 99 StPO an. Dieser erlaubt für ge-

wöhnliche Postsendungen und Telegramme<sup>157</sup> die Beschlagnahme, solange sie sich im Gewahrsam des Post- oder Telekommunikationsanbieters befinden. Eingeschlossen sind damit auch Zeiten, in denen z.B. ein Brief nicht wirklich befördert, sondern z.B. in einem Postfach gelagert oder nach dem Sortieren zum Austragen durch den Briefträger bereitgelegt wird.<sup>158</sup> Dieser Situation kommt das Zwischenspeichern einer E-Mail auf einem Mail-Server bei funktionaler Betrachtung sehr nahe. Auch in systematischer Hinsicht ist es daher wünschenswert, die Zwischenspeicherung von Nachrichten als Telekommunikation zu behandeln.

Insgesamt ist mithin eine Auslegung des Begriffs "Telekommunikation" zu befürworten, die zwischengespeicherte E-Mails einbezieht; die Rechte des Betroffenen werden dabei weiterhin durch die übrigen Voraussetzungen des § 100a StPO gewahrt. Gleichzeitig führt diese Interpretation weg von rein technischen Merkmalen und hin zu einer materiellen Sichtweise, bei der die übertragene Nachricht als Information im Vordergrund steht. Demzufolge liegt eine Telekommunikation solange vor, bis eine Nachricht den Empfänger erreicht hat, d.h. bis sie sich in seinem Gewahrsam befindet. Bezogen auf die Gegebenheiten des E-Mail-Verkehrs bedeutet dies, daß der Empfänger die E-Mails von dem für ihn zuständigen Mail-Server auf seinen PC heruntergeladen haben muß.

Auch auf der Basis einer eigenständigen Bestimmung des Begriffs der Telekommunikation, unabhängig vom TKG, erscheinen die Erwägungen der Rechtsprechung daher jedenfalls im Ergebnis überzeugend. Geht man vom Vorliegen einer Telekommunikation aus, so ist es nur konsequent, den Mail-Server, der mit einer Ver-

---

<sup>157</sup> Dagegen nicht auch für E-Mails, siehe oben E.IV.

<sup>158</sup> Vgl. *Kleinknecht/Meyer-Goßner*, § 99 Rn. 9.

bindung zum Internet ausgestattet ist, als Telekommunikationsanlage aufzufassen.<sup>159</sup> Richtig ist nach dem oben Gesagten auch, daß der komplexe Übermittlungsvorgang von E-Mails nicht in verschiedene Phasen aufgespalten werden kann.<sup>160</sup>

### **cc) Ergebnis**

Als Ergebnis der Untersuchung des Begriffs der Telekommunikation in § 100a StPO kann festgehalten werden, daß dieser auch E-Mails umfaßt, die auf einem Mail-Server gespeichert sind und für den Empfänger zum Herunterladen auf dessen eigenen PC bereitgehalten werden. Dies ergibt sich aus zwei Begründungsansätzen. Geht man davon aus, daß § 100a StPO auf das Telekommunikationsrecht verweist, so folgt die Einbeziehung zwischengespeicherter E-Mails aus der entsprechenden Verwendung des Begriffs "Telekommunikation" im TKG. Aber auch eine vom TKG losgelöste eigenständige Interpretation führt aus teleologischen und systematischen Gründen zum gleichen Ergebnis.

### **c) Begriff der Überwachung**

Das Abrufen von E-Mails, die auf einem Mail-Server gespeichert sind, müßte sich als Überwachung einordnen lassen. Dagegen könnte man einwenden, eine Überwachung setze eine Beteiligung des Staates als Dritter voraus, der einen zwischen anderen Personen stattfindenden Kommunikationsvorgang kontrolliert; bei einem Abruf von E-Mails bauten die Strafverfolgungsbehörden dagegen selbst erst eine Verbindung zum Mail-Server auf.<sup>161</sup> Diese Argumentation ist aber nur bei einem engen Verständnis des Begriffs "Telekommunikation" tragfähig, das gespeicherte E-Mails

---

<sup>159</sup> BGH CR 1996, 488 (489).

<sup>160</sup> LG Hanau MMR 2000, 175 (176).

<sup>161</sup> Bär, Online-Kommunikation, S. 623. Diese Aussage bezieht sich zwar auf das Eindringen in einen Rechner ohne Wissen des Betreibers, läßt sich aber auch auf den Abruf unter Mitwirkung des Betreibers übertragen.

ausklammert. Nach der hier vertretenen Auffassung ist dagegen ein Telekommunikationsvorgang durch das Zwischenspeichern nicht beendet oder unterbrochen. Nehmen die Strafverfolgungsbehörden von zwischengespeicherten E-Mails Kenntnis, so befindet sich der Staat demnach tatsächlich in der Rolle des außenstehenden, in den Kommunikationsvorgang eingreifenden Dritten.

Daß die staatlichen Behörden zur technischen Realisierung der Kontrollmaßnahme u.U. selbst eine Verbindung aufbauen, steht der Annahme einer Überwachung nicht entgegen. Hierbei handelt es sich um ein Detail, das durch die technischen Gegebenheiten bedingt ist. Wird aber bereits beim Begriff der Telekommunikation der rein technische Bezug zugunsten einer mehr materiell orientierten Betrachtung aufgegeben, so muß dies konsequenterweise auch für den Begriff der Überwachung gelten. Überwachung bedeutet damit im vorliegenden Zusammenhang das Verschaffen von Kenntnissen, unabhängig von den technischen Einzelheiten dieses Vorgangs.<sup>162</sup>

Das Abrufen von E-Mails von einem Mail-Server ist daher auch der Überwachung i.S.d. § 100a StPO zuzuordnen.

#### **d) Ergebnis**

Wie die vorangegangenen Überlegungen ergeben, sind Bedenken gegen eine Anwendung von § 100a StPO auf den Abruf von zwischengespeicherten E-Mails im Ergebnis nicht gerechtfertigt. Vielmehr ist die Maßnahme aufgrund dieser Vorschrift als zulässig zu betrachten.

---

<sup>162</sup> Vgl. auch die Definition bei Kudlich, Strafprozessuale Probleme, S. 233.

## 2. Zugriff nach § 94 StPO

Angesichts der hohen Hürden, die § 100a StPO, insbesondere durch das Erfordernis einer Katalogtat, für einen Abruf von Nachrichten aufstellt, ist den Strafverfolgungsbehörden sicherlich daran gelegen, einen einfacheren Weg zum Abruf von Nachrichten von einem Mail-Server zu finden.<sup>163</sup> Bedenkt man, daß die E-Mails während der Phase der Zwischenspeicherung auf dem Mail-Server auf einem Datenträger verkörpert sind, so kommt insbesondere eine Beschlagnahme dieses Datenträgers nach § 94 StPO in Betracht. Dem Wortlaut nach ist ein solcher Zugriff, wie dargestellt wurde, tatsächlich möglich.<sup>164</sup>

Eine bedenkenlose Anwendung von § 94 StPO würde allerdings dazu führen, daß die Schutzvorschriften des § 100a StPO unterlaufen werden könnten. Denn § 94 StPO sieht – abgesehen von der potentiellen Bedeutung als Beweismittel – keinerlei Einschränkungen vor, insbesondere keinen dem § 100a StPO vergleichbaren Straftatenkatalog und keine Subsidiaritätsklausel. Gleichwohl wird eine Anwendung von § 94 StPO von Teilen der Rechtsprechung und Literatur befürwortet.<sup>165</sup> Diese Auffassung ist aber im Ergebnis aus einer Reihe von Gründen nicht haltbar.

### a) Verstoß gegen Art. 10 GG

Zu beachten ist, daß die Rechtfertigung eines Eingriffs in Art. 10 Abs. 1 GG in Rede steht.<sup>166</sup> Ein solcher Eingriff ist zwar, wie festgestellt, nach Art. 10 Abs. 2 Satz 1 GG aufgrund eines Gesetzes

---

<sup>163</sup>Vgl. *Meseke*, in: *Kriminalistik* 2000, 245 (246), der beklagt, daß verschiedene wichtige Delikte in § 100a StPO nicht genannt seien.

<sup>164</sup>Oben E.III.

<sup>165</sup>Etwa *Palm/Roy*, *Mailboxen*, S. 1795, *Bär*, *Computerdaten*, S. 297; BGH CR 1996, 488 (489) hält eine Beschlagnahme nach § 94 StPO aus ermittlungstaktischen Gründen nicht für angemessen, woraus zu schließen ist, daß sie aber rechtlich zulässig sein soll.

<sup>166</sup>Oben C.I.5.b.aa.

möglich.<sup>167</sup> § 94 StPO erfüllt aber nicht die Anforderungen, die an ein Gesetz gestellt werden müssen, das einen Gesetzesvorbehalt ausfüllen soll. Zwar liegt kein Verstoß gegen das Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG vor, denn bei § 94 StPO handelt es sich um eine vorkonstitutionelle Norm, auf die das Zitiergebot keine Anwendung findet.<sup>168</sup> § 94 StPO trifft aber keine Bestimmungen zu den wesentlichen Aspekten eines Grundrechtseingriffs, insbesondere zu Art, Umfang und Voraussetzungen.

Anders als z.B. die Postbeschlagnahme nach § 99 StPO oder auch § 100a StPO enthält er keine Aussagen zu einem Eingriff gerade in Art. 10 Abs. 1 GG, sondern bezieht sich nur allgemein auf "Gegenstände". § 94 StPO ähnelt damit den Generalklauseln in den Polizeigesetzen der Länder, auf deren Grundlage intensive Grundrechtseingriffe ebenfalls unzulässig sind.<sup>169</sup> Die Regelung muß daher wegen ihrer Unbestimmtheit verfassungskonform in der Weise ausgelegt werden, daß sie nicht zu Beschlagnahmen ermächtigt, die zu einem intensiven Grundrechtseingriff führen. Eine solche intensive Beeinträchtigung wäre aber angesichts des hohen Rangs des Brief-, Post- und Fernmeldegeheimnisses bei einem Eingriff in Art. 10 Abs. 1 GG gegeben.

Eine Anwendung von § 94 StPO ist damit in der vorliegenden Konstellation ausgeschlossen.

## **b) Verhältnis zu § 99 StPO**

Auch die Systematik der Eingriffsbefugnisse innerhalb der StPO spricht gegen eine Beschlagnahmebefugnis für Datenträger von

---

<sup>167</sup> Oben E.I.

<sup>168</sup> *Pieroth/Schlink*, Rn. 311.

<sup>169</sup> Vgl. *Rachor*, in: *Lisken/Denninger* (Hg.), Rn. 456 sowie Rn. 461 zur Speicherung von Daten.

Mail-Servern, auf denen sich E-Mails befinden. Dies zeigt ein Vergleich mit der Situation bei der Beschlagnahme traditioneller Postsendungen. In diesem Fall ist eine Beschlagnahme nach § 94 StPO ab dem Zeitpunkt ausgeschlossen, in dem ein Postunternehmen Gewahrsam an der Postsendung erlangt hat, weil danach nur noch die gegenüber § 94 StPO strengeren Voraussetzungen des § 99 StPO<sup>170</sup> gelten sollen. Diese Sonderregelung wurde gerade wegen des mit einer Beschlagnahme verbundenen Eingriffs in das Post-, Brief- und Fernmeldegeheimnis – heute kodifiziert in Art. 10 Abs. 1 GG – geschaffen.<sup>171</sup>

Auf – auch zwischengespeicherte – E-Mails ist § 99 StPO zwar nicht anwendbar.<sup>172</sup> Dies hat seinen Grund aber nur in der fehlenden Körperlichkeit des zu übermittelnden Gegenstandes, während die Schutzbedürftigkeit bei einem traditionellen Brief und bei E-Mails gleich groß ist. Obwohl dementsprechend § 99 StPO nicht unmittelbar zu einer Sperre für § 94 StPO führen kann, muß die Absicht des Gesetzgebers, wegen Art. 10 Abs. 1 GG für Eingriffe in den Übermittlungsvorgang von Nachrichten eine abschließende Sonderregelung zu schaffen, gleichwohl berücksichtigt werden. Auch hier kann wieder auf die Dogmatik des Polizeirechts verwiesen werden, nach der ein Rückgriff auf die Generalklausel nicht in Betracht kommt, wenn ein Komplex abschließend geregelt wurde.<sup>173</sup> Im Strafprozeßrecht ist der Zugriff der Strafverfolgungsbehörden auf Nachrichten in der Übermittlungsphase durch § 99 StPO abschließend geregelt. Daß hiervon E-Mails nicht erfaßt sind, führt deswegen nicht dazu, daß auf diese nach dem generalklauselartigen § 94 StPO zugegriffen werden könnte.

---

<sup>170</sup> Zu den Unterschieden von § 94 und 99 StPO *Bär*, Computerdaten, S. 293 f.

<sup>171</sup> *Klenknecht/Meyer-Goßner*, § 99 Rn. 1.

<sup>172</sup> Oben E.IV.

<sup>173</sup> *Rachor*, in: *Lisken/Denninger* (Hg.), Rn. 456.

Auch aus diesem Grund ist ein Rückgriff auf § 94 StPO daher unzulässig. Es wäre auch widersprüchlich, zwar eine erweiternde Auslegung von § 99 StPO zu Lasten der Betroffenen für ausgeschlossen zu betrachten, daraus aber zu folgern, daß dann die allgemeine Vorschrift des § 94 StPO herangezogen werden könne.<sup>174</sup> Dadurch würde der Grundrechtsschutz angesichts der Weite der Formulierung des § 94 StPO gerade verkürzt.<sup>175</sup>

### **c) Verstoß gegen § 85 TKG**

Schließlich würde eine Beschlagnahme nach § 94 StPO auch gegen das Fernmeldegeheimnis nach § 85 TKG verstoßen, dem die zwischengespeicherten E-Mails als Telekommunikation unterliegen. Nach § 85 Abs. 3 Satz 1 TKG ist es den Anbietern von Telekommunikationsdiensten – zu denen auch die Betreiber von Mail-Servern zählen – untersagt, sich oder anderen Kenntnis vom Inhalt von Telekommunikation, also auch von E-Mails, zu verschaffen. Das Verhältnis zu gesetzlichen Regelungen, die in das Fernmeldegeheimnis eingreifen könnten, stellen § 85 Abs. 3 Sätze 3 und 4 TKG klar. Eine Weitergabe von Informationen ist danach nur zulässig, soweit sich ein Gesetz ausdrücklich auf Telekommunikationsvorgänge bezieht; als Ausnahme von diesem Grundsatz verpflichtet auch § 138 StGB, der sich nicht auf Telekommunikation bezieht, zur Weitergabe. Im Bereich der StPO beziehen sich nur die §§ 100a, 100b StPO ausdrücklich auf Telekommunikationsvorgänge, nicht dagegen § 94 StPO. Eine Beschlagnahme nach § 94 StPO würde daher gegen § 85 TKG verstoßen.<sup>176</sup>

Einem Konflikt mit § 85 TKG könnte man demnach nur entgehen,

---

<sup>174</sup> So aber *Bär*, Computerdaten, S. 296, 297.

<sup>175</sup> So auch *Germann*, S. 555, 535 f. (insbesondere Fn. 1249), der zu Recht feststellt, daß unter dem Aspekt des Grundrechtsschutzes dann sogar eine analoge Anwendung von § 99 StPO vorzuziehen wäre.

<sup>176</sup> So auch *Germann*, S. 536.

wenn durch die Beschlagnahme keine "Weitergabe" i.S.d. § 85 Abs. 3 Satz 3 TKG erfolgen würde. Hierfür spricht immerhin, daß § 94 StPO den Strafverfolgungsbehörden auch den aktiven Zugriff auf Datenträger erlaubt und sie – anders als bei § 100a StPO – nicht ausschließlich auf eine Mitwirkung des Betroffenen (nach § 95 Abs. 1 StPO) angewiesen sind. Entscheidend ist aber die in § 85 Abs. 3 TKG klar zum Ausdruck kommende Absicht des Gesetzgebers, die Einschränkung des Fernmeldegeheimnisses nach § 85 Abs. 1 TKG auf ein Minimum zu beschränken und ihm den Vorrang einzuräumen, solange sich nicht aus gesetzlichen Vorschriften eindeutig das Gegenteil ergibt.<sup>177</sup> Die Vorgabe in § 85 Abs. 3 Satz 3 TKG, daß sich eine einschränkende Vorschrift "ausdrücklich" auf Telekommunikationsvorgänge beziehen muß, hat daher eine ähnliche Klarstellungsfunktion wie das Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG im Zusammenhang mit Einschränkungen von Art. 10 Abs. 1 GG.<sup>178</sup> Mithin ergibt sich eine zu Art. 10 Abs. 1 GG parallele Wertung.

#### **d) Ergebnis**

Aus diesen Überlegungen folgt, daß eine Beschlagnahme (§ 94 StPO) von Datenträgern in Mail-Servern, die E-Mails enthalten, unzulässig ist. Zwischengespeicherte E-Mails können damit von den Strafverfolgungsbehörden nur aufgrund und unter den Vor-

---

<sup>177</sup> Dementsprechend wird auch in dem am 24. Oktober 2001 von der Bundesregierung beschlossenen Entwurf der auf § 88 Abs. 2 TKG basierenden Telekommunikationsüberwachungsverordnung (TKÜV) die Beschlagnahme nicht erwähnt. Vielmehr werden in § 1 Nr. 1 TKÜV-E aus dem Strafprozeßrecht lediglich die §§ 100a, 100b StPO genannt, obwohl sicherlich auch bei Datenträgern im Interesse der Strafverfolgung ein Bedürfnis nach technischen Regelungen besteht. Der Text der Entwurfsfassung ist erhältlich unter [http://www.bmwi.de/textonly/Homepage/download/telekommunikation\\_post/TKUEV.pdf](http://www.bmwi.de/textonly/Homepage/download/telekommunikation_post/TKUEV.pdf). Zur Verabschiedung der TKÜV siehe die Pressemitteilung des Bundeswirtschaftsministeriums vom 24. Oktober 2001 unter <http://www.bmwi.de/Homepage/Presseforum/Pressemitteilungen/2001/1A24prm1.jsp>.

<sup>178</sup> Zum Zitiergebot oben D.V.

aussetzungen von § 100a StPO abgerufen werden. Im Ergebnis ist daher dem Teil der Rechtsprechung zuzustimmen, der eine Anwendbarkeit von § 94 StPO verneint.<sup>179</sup>

#### **IV. Abrufen der E-Mails vom Mail-Server durch den Empfänger**

Baut der Empfänger eine Internet-Verbindung zu seinem Mail-Server auf und lädt die dort für ihn gespeicherten Nachrichten herunter, so ist dieser Vorgang mit der Übertragung der abzusendenden E-Mails durch den Absender vergleichbar; lediglich die "Flußrichtung" der Daten ist entgegengesetzt. Ansatzpunkte für eine unterschiedliche rechtliche Behandlung ergeben sich daraus allerdings weder in bezug auf die beeinträchtigten Grundrechte noch auf die Normen zu ihrer Rechtfertigung. Es kann daher vollständig auf die Ausführungen zur Übertragung der E-Mails durch den Absender verwiesen werden.

#### **V. Nachrichten auf dem PC des Empfängers**

Hat der Empfänger die E-Mails erfolgreich auf seinen Rechner heruntergeladen, so ist damit der Vorgang der Telekommunikation beendet, weil die Nachrichten ihr Ziel erreicht haben; nun befinden sich die Mitteilungen im Gewahrsam des Empfängers. Gleichzeitig entfällt damit auch der Schutz des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 Abs. 1 GG), weil die Übermittlung nicht mehr andauert.<sup>180</sup> Die rechtliche Situation entspricht somit derjenigen von E-Mails, die sich auf dem PC des Absenders befinden und dort auf die Übertragung zu dessen Mail-Server warten. Auf diese Erörterungen wird daher ebenfalls verwiesen.

---

<sup>179</sup> LG Hanau MMR 2000, 175 (175 f.).

<sup>180</sup> Oben C.I.3.e.

## **VI. Zusammenfassung**

Wie die Untersuchung der möglichen Ermächtigungsgrundlagen gezeigt hat, ist der Zugriff auf E-Mails auf ihrem Weg vom Absender zum Empfänger unterschiedlich stark beschränkt. Solange sich Nachrichten noch auf dem PC des Absenders befinden und sobald der Empfänger sie von seinem Mail-Server heruntergeladen hat, können die Strafverfolgungsbehörden nach § 94 StPO die Datenträger beschlagnahmen, auf denen die E-Mails gespeichert sind. Dabei ist in der Regel die Beschlagnahme der gesamten Zentraleinheit mangels Erforderlichkeit unverhältnismäßig; wenn möglich, muß die Beschlagnahme durch Kopieren der relevanten Datenbestände erfolgen.

Während der Übertragung durch das Internet greift dagegen der volle Schutz durch § 100a StPO ein, der eine Überwachung nur unter strengen Voraussetzungen, insbesondere dem Verdacht wegen einer Katalogtat, gestattet. Das gleiche gilt für Nachrichten, die auf dem Mail-Server des Empfängers zwischengespeichert und für ihn bereitgehalten werden. Wie sowohl eine genauere Betrachtung des TKG als auch ein eigenständiger Definitionsansatz zeigen, ist auch die Zwischenspeicherung als Telekommunikation i.S.d. § 100a StPO anzusehen. Gleichzeitig ist eine Beschlagnahme der entsprechenden Datenträger beim Betreiber des Mail-Servers unzulässig, weil § 94 StPO aus verfassungsrechtlichen, systematischen und teleologischen Gründen keine Beschlagnahme von Gegenständen erlaubt, auf denen sich Daten befinden, die dem Schutz von Art. 10 Abs. 1 GG und § 85 TKG unterliegen.

## **G. Die Identifizierung der Kommunikationsteilnehmer**

Neben den Inhalten der E-Mail-Kommunikation kann es für die Strafverfolgungsbehörden auch interessant sein, die Teilnehmer der Kommunikation zu ermitteln. Eine Identifizierung von Absender und Empfänger ist mit Hilfe der Daten möglich, die automatisch im Verlauf der E-Mail-Kommunikation entstehen und gespeichert werden, wobei allerdings u.U. eine Vielzahl verschiedener Daten kombiniert werden müssen.<sup>181</sup> Daher soll auch dieser Aspekt der Überwachung des E-Mail-Verkehrs behandelt werden. Zunächst werden die verschiedenen Arten der Daten und die durch ihre Ermittlung seitens der Strafverfolgungsbehörden jeweils beeinträchtigten Grundrechte zusammengestellt. Anschließend folgt die Erörterung möglicher Eingriffsbefugnisse.

### **I. Kommunikationsdaten und ihre Grundrechtsrelevanz**

#### **1. Arten von Kommunikationsdaten**

Daten, die im Zusammenhang mit der Kommunikation per E-Mail stehen, lassen sich in zwei Gruppen einteilen:

- *Verbindungsdaten* entstehen aufgrund eines konkreten Kommunikationsvorgangs. Sie sind die näheren Umstände der Kommunikation, die von Art. 10 Abs. 1 GG geschützt werden.<sup>182</sup>
- *Bestandsdaten* sind dagegen diejenigen persönlichen Daten, die allgemein zur Durchführung eines Vertragsverhältnisses über Telekommunikationsdienstleistungen erforderlich sind.<sup>183</sup> Sie entstehen nicht anlässlich einer konkreten Telekommunikation

---

<sup>181</sup> Vgl. oben B.III.

<sup>182</sup> Vgl. oben C.I.1; zum Begriff außerdem *Gundermann*, in: DuD 1999, 681 (681) Fn. 5.

<sup>183</sup> A.a.O., Fn. 6.

und sind daher nicht durch Art. 10 Abs. 1 GG, sondern durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt.<sup>184</sup>

Klar ist, daß die persönlichen Angaben wie Name und Anschrift zu den Bestandsdaten zu zählen sind. Streitig ist dies dagegen hinsichtlich der Einordnung der IP-Adressen. Teilweise werden diese als Bestandsdaten betrachtet.<sup>185</sup> Tatsächlich muß hier aber differenziert werden. Beschreiben IP-Adressen die beteiligten Mail-Server und damit den Übertragungsweg einer E-Mail, sind diese Aufzeichnungen Verbindungsdaten, weil sie anlässlich eines konkreten Kommunikationsvorgangs entstanden sind. Ebenso fallen Aufzeichnungen zu den praktisch wichtigen dynamischen IP-Adressen erst mit der Herstellung einer Verbindung zum Internet an und sind daher ebenfalls eindeutig Verbindungsdaten.<sup>186</sup>

Eine Einordnung als Bestandsdatum kommt damit nur bei statischen IP-Adressen in Frage, weil deren Zuteilung ausdrücklicher Inhalt des Vertrags mit dem Zugangsvermittler ist. Gleiches gilt für E-Mail-Adressen und Login-Namen; ihre Zuweisung ist ebenfalls eindeutiger Bestandteil des Vertrags mit dem jeweiligen Diensteanbieter. Diese Daten sind daher Bestandsdaten. Zu beachten ist aber, daß diese Daten immer auch einen konkreten Kommunikationsvorgang bezeichnen, indem z.B. der Zeitpunkt der Übermittlung des Login-Namens bei der Einwahl in den Terminal-Server festgehalten wird; ebenso wird die E-Mail-Adresse in konkreten E-Mails verwendet. Statische IP-Adresse, E-Mail-Adresse und Login-Name sind daher andererseits auch den Verbindungsdaten zuzurechnen. Die rechtliche Behandlung muß davon abhän-

---

<sup>184</sup> Oben C.I.1 und II.1.

<sup>185</sup> Argumentation der Sicherheitsbehörden bei *Gundermann*, in: *DuD* 1999, 681 (686); ebenso wohl auch *Meseke*, in: *Kriminalistik* 2000, 245 (249).

<sup>186</sup> So auch *Gundermann*, in: *DuD* 1999, 681 (686).

gen, zu welchem Zweck die Daten verwendet werden sollen. Geht es nur um die Ermittlung der persönlichen Daten wie Name und Anschrift, so sind die Regelungen für Bestandsdaten einschlägig. Sollen dagegen mit Hilfe z.B. der E-Mail-Adresse oder des Login-Namens konkrete Kommunikationsvorgänge nachvollzogen werden, dann kann dies nur nach den Vorschriften über Verbindungsdaten geschehen.

## **2. Quellen für Verbindungs- und Bestandsdaten**

Verbindungsdaten werden in einer Vielzahl verschiedener Dateien bei verschiedenen Personen aufgezeichnet. Im einzelnen sind dies:

- E-Mails auf dem PC des Empfängers:

E-Mail-Adresse von Absender und Empfänger, Datum und Zeit der Absendung, IP-Adressen der beteiligten Mail-Server<sup>187</sup>

- E-Mails auf dem Mail-Server des Empfängers:

die selben Daten

- Logdateien der beteiligten Mail-Server:

IP-Adresse des einsendenden bzw. abrufenden PC's, Datum und Zeit des Vorgangs<sup>188</sup>

- Logdatei beim Zugangsvermittler:

Datum, Zeit und Dauer des Anrufs, dem Benutzer über seinen Login-Namen zugewiesene IP-Adresse, evtl. Telefonnummer des Anrufers (bei Internet-by-call-Diensten<sup>189</sup>)<sup>190</sup>

- Logdatei des Betreibers des Telefonnetzes:

Datum, Zeit, Dauer und Ziel (Rufnummer des Zugangsvermittlers) des Anrufs<sup>191</sup>

Bestandsdaten finden sich in den Kundendateien der jeweiligen

---

<sup>187</sup> Oben A.II.4.

<sup>188</sup> Oben A.II.6.b.

<sup>189</sup> Dazu oben B.III.2.

<sup>190</sup> Oben A.II.5 und 6.a.

<sup>191</sup> Oben A.II.5 und 6.a

Diensteanbieter. Sie enthalten die vollständigen Personalien der Internet-Nutzer, d.h. von Absender und Empfänger, ferner Daten zum Vertragsverhältnis wie den zugewiesenen Login-Namen und die zugewiesene E-Mail-Adresse.

## **II. Vorbemerkung zu den Eingriffsbefugnissen**

### **1. Relevante Normen**

Im folgenden wird untersucht, mit Hilfe welcher gesetzlichen Grundlagen die Strafverfolgungsbehörden Einsicht in die genannten Dateien nehmen können. In Betracht kommen neben den Normen der StPO Auskunftsansprüche nach dem TKG.

Nicht mehr behandelt werden hier die Bestimmungen, die bereits keine Einsicht in die Inhalte von E-Mails erlauben.<sup>192</sup> Es sind keine Anhaltspunkte dafür ersichtlich, daß nach diesen Vorschriften zwar nicht der Zugriff auf Inhalte, wohl aber auf Verbindungs- oder Bestandsdaten zulässig sein könnte. Nicht mehr behandelt wird auch der Auskunftsanspruch nach § 12 FAG; diese Regelung ist am 31. Dezember 2001 außer Kraft getreten.<sup>193</sup> Aus dem Bereich der StPO verbleiben damit die §§ 94 und 100a StPO sowie der neue § 100g StPO, der mit Wirkung seit 1. Januar 2002 die Nachfolgeregelung zu § 12 FAG darstellt. Diese Bestimmung wurde zusammen mit Verfahrensregelungen in § 100h StPO durch das Gesetz zur Änderung der Strafprozeßordnung vom 21. Dezember 2001 eingefügt.<sup>194</sup>

Das Telekommunikationsrecht sieht Auskunftspflichten der Anbieter von Telekommunikationsdiensten in § 89 Abs. 6 TKG sowie im

---

<sup>192</sup> Oben E.IV bis VII.

<sup>193</sup> Siehe § 28 Satz 2 FAG in der Fassung des Gesetzes zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20. Dezember 1999 (BGBl 1999 I, 2491 (2492)).

<sup>194</sup> BGBl 2001 I, 3879.

automatisierten Verfahren nach § 90 TKG vor. § 90 TKG betrifft allerdings nur die geschäftsmäßigen Betreiber von rufnummernbasierten Netzen, zu denen das Internet nicht gehört.<sup>195</sup> Die Regelung ist damit nicht auf Absender und Empfänger anwendbar, ferner nicht auf die Zugangsvermittler und die Betreiber der Mail-Server.<sup>196</sup> Relevant wird sie nur für den Betreiber des Telefonnetzes.

## **2. Verschaffen der Zugriffsmöglichkeit**

Es wurde bereits festgestellt, daß es den Strafverfolgungsbehörden weder nach § 100a StPO noch nach § 94 StPO erlaubt ist, sich die Zugriffsmöglichkeit auf Daten durch Hacking zu verschaffen.<sup>197</sup> Auch die hier noch hinzukommenden Bestimmungen geben ein solches Recht nicht.

§ 100g Abs. 1 StPO sieht lediglich ein Recht der Strafverfolgungsbehörden vor, Auskunft zu verlangen, und macht damit bereits im Wortlaut deutlich, daß ein Eindringen des Staates in Rechner-systeme der Verpflichteten nicht zulässig sein soll. Zudem kann auch hier auf das bereits zu § 100a StPO ausgeführte Argument verwiesen werden, daß eine Vorschrift nicht so ausgelegt werden darf, daß sie andere Grundrechte beeinträchtigt als vom Gesetzgeber ausdrücklich zugelassen.<sup>198</sup> Nach Art. 3 des Gesetzes zur Änderung der StPO soll durch § 100g StPO aber lediglich Art. 10 Abs. 1 GG eingeschränkt werden, nicht dagegen Art. 13 Abs. 1 GG, wie es für staatliches Hacking erforderlich wäre.<sup>199</sup>

Das gleiche gilt für den Auskunftsanspruch nach § 89 Abs. 6 TKG

---

<sup>195</sup> *Gundermann*, in: DuD 1999, 681 (684 f.).

<sup>196</sup> Vgl. *Wuermeling/Felixberger*, in: CR 1997, 555 (561).

<sup>197</sup> Oben D.V und VI.

<sup>198</sup> Oben D.V.

<sup>199</sup> Zum Eingriff in Art. 13 Abs. 1 GG durch staatliches Hacking oben C.IV.2.a.bb.

und das automatisierte Abrufverfahren nach § 90 TKG. Beide Vorschriften setzen schon nach ihrem Wortlaut eine Mitwirkung des jeweiligen Diensteanbieters voraus. Eine Einschränkung von Art. 13 Abs. 1 GG ist hier ebenfalls nicht vorgesehen.

Im Ergebnis ist somit staatliches Hacking auch zum Zugriff auf Verbindungs- und Bestandsdaten unzulässig. Dieser Punkt wird daher im folgenden nicht mehr gesondert untersucht.

### **3. Gesetzesvorbehalte**

Bei der Ermittlung von Verbindungsdaten ist ein Eingriff in Art. 10 Abs. 1 GG zu rechtfertigen,<sup>200</sup> bei der Ermittlung von Bestandsdaten ein solcher in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.<sup>201</sup> Beide Grundrechte unterliegen einem einfachen Gesetzesvorbehalt und sind daher grundsätzlich einschränkbar. Für die Rechtfertigung des Eingriffs gelten daher dieselben Maßstäbe wie beim Zugriff auf die Inhalte von E-Mails.<sup>202</sup>

## **III. E-Mails auf dem PC des Empfängers**

### **1. Zugriff nach § 94 StPO**

Die Nachrichten, die der Empfänger auf seinen PC heruntergeladen hat, enthalten diverse Verbindungsdaten. Für den Zugriff auf den Inhalt dieser E-Mails hat sich einzig die Beschlagnahme nach § 94 StPO als einschlägig erwiesen.<sup>203</sup> Praktisch ist damit auch die Beschlagnahme der Verbindungsdaten verbunden, weil sich diese zusammen mit dem Inhalt in der selben Datei befinden. Aber auch rechtlich bestehen keine Bedenken, mit Rücksicht auf die Verbindungsdaten die Beschlagnahme auszuschließen oder

---

<sup>200</sup> Oben C.I.5.b.aa

<sup>201</sup> Oben C.II.2.b.aa.

<sup>202</sup> Oben E.I.

<sup>203</sup> Oben F.I.2.

einzuschränken. Es gibt kein Grundrecht, das die Verbindungsdaten stärker schützt als den Inhalt. Insbesondere gilt auch Art. 10 Abs. 1 GG hier nicht mehr.<sup>204</sup>

Ein Zugriff auf Verbindungsdaten, sei es in einzelnen Dateien, sei es – wie typisch – in Verbindung mit dem Zugriff auf Inhalten von E-Mails ist daher nach § 94 StPO zulässig.

## **2. Sonstige Eingriffsbefugnisse**

Ein Zugriff nach § 100a StPO kommt dagegen, wie schon hinsichtlich der Inhalte, nicht in Betracht, weil keine Telekommunikation mehr stattfindet.<sup>205</sup> Auch Auskunftsansprüche nach § 100g StPO oder §§ 89 Abs. 6, 90 TKG scheiden aus, weil sie sich nur gegen den geschäftsmäßigen Erbringer von Telekommunikationsdiensten richten; zu diesem Kreis gehört der Empfänger als Privatperson, die Telekommunikationsdienste nutzt, nicht.

## **IV. E-Mails auf dem Mail-Server des Empfängers**

### **1. Zugriff nach § 100a StPO**

§ 100a StPO erlaubt den Strafverfolgungsbehörden den Zugriff auf die Inhalte zwischengespeicherter Nachrichten.<sup>206</sup> Mit dem Zugriff ist auch die Kenntnisnahme von den Verbindungsdaten verbunden, weil diese zusammen mit dem Inhalt in der selben Datei gespeichert sind. Wiederum steht dieser Umstand aber einer Kenntnisnahme des Inhalts nicht entgegen, denn § 100a StPO erscheint als Ermächtigungsgrundlage für den Zugriff auf Verbindungsdaten ebenfalls geeignet. Dies folgt aus dem Begriff der “Überwachung”. Damit ist nicht nur die Erfassung von Inhalten, sondern auch der näheren Umstände der Telekommunikation,

---

<sup>204</sup> Oben C.I.3.e.

<sup>205</sup> Vgl. zum Zugriff auf Inhalte oben F.I.1.

<sup>206</sup> Oben F.III.1.

also der Verbindungsdaten gemeint.<sup>207</sup> Mit einer Überwachung von Telekommunikation nach § 100a StPO ist nämlich notwendigerweise auch die Kenntnisnahme ihrer Umstände verbunden.<sup>208</sup>

Über den Abruf von Nachrichten, die auf dem Mail-Server des Empfängers gespeichert sind, können die Strafverfolgungsbehörden aufgrund von § 100a StPO daher zulässigerweise auch an die Verbindungsdaten gelangen.

## **2. Zugriff nach § 94 StPO**

Eine Beschlagnahme nach § 94 StPO kommt dagegen auch hinsichtlich der Verbindungsdaten nicht in Betracht. Bezüglich des Nachrichteninhalts wurde bereits festgestellt, daß § 94 StPO nicht anwendbar ist.<sup>209</sup> Nichts anderes kann gelten, wenn es den Strafverfolgungsbehörden darum geht, Einsicht in Verbindungsdaten zu erhalten; denn auch die Verbindungsdaten unterstehen dem Schutz von Art. 10 Abs. 1 GG und – als nähere Umstände der Telekommunikation – von § 85 TKG.

## **3. Auskunftsanspruch nach § 100g Abs. 1 StPO**

Nach § 100g Abs. 1 StPO haben die geschäftsmäßigen Erbringer von Telekommunikationsdiensten Auskunft über Telekommunikationsverbindungsdaten zu erteilen. Denkbar ist daher, daß der Betreiber des Mail-Servers Einblick in die E-Mails nimmt und der anfragenden Strafverfolgungsbehörde diejenigen Daten im Header der E-Mail mitteilt, die in § 100g Abs. 3 StPO genannt sind. Auf dieser Basis können die Strafverfolgungsbehörden folgende Er-

---

<sup>207</sup> Bär, Computerdaten, S. 325, zur Überwachung des Fernmeldeverkehrs nach § 100a Abs. 1 a.F.; vgl. auch *Germann*, S. 543.

<sup>208</sup> Dementsprechend definiert auch § 4 Nr. 15 TKÜV-E (zur TKÜV-E oben Fn. 177) die zu überwachende Telekommunikation als Inhalte zuzüglich der sie bezeichnenden näheren Umstände

<sup>209</sup> Oben F.III.2.

kenntnisse gewinnen:

- E-Mail-Adressen von Absender und Empfänger  
Diese sind von § 100g Abs. 3 Nr. 1 StPO erfaßt.<sup>210</sup>
- Datum und Zeit, wie sie im Vorspann der E-Mail enthalten sind  
(§ 100g Abs. 3 Nr. 2 StPO)

Diese Daten werden von § 100g Abs. 3 StPO erfaßt, weil es sich nach der hier vertretenen Auffassung um Daten der *Telekommunikation*<sup>211</sup> handelt.

Im Vergleich zu § 100a StPO, der im Ergebnis den Zugriff auf alle in der E-Mail enthaltenen Verbindungsdaten (z.B. auch den Übertragungsweg) ermöglicht, reicht die Auskunft nach § 100g Abs. 1 StPO weniger weit, unterliegt aber auch geringeren Anforderungen. U.a. genügt bereits der Verdacht einer Straftat von erheblicher Bedeutung, ohne daß es sich um eine Katalogtat nach § 100a StPO handeln muß, wie durch das Wort "insbesondere" im einleitenden Satzteil deutlich wird. Der Anspruch nach § 100g Abs. 1 StPO hat daher eine eigenständige Bedeutung.

#### **4. Auskunftsanspruch nach § 89 Abs. 6 TKG**

Nach § 89 Abs. 6 TKG haben die geschäftsmäßigen Erbringer von Telekommunikationsdiensten Auskunft über die persönlichen Daten ihrer Kunden zu geben, die sie für die Begründung eines Vertragsverhältnisses erhoben haben. Unabhängig von der rechtlichen Bedeutung dieser Vorschrift ist jedenfalls eindeutig, daß sie sich nicht auf Auskünfte über konkrete Kommunikationsvorgänge, also Verbindungsdaten, bezieht.<sup>212</sup> Da in E-Mails nur Verbindungsdaten gespeichert sind, besteht ein Auskunftsanspruch nach § 89

---

<sup>210</sup> Vgl. die Gesetzesbegründung, BT-Drucks. 14/7008, S. 7.

<sup>211</sup> Vgl. dazu oben F.III.1.b.aa.

<sup>212</sup> Bär, Online-Kommunikation, S. 640.

Abs. 6 TKG hier nicht.

## **V. Logdateien der Diensteanbieter**

Auch aus den Logdateien, die auf dem Mail-Server, dem Terminal-Server des Zugangsvermittlers sowie beim Betreiber des Telefonnetzes geführt werden, können sich Aufschlüsse über die Identität von Kommunikationsteilnehmern ergeben. Da es sich hierbei um Verbindungsdaten handelt, werden alle Dateien gemeinsam erörtert.

### **1. Zugriff nach § 100a StPO**

#### **a) Allgemeines**

Ein Zugriff auf diese Daten nach § 100a StPO ist grundsätzlich möglich. Dies gilt für Angaben zu Datum, Zeit und Dauer einer Verbindungsaufnahme (Anruf, Einsenden einer E-Mail, Abrufen einer E-Mail), aber auch für IP-Adressen und die Tatsache, welchem Benutzer zu einer bestimmten Zeit eine bestimmte IP-Adresse zugewiesen ist. Dies folgt aus der Tatsache, daß es sich einerseits bei der IP-Adresse um die "Internet-Identität" einer Person handelt, die einen bestimmten Kommunikationsdienst benutzt, und andererseits für eine Maßnahme nach § 100a StPO die reale Identität des Beschuldigten noch nicht bekannt zu sein braucht.<sup>213</sup>

Vielmehr soll diese reale Identität gerade ermittelt werden. Die Nutzung der IP-Adressen entspricht daher genau dem Zweck des § 100a StPO. Die Situation ist vergleichbar mit einer Überwachung, die den Zweck verfolgt, die reale Bedeutung von Codewörtern oder Codenamen zu ermitteln.

#### **b) zeitlicher Anwendungsbereich**

§ 100a StPO gilt nur für die in der Zukunft, d.h. für die nach

---

<sup>213</sup> *Kleinknecht/Meyer-Goßner*, § 100a Rn. 9.

Erlaß einer entsprechenden Anordnung stattfindende Telekommunikation. Dies wird aus der Verwendung der Begriffe “Überwachung” und “Aufzeichnung” deutlich, die implizieren, daß ein künftiger Vorgang, dessen Zeitpunkt noch nicht feststeht, der staatlichen Kontrolle unterworfen werden soll. Aufgrund von §§ 100a, 100b Abs. 3 StPO kann daher von den Diensteanbietern z.B. nicht eine zurückliegende Verfolgung von Einwahlvorgängen anhand ihrer Logdateien oder eine Herausgabe dieser Unterlagen verlangt werden.

## **2. Zugriff nach § 94 StPO**

Eine Beschlagnahme der Logdateien kommt nicht in Betracht, weil die Strafverfolgungsbehörden dadurch Kenntnis von Verbindungsdaten erhalten würden. Zu einem solchen Eingriff in Art. 10 Abs. 1 GG und § 85 TKG ermächtigt § 94 StPO aber nicht.<sup>214</sup>

## **3. Auskunftsanspruch nach § 100g Abs. 1 StPO**

Möglich ist dagegen die Abfrage von Verbindungsdaten für die Vergangenheit nach § 100g Abs. 1 StPO. Die für die Strafverfolgungsbehörden relevanten Daten (Rufnummern, Login-Namen, IP-Adressen o.ä.) können unter § 100g Abs. 3 Nr. 1 subsumiert werden. Unter dem Begriff “Kennung” ist nicht nur die telefonische Rufnummer, sondern auch eine E-Mail-Adresse oder auch IP-Adresse<sup>215</sup> zu verstehen. “Berechtigungskennung” ist u.a. der beim Aufbau der Verbindung angegebene Login-Name. Zeitangaben hat der Diensteanbieter nach § 100g Abs. 3 Nr. 2 zu übermitteln. Möglich ist damit insbesondere eine Auskunft über die Zuordnung dynamischer IP-Adressen zu einem Benutzer bzw. dessen Login-Namen.

---

<sup>214</sup> Oben F.III.2.a und c.

<sup>215</sup> So ausdrücklich die Gesetzesbegründung, BT-Drucks. 14/7008, S. 7.

Auskunft über diese Daten können die Strafverfolgungsbehörden aufgrund einer entsprechenden Anordnung auch für die Zukunft verlangen (§ 100g Abs. 1 Satz 3 StPO).

#### **4. Auskunftsansprüche nach §§ 89 Abs. 6 und 90 TKG**

Ein Anspruch nach § 89 Abs. 6 TKG scheidet aus dem bereits dargestellten Grund aus, daß sich diese Bestimmung nur auf Bestandsdaten bezieht, es hier aber um die Auskunft über Verbindungsdaten geht. Das gleiche gilt für § 90 TKG; damit können die Strafverfolgungsbehörden beim Betreiber des Telefonnetzes einen Teil der Bestandsdaten (Name und Anschrift) von Absender und Empfänger ermitteln, dagegen keine Verbindungsdaten.

## **VI. Kundendateien der Diensteanbieter**

Die Umsetzung der mit Hilfe der vorgenannten Methoden gesammelten Informationen in aussagefähige Personendaten, die für die weiteren Ermittlungen verwendet werden können, macht in der Regel einen Zugriff auf eine weitere Datei erforderlich, in der die Diensteanbieter die Zuordnung von Login-Namen, E-Mail-Adressen – und ggf. auch *statischen* IP-Adressen – oder Rufnummern zu den wirklichen Namen der Kunden einschließlich weiterer Daten wie Anschriften festhalten. Bei diesen Daten handelt es sich um Bestandsdaten.

### **1. Zugriff nach § 100a StPO**

Ein Zugriff nach § 100a StPO ist nicht möglich. Die Kundendateien gehören weder zur Telekommunikation noch ist die Zuordnung ein näherer Umstand einer Telekommunikation. Diese Daten entstehen nicht im Zusammenhang mit einem konkreten Kommunikationsvorgang, sondern dienen allgemein der Durchführung des Vertragsverhältnisses zwischen Privatperson und Diensteanbieter.

## **2. Auskunftsanspruch nach § 100g Abs. 1 StPO**

Ebenfalls keinen Zugriff können die Strafverfolgungsbehörden durch eine Auskunft nach § 100g Abs. 1 StPO erhalten. Bei den Bestandsdaten handelt es sich nicht um Telekommunikationsverbindungsdaten, also Daten, die zu einem konkreten Telekommunikationsvorgang gehören. Ihre Abfrage fällt daher nicht in den Anwendungsbereich von § 100g Abs. 1 StPO.<sup>216</sup>

## **3. Auskunftsanspruch nach § 89 Abs. 6 TKG**

Nach seinem Wortlaut ermöglicht es § 89 Abs. 6 TKG den Strafverfolgungsbehörden, Auskünfte über persönliche Daten zu verlangen, die für die Begründung und Durchführung eines Vertragsverhältnisses notwendig sind. Dazu gehört gerade auch die Zuordnung von wirklichen Namen zu Login-Namen, E-Mail-Adressen, Rufnummern o.ä., weil diese unabhängig von einem konkreten Kommunikationsvorgang ist. Bedeutung und genauer Inhalt der Vorschrift sind allerdings in mehrfacher Hinsicht umstritten.

### **a) Rechtsnatur**

Diskutiert wird, ob die Vorschrift den darin genannten Stellen tatsächlich eine Befugnis zur Anforderung einer Auskunft einräumt oder lediglich für die Diensteanbieter die datenschutzrechtliche Erlaubnis zur Datenübermittlung darstellt.<sup>217</sup> In der Praxis erfolgen Anfragen derzeit auf der Basis von § 89 Abs. 6 TKG.<sup>218</sup>

Für einen lediglich datenschutzrechtlichen Charakter spricht zwar der Standort der Vorschrift in § 89 TKG, der sich allgemein mit dem Datenschutz befaßt. Eine Betrachtung des Wortlauts kann

---

<sup>216</sup> BT-Drucks. 14/7008, S. 7.

<sup>217</sup> *Wuermeling/Felixberger*, in: CR 1997, 555 (559).

<sup>218</sup> BT-Drucks. 14/7008, S. 7.

jedoch nur dazu führen, darin zugleich auch eine Befugnisnorm zu sehen. Dies folgt aus der Formulierung, nach der die Auskunft möglich sein soll, soweit dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist. Hielte man die Bestimmung nicht für eine Befugnisnorm, so müßten in der StPO und im OWiG Rechtsgrundlagen für eine Datenerhebung bei Dritten zur Verfügung stehen.<sup>219</sup> Solche Befugnisse existieren in der StPO aber nur sehr eingeschränkt<sup>220</sup> und im OWiG überhaupt nicht. Einem Auskunftersuchen durch Verwaltungsbehörden steht zudem nicht § 46 Abs. 3 OWiG entgegen, weil die Kundendaten nicht dem Brief-, Post- und Fernmeldegeheimnis unterliegen.

In § 89 Abs. 6 TKG keine Befugnisnorm zu sehen, würde somit bedeuten, dem Gesetzgeber zu unterstellen, er habe trotz ausdrücklicher Erwähnung des Zwecks der Strafverfolgung und der Verfolgung von Ordnungswidrigkeiten eine Norm praktisch ohne Anwendungsbereich für die zuständigen Behörden geschaffen. Dies ist aber nicht überzeugend. Vielmehr ist davon auszugehen, daß die Strafverfolgungsbehörden aufgrund von § 89 Abs. 6 TKG tatsächlich berechtigt sind, die beschriebenen Auskünfte zu verlangen. Die Abfrage von Bestandsdaten ist somit nach § 89 Abs. 6 TKG zulässig.

#### **b) Bezeichnung des Kunden**

Offensichtlich ist, daß die Diensteanbieter über Bestandsdaten nur Auskunft geben können, wenn ihnen ein bestimmtes anderes Datum vorgelegt wird, anhand dessen sie den Kunden, d.h. Absender und Empfänger, identifizieren können. Streitig ist, ob es sich bei diesem Datum ebenfalls um ein Bestandsdatum handeln muß

---

<sup>219</sup> *Wuermeling/Felixberger*, in: CR 1997, 555 (560).

<sup>220</sup> Z.B. ist § 98a StPO zum maschinellen Abgleich von Daten nur bei bestimmten Straftaten von erheblicher Bedeutung anwendbar.

(z.B. Name, Kundennummer o.ä.), oder ob dies auch ein Verbindungsdatum sein kann.

Relevant ist dieser Streit, wenn die Strafverfolgungsbehörden auf eine dynamisch zugewiesene IP-Adresse stoßen. Da es sich hierbei um ein Verbindungsdatum handelt, stellt sich die Frage, ob diese Adresse als Identifizierungsmerkmal verwendet werden kann mit dem Ziel, die Person zu ermitteln, deren Rechner die Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Dies wird teilweise mit der Begründung bejaht, daß mit der Anfrage nur Bestandsdaten erlangt werden sollten.<sup>221</sup> Diese Auffassung verkennt aber den Sinn des Schutzes der Verbindungsdaten. Dieser dient gerade dazu, eine Identifizierung der Kommunikationsteilnehmer anhand ihrer Verbindungsdaten nur unter verschärften Voraussetzungen zuzulassen, wie sie sich in § 100g Abs. 1 StPO finden.

Als Bezeichnung zur Identifizierung eines Kunden, d.h. von Absender und Empfänger, kommen daher nur andere Bestandsdaten in Frage. Insbesondere die Zuordnung von dynamischen IP-Adressen und Namen kann nur über § 100g Abs. 1 StPO erfolgen.<sup>222</sup>

#### **4. Auskunftsanspruch nach § 90 TKG**

Über ein Auskunftersuchen nach § 90 TKG können die Strafverfolgungsbehörden den Namen und die Anschrift von Absender und Empfänger aus der Kundendatei des Betreibers des Telefonnetzes ermitteln.

#### **5. Zugriff nach § 94 StPO**

Praktisch dürfte eine Beschlagnahme kaum in Frage kommen, weil mit ihr nicht mehr Erkenntnisse gewonnen werden können

---

<sup>221</sup> Meseke, in: Kriminalistik 2000, 245 (249).

<sup>222</sup> Vgl. Gundermann, in: DuD 1999, 681 (686) zum früheren § 12 FAG.

als über § 89 Abs. 6 TKG. Dazu kommt die Einschränkung, daß die Beschlagnahme nach § 98 Abs. 1 StPO grundsätzlich durch den Richter angeordnet werden muß, während die Auskunft nach § 89 Abs. 6 TKG auch schon von den Strafverfolgungsbehörden verlangt werden kann.

Auch rechtlich bereitet eine Beschlagnahme erhebliche Schwierigkeiten. Selbst wenn man sie grundsätzlich für möglich hält, ergeben sich Probleme aber sowohl in bezug auf die Berufsfreiheit der Diensteanbieter als auch das Recht auf informationelle Selbstbestimmung Unbeteiligter. Aus diesem Grund wäre die Inverwahrnehmung des Datenträgers, der die gesamte Kundendatei und damit zum Großteil für die Strafverfolgungsbehörden nicht relevante Daten enthält, wegen des Risikos überschießender Datengewinnung unzulässig.<sup>223</sup> Die Sicherstellung der relevanten Daten müßte daher in anderer Weise (§ 94 Abs. 1 2. Alt. StPO) durch Anfertigung von Kopien erfolgen.<sup>224</sup> Das Ermittlungsergebnis entspricht damit aber den Erkenntnissen aus einer Auskunft des Diensteanbieters nach § 89 Abs. 6 TKG.

## **VII. Zusammenfassung**

Die Teilnehmer einer Kommunikation lassen sich mit Hilfe von Verbindungs- und Bestandsdaten identifizieren. Die relevanten Informationen sind in einer Vielzahl verschiedener Quellen enthalte, für die verschiedene Ermächtigungsgrundlagen gelten. Dabei kommt es in wesentlichen Punkten zu einem Gleichlauf mit dem Zugriff auf die Inhalte von E-Mails.

Soweit Verbindungsdaten aus E-Mails ermittelt werden sollen, die

---

<sup>223</sup> Bär, Computerdaten, S. 276 f.

<sup>224</sup> Dazu näher oben F.I.2.b.

auf dem PC des Empfängers liegen, ist dies mit einer Beschlagnahme des jeweiligen Datenträgers nach § 94 StPO möglich.

Solange E-Mails auf einem Mail-Server zwischengespeichert sind, können die Verbindungsdaten ebenfalls zusammen mit dem Inhalt nach § 100a StPO ermittelt werden, da die näheren Umstände der Telekommunikation von dieser Bestimmung noch erfaßt sind. In Betracht kommt außerdem ein Auskunftsanspruch gegen den Betreiber des Mail-Servers gemäß § 100g Abs. 1 StPO auf Mitteilung bestimmter Umstände aus dem Header der E-Mail; dies ist bedeutsam, weil § 100g Abs. 1 StPO niedrigere Tatbestandsvoraussetzungen als § 100a StPO hat.

Weitere wichtige Daten wie IP-Adressen und Login-Namen können die Logdateien der beteiligten Diensteanbieter liefern. Ein Zugriff auf diese Informationen durch eine Beschlagnahme nach § 94 StPO oder §§ 89 Abs. 6, 90 TKG scheidet aus, weil die Daten als Umstände der Kommunikation dem Brief-, Post- und Fernmeldegeheimnis unterliegen. Möglich ist dagegen die Anwendung von § 100a StPO und § 100g Abs. 1 StPO. Damit können Erkenntnisse über konkrete Kommunikationsvorgänge gewonnen werden, insbesondere die Zuordnung dynamischer IP-Adressen zu Login-Namen.

Die Bestandsdaten in den Kundendateien der Diensteanbieter sind nur durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt. Ihre Abfrage ist nach § 89 Abs. 6 TKG möglich, sofern zur Identifizierung des Kunden ein anderes Bestandsdatum bekannt ist. Name und Anschrift können beim Betreiber des Telefonnetzes auch über § 90 TKG ermittelt werden. Eine Beschlagnahme nach § 94 StPO ist angesichts dieser Befugnisse praktisch nicht relevant.

## **H. Zusammenfassung und Ausblick**

### **I. Ergebnisse der Untersuchung**

Die zunehmende Verbreitung des Kommunikationsmittels E-Mail wirft angesichts der Tatsache, daß diese Technik in den Bestimmungen des Grundgesetzes nicht explizit erwähnt ist, eine Reihe rechtlicher Fragen auf.

Aus verfassungsrechtlicher Sicht ist festzustellen, daß die Überwachung von E-Mail verschiedene Grundrechte berührt. Zu unterscheiden sind dabei die Partner der Kommunikation einerseits und der Betreiber eines Mail-Servers oder andere Diensteanbieter andererseits. Zugunsten der Kommunikationspartner schützt das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG eine E-Mail vom Zeitpunkt der Übertragung an den Mail-Server des Absenders bis zum Herunterladen der Nachricht durch den Empfänger von dessen Mail-Server; inbegriffen ist der Zeitraum, während dessen die E-Mail auf dem Mail-Server des Empfängers zwischengespeichert wird. Zugunsten der Diensteanbieter schließt es Art. 13 Abs. 1 GG aus, daß sich die Strafverfolgungsbehörden die Möglichkeit zum Zugriff auf für sie interessante Daten durch staatliches Hacking verschaffen; insoweit fehlt zumindest eine einfachgesetzliche Ermächtigungsgrundlage.

Der Zugriff auf Inhalte von E-Mails ist während der Übertragungsphase nur aufgrund von § 100a StPO möglich. Das gleiche gilt, solange sich eine Nachricht auf dem Mail-Server des Empfängers befindet. Eine Beschlagnahme nach § 94 StPO ist daneben ausgeschlossen. Sie ist vielmehr nur hinsichtlich E-Mails möglich, die sich noch auf dem PC des Absenders oder bereits auf dem PC des Empfängers befinden. Es zeigt sich somit das auch dem jeweiligen Grundrechtsschutz entsprechende Bild, daß die Ermittlungsmög-

lichkeiten der Strafverfolgungsbehörden solange eingeschränkt sind wie eine E-Mail sich weder im Machtbereich des Absenders noch des Empfängers befindet.

Verbindungsdaten von E-Mails können von den Strafverfolgungsbehörden in der Regel auf die gleiche Weise ermittelt werden wie der Inhalt von E-Mails. Für Informationen aus Logdateien steht wegen des Schutzes durch Art. 10 Abs. 1 GG nur ein Auskunftsanspruch nach § 100g Abs. 1 StPO offen. Bestandsdaten in Kundendateien stehen nicht unter dem Schutz des Art. 10 Abs. 1 GG, sondern nur des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG); sie können von den Strafverfolgungsbehörden im Wege von Auskunftsverlangen nach § 89 Abs. 6 TKG und – beschränkt auf den Betreiber des Telefonnetzes – nach § 90 TKG genutzt werden.

## **II. Die Notwendigkeit einer gesetzlichen Neuregelung**

Betrachtet man die Grundfrage dieser Arbeit, inwieweit die hergebrachten Ermächtigungsgrundlagen auf die moderne Kommunikationsform E-Mail anwendbar sind, so fällt das Ergebnis zunächst positiv aus. Mit § 100a StPO steht eine Bestimmung zur Verfügung, die während der Übermittlung von E-Mails deren lückenlose Kontrolle erlaubt. Dies scheint auch rechtspolitisch sinnvoll, weil bisher auch schon andere moderne Kommunikationstechniken wie Telefax der Überwachung unterworfen waren.<sup>225</sup>

Unabhängig davon, ob man dennoch die Ermittlungsmöglichkeiten auf ein nicht mehr akzeptables Minimum beschränkt sieht,<sup>226</sup> ändert sich dieser Eindruck aber bei einem Blick auf die

---

<sup>225</sup> *Kleinknecht/Meyer-Goßner*, § 100a Rn. 2.

<sup>226</sup> So *Bär*, Anmerkung, S. 177.

Kommunikationsformen Brief und Telegramm. In ihnen können dieselben Inhalte wie in E-Mails übermittelt werden. Gleichwohl sind die Zugriffsmöglichkeiten der Strafverfolgungsbehörden hier deutlich größer.

Zwar scheidet während der Beförderungsphase eine einfache Beschlagnahme nach § 94 StPO aus, weil in diesem Zeitraum nur der speziellere § 99 StPO anwendbar ist. Auch diese Vorschrift schützt den Brief oder das Telegramm aber nicht in gleicher Weise wie § 100a StPO eine E-Mail, denn § 99 StPO sieht weder einen Straftatenkatalog noch eine Subsidiaritätsklausel vor. Diese Einschränkungen werden nicht dadurch kompensiert, daß im Falle des § 99 StPO die Beschlagnahmeverbote des § 97 StPO anwendbar sind; diese betreffen nämlich nur Sonderfälle, während die strengen Anforderungen für E-Mails aller Art gelten.<sup>227</sup>

Im Ergebnis hängen damit der Schutz einerseits und die Möglichkeiten der Strafverfolgungsbehörden andererseits nach geltendem Recht davon ab, ob Nachrichten in körperlicher oder unkörperlicher Form übermittelt werden. Dies führt zu rechtlichen wie rechtspolitischen Fragen.

Auf rechtlicher Ebene stellt sich das Problem eines möglichen Verstoßes gegen den Gleichheitssatz (Art. 3 Abs. 1 GG). Eine Ungleichbehandlung von Sachverhalten ist nur solange zulässig wie zwischen ihnen Unterschiede von solcher Art und solchem Gewicht bestehen, daß eine abweichende Behandlung gerechtfertigt erscheint.<sup>228</sup> Zu prüfen wäre, ob die bloße Tatsache der Körperlichkeit einer Nachricht ein Umstand ist, der einen solchen

---

<sup>227</sup> So im Ergebnis auch *Germann*, S. 535; a.A. *Palm/Roy*, Mailboxen, S. 1795 f., die keinen Wertungswiderspruch erkennen.

<sup>228</sup> *Jarass/Pieroth*, Art. 3 Rn. 27.

Unterschied begründen kann. Eine Antwort muß allerdings an dieser Stelle offen bleiben.

Rechtspolitisch erscheint die gegenwärtige Situation unbefriedigend, weil sich Straftäter durch die Wahl des Kommunikationsmittels E-Mail bewußt einer Überwachung entziehen können. Dies könnte in Zukunft zu einem Verlust der Effektivität der traditionellen Briefkontrolle führen.

Eine Reform der Überwachungsvorschriften ist daher äußerst wünschenswert. Ausgangspunkt sollte dabei die Konzentration auf die Nachricht als solche sein, unabhängig von der Form der Kommunikation, die für ihre Übermittlung benutzt wird. Nur durch eine solche, im weitesten Sinne technikneutrale Formulierung kann der überall anzutreffenden Konvergenz, d.h. der Verschmelzung früher getrennter Techniken, Rechnung getragen werden. Diese Vorgehensweise würde verhindern, daß die Bestimmungen zu schnell veralten, und damit auch der Rechtssicherheit in einem sensiblen Bereich dienen.