Ulf Buermeyer

Technischen Grundlagen und rechtliche Grenzen der Quellen-Telekommunikationsüberwachung

insbesondere: der Begriff der »laufenden Kommunikation« im Sinne der Online-Durchsuchungs-Entscheidung[1]

I. Einleitung

Die Überwachung der Kommunikation im Internet sowie der Zugriff auf Computer über das Netz sind spätestens seit der Diskussion um die sogenannte Online-Durchsuchung|[2] zum Dauerbrenner in der innenpolitischen Debatte geworden. Zur Klärung der verfassungsrechtlichen Fragen hat das BVerfG bereits 2008 mit seinem Urteil zum nordrhein-westfälischen Verfassungsschutzgesetz|[3] (sogenannte »Online-Durchsuchungs-Entscheidung«, im Folgenden: OD-Entscheidung) einen maßgeblichen Beitrag geleistet: Mit der Herleitung und Ausformung des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme|[4] – kurz »IT-Grundrecht« oder »Computer-Grundrecht« genannt – hat das Gericht für Online-Durchsuchungen klare rechtliche Voraussetzungen definiert. Und auch dort, wo die Entscheidung zunächst weniger ausdifferenziert erscheint, so zur Frage der Zulässigkeit der Telekommunikationsüberwachung unter Einsatz von Trojanern, deutet sie doch hinreichend genau an,|[5] welche Anforderungen an eine verfassungsgemäße »Quellen-TKÜ« zu stellen sind.

1 Der Beitrag beruht auf einer gutachterlichen Stellungnahme des Verfassers für das Bundesministerium der Justiz sowie einem früheren Beitrag für die HRRS[65] und wurde für den Strafverteidigertag auf den rechtlichen und tatsächlichen Stand vom Dezember 2012 gebracht. Der Autor ist Beisitzer einer Schwurgerichtskammer des Landgerichts Berlin und ehemaliger wissenschaftlicher Mitarbeiter des Bundesverfassungsgerichts (Dezernate Prof. Dr. Hassemer und Prof. Dr. Voßkuhle). Der Beitrag gibt allein seine persönliche Auffassung wieder.

2 Zu den Begrifflichkeiten und zum technischen Hintergrund vgl. eingehend *Buermeyer* HRRS 2007, 154 ff.

3 Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 = HRRS 2008 Nr. 160.

4 Vgl. grundlegend *Bäcker* in *Uerpmann/Witzack (Hrsg.)*, Das neue Computer-Grundrecht, S. 1 ff, *Hornung* CR 2008, S. 299 ff.

5 Vgl. *Buermeyer/Bäcker* a.a.O. m. w. N., vgl. oben Fn. 1.

Der Begriff »Quellen-TKÜ« bezeichnet das Überwachen von Telefongesprächen, die nicht über klassische Telefonverbindungen (Festnetz bzw. Mobilfunk), sondern über das Internet geführt werden (sog. Voice-over-IP- oder kurz VoIP-Verbindungen), durch Infektion des verwendeten Endgeräts|[6] mit einer Überwachungssoftware. Hintergrund hierfür ist, dass bei VoIP die Audio-Daten in den beteiligten Rechnern oder Smartphones regelmäßig noch vor dem Versand der Daten über das Internet verschlüsselt werden. In einem solchen Fall ist das »klassische« Überwachen der Telekommunikation etwa beim Internet-Zugangsanbieter (§ 100a Abs. 1 i.V.m. § 100b Abs. 3 StPO) wenig effektiv: Zwar lässt sich dort der verschlüsselte Datenstrom mitschneiden und hieraus auch der VoIP-Datenstrom isolieren. Doch ist es nur mit erheblichem Aufwand oder - je nach eingesetztem Verschlüsselungsverfahren - gar nicht möglich, die Daten zu entschlüsseln und so die Sprache wieder hörbar zu machen.|[7] Ein erfolgversprechender Zugriff auf verschlüsselt geführte Internet-Telefongespräche ist daher regelmäßig|[8] nicht mehr durch Zugriff auf der Übertragungsstrecke, sondern nur noch durch »Anzapfen« eines der beteiligten Endgeräte möglich, um dort den noch bzw. bereits wieder entschlüsselten Telefonverkehr »an der Quelle« abgreifen zu können. Damit läuft die eingesetzte Verschlüsselung auf der Übertragungsstrecke letztlich leer. Aus dem Zugriff am Endgerät, also an der Quelle, leitet sich auch die gängige Bezeichnung »Quellen-TelekommunikationsÜberwachung« oder kurz »Quellen-TKÜ« ab.

Der Erste Senat des BVerfG war sich dieser technischen Möglichkeit durchaus bewusst, weswegen die OD-Entscheidung auch hierzu verfassungsrechtliche Vorgaben formuliert.|[9] Diese Aussagen der OD-Entscheidung werden in der Praxis jedoch nicht immer ernst genug genommen. Zwar hat der Verfasser gemeinsam mit *Bäcker* bereits 2009 am Beispiel eines amtsgerichtlichen Beschlusses die mitunter bedenklich selektive Rezeption der OD-Entscheidung kritisiert und die verfassungsrechtlichen Voraussetzungen einer Quellen-TKÜ dargelegt,|[10] insbesondere im repressiven Bereich das Erfordernis einer

6 Dabei handelt es sich keineswegs mehr regelmäßig um Computer im klassischen Sinne. Auf leistungsfähigen Mobilfunkgeräten (»Smartphones“) - etwa dem *iPhone* - aber auch auf Tablet-Computern (etwa dem *iPad*) lassen sich kleine Programme (sog. Apps) installieren, um über den Internet-Zugang des Handys Internet-Telefondienste zu nutzen. Auch Skype ist für iPhone & iPad ebenso wie für andere mobile Plattformen verfügbar.

7 Zu technischen Einzelheiten vgl. bereits *Buermeyer* HRRS 2007, 154, 159 f. und *Sankol* CR 2008, 13.

8 Insbesondere für den Dienst Skype liegt gibt es allerdings ernstzunehmende Anhaltspunkte dafür, dass der Betreiber durchaus in der Lage ist, auch Skype-Gespräche abzuhören, vgl. unten unter III. 4.

9 Vgl. unten unter IV.

10 Vgl. oben Fn. 1.

dedizierten Rechtsgrundlage in der StPO. Auch teilt die rechtwissenschaftliche Literatur diese Rechtsansicht inzwischen nahezu einhellig,[11] ebenso der Generalbundesanwalt,[12] während lediglich einige ältere Stimmen aus der untergerichtlichen Rechtsprechung eine Quellen-TKÜ bereits auf der Grundlage des § 100a Abs. 1 StPO für zulässig hielten.[13]

Jedoch scheint die polizeiliche und nachrichtendienstliche Praxis das Instrument für so unverzichtbar zu halten, dass die verfassungsrechtlichen Anforderungen an eine rechtmäßige Quellen-TKÜ – insbesondere in Abgrenzung zu einer Online-Durchsuchung – nicht selten aus dem Blick zu geraten drohen. Der Bayerische Trojaner-Skandal,[14] der die *Frankfurter Allgemeine Zeitung* zu einer mehrseitigen Sonderbeilage[15] veranlasste, machte auf erschütternde Weise deutlich, wie wenig Bedeutung die handelnden Beamten dem Grundgesetz in seiner Auslegung durch die OD-Entscheidung im Überschwang des Ermittlungseifers letztlich beimaßen: Ohne erkennbares Unrechtsbewusstsein wurde eine grob unzulängliche Überwachungssoftware der hessischen Firma *Digitask* eingesetzt und sowohl eine Quellen-TKÜ als auch eine – wohl unstreitig rechtwidrige[16] – Online-Durchsuchung auf der Grundlage der StPO durchführt.[17]

11 Vgl. etwa *Albrecht*, JurPC Web-Dok. 59/2011; *Albrecht/Dienst* JurPC 5/2012; *Becker/Meinicke* StV 2011, 50; *Böckenförde* JZ 2008, 925, 934; *Braun* K&R 2011, 681; *Heckmann* in seiner soweit ersichtlich noch nicht veröffentlichten Stellungnahme für das Bundesministerium der Justiz vom Januar 2012; *Hoffmann-Riem* JZ 2008, 1009, 1014; *Hornung* CR 2008, 299, 300; *Vogel/Brodowski* StV 2009, 632 und *Wolter* SK-StPO § 100a Rn. 30. Auch *Bär*, lange Zeit ein Befürworter der Quellen-TKÜ schon nach geltender StPO, ist hiervon offenbar auch unter dem Eindruck des Landshuter Trojaner-Skandals abgerückt und vertritt nunmehr, dass es zumindest einer Klarstellung in der StPO bedürfe (MMR 2011, 691, 693). Anders hingegen noch *Schmitt* in *Meyer-Goßner,* StPO, § 100a StPO Rn. 7a, der darauf verweist, dass der Ermittlungsrichter (!) die technischen Anforderungen an eine zulässige Quellen-TKÜ auch auf der Grundlage von § 100a Abs. 1 StPO selbst regeln könne. Letzteres dürfte mit der Realität im ermittlungsrichterlichen Dezernat zumal an den Amtsgerichten nur wenig gemein haben, da die Regelung der Anforderungen insbesondere die technische Spezifikation des einzusetzenden Trojaners (!) und die genauen Umstände seines Einsatzes umfassen müsste. Dieser Ansatz berücksichtigt außerdem nicht den verfassungsrechtlichen Wesentlichkeitsgrundsatz (Art. 20 Abs. 3 GG), der den Gesetzgeber verpflichtet, die für die Grundrechtsausübung wesentlichen Fragen selbst und durch formelles Gesetz zu regeln. § 100b StPO schweigt indes zum Einsatz von Trojanern im Strafverfahren, und die Frage, welche Spionagesoftware der Staat in die Systeme seiner Bürger einbringen darf, scheint dem *Verf.* eine durchaus wesentliche zu sein.

12 Dies ergibt sich aus der Antwort der Bundesregierung auf eine Kleine Anfrage der Bundestagsfraktion der SPD, http://dipbt.bundestag.de/dip21/btd/17/110/1711087.pdf.

13 LG Hamburg, Beschluss vom 13. September 2010 - 608 Qs 17/10 - MMR 2011, 693; AG Bayreuth, Beschluss vom 17. September 2009 - Gs 911/09 - MMR 2010, 266; LG Landshut, 4 Qs 346/10.

14 Vgl. die zugrundeliegende Analyse des bayerischen Staatstrojaners durch den des *Chaos Computer Clubs:* http://www.ccc.de/de/updates/2011/staatstrojaner.

15 Frankfurter Allgemeine Zeitung vom 9. Oktober 2011: »Anatomie eines digitalen Ungeziefers“.

16 Statt aller *Schmitt* in *Meyer-Goßner*, StPO, § 100a Rn. 7b.

17 So der Prüfbericht des Bayerischen Landesbeauftragten für den Datenschutz *Petri*, http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

Das Vorgehen des bayerischen Landeskriminalamts mag zwar besonders grob erscheinen, doch stellen rechtswidrige Quellen-TKÜ-Maßnahmen im Rahmen strafprozessualer Ermittlungen|[18] keineswegs eine absolute Ausnahme dar, wie zuletzt die Antwort der Bundesregierung|[19] auf eine Kleine Anfrage der SPD-Fraktion im Deutschen Bundestag|[20] deutlich machte. Trotz dieser rechtsstaatlich unbefriedigenden Praxis ist bisher kein Gesetzentwurf in den Deutschen Bundestag eingebracht worden, der Online-Durchsuchung und/oder Quellen-TKÜ zu strafprozessualen Zwecken normenklar regeln oder auch eindeutig untersagen würde. Zu wünschen wäre demgegenüber, dass der Bundesgesetzgeber Voraussetzungen und Grenzen der Telekommunikationsüberwachung unter Einsatz von Trojanern möglichst umgehend und präzise regelt. Politische Akteure sollten davor auch nicht aus Sorge zurückscheuen, als Trojaner-Befürworter gebrandmarkt zu werden: Das Gegenteil ist der Fall, denn gegenwärtig vermag niemand auszuschließen, dass allzu sorglose Ermittlungsrichter noch Quellen-TKÜ-Maßnahmen auf Grundlage der derzeitigen StPO und damit ohne hinreichende grundrechtsschonende Begleitregelungen anordnen, wie sie nur eine spezielle gesetzliche Grundlage schaffen kann.

Vor diesem Hintergrund verfolgt dieser Beitrag das Ziel, die rechtpolitische Diskussion in zweierlei Hinsicht anzuregen und zu bereichern:

Zum einen soll ein Abriss der Kommunikation im Netz (unten II.) sowie der technischen Möglichkeiten und Grenzen ihrer Überwachung (unten III.) einen Überblick darüber verschaffen, worum es bei der Quellen-TKÜ überhaupt geht. Denn angesichts der allfälligen Fixierung auf die IP-Telefonie-Software *Skype* gerät nicht selten aus dem Blick, dass es hierzu eine Vielzahl an Alternativen gibt und auch andere verschlüsselte Formen der Kommunikation Bedeutung für die Strafverfolgung haben können, deren technische Details mitunter auch rechtlich zu einer differenzierten Betrachtung Anlass geben.

18 Im präventivpolizeilichen Bereich stellen sich die hier angesprochenen Rechtsfragen weniger gravierend, denn jedenfalls das BKA verfügt insoweit über eine Rechtgrundlage für Online-Durchsuchung (§ 20k BKAG) wie Quellen-TKÜ (§ 20l Abs. 2 BKAG) – freilich vorbehaltlich der Frage, ob die genannten Normen ihrerseits verfassungsgemäß sind: Über hiergegen erhobene Verfassungsbeschwerden ist bisher nicht entschieden.

19 http://dipbt.bundestag.de/dip21/btd/17/115/1711598.pdf; die genauen Zahlen verbergen sich in einem »VS-nfD“ gekennzeichneten Anhang, der nach den bisher öffentlich gewordenen Informationen für die Jahre 2008 bis 2011 im Bereich der Bundesbehörden eine Anzahl im unteren zweistelligen Bereich ausweist. Insgesamt ist für Bundes- und Landesbehörden von etwa einhundert durchgeführten Quellen-TKÜ-Maßnahmen in den Jahren 2008 bis 2011 auszugehen.

20 http://dipbt.bundestag.de/dip21/btd/17/110/1711087.pdf

Zum anderen möchte der Beitrag den Blick dafür schärfen, welche Kommunikationsinhalte überhaupt aus verfassungsrechtlicher Perspektive zu welcher Zeit mit einer Quellen-TKÜ erhoben werden dürfen (unten IV.). Beispielsweise werden mitunter Anwendungsbeispiele für die Notwendigkeit einer Quellen-TKÜ ins Feld geführt, für die jedoch aus verfassungsrechtlichen Gründen eine vollumfängliche Online-Durchsuchung erforderlich wäre. Insoweit ist die verfassungsrechtlich vorgeprägte Differenzierung zwischen Transportverschlüsselung und Inhaltsverschlüsselung maßgeblich.

II. Stichwortartige Übersicht über die derzeitigen Kommunikationsformen, die für die Telekommunikationsüberwachung von Bedeutung sind

Die folgende Übersucht versteht sich als *tour d'horizon*, erhebt aber keinen Anspruch auf Vollständigkeit.

1. Telefonie

- klassisch/leitungsgebunden und mobil, d.h. GSM[21], UMTS[22], LTE[23]
  - zwischen Telefonie-Endgeräten (jeweils mobil oder leitungsgebunden)
  - zwischen Telefonie-Endgeräten und Endgeräten, die VoIP[24]-Dienste nutzen, unter Verwendung eines Gateways – Beispiel: Skype-In[25] und Skype-Out[26]
- VoIP-Telefonie (Sprachtelefonie über IP-Netze, insbesondere das Internet)
  - unter Einschaltung eines »Providers«, der optional auch einen Übergang ins klassische Telefonnetz bietet
  - Skype
  - SIP[27] / RTP[28] für VoIP (Vielzahl von Anbietern, z.B. Sipgate GmbH)

21 Global Standard for Mobile Telecommunication – erster voll digitalisierter »Handy"-Standard

22 Universal Mobile Telecommunications System – Nachfolgesystem von GSM mit deutlich erhöhter Datenrate

23 Long Term Evolution – Nachfolgesystem zu UMTS mit nochmals deutlich gesteigerter Übertragungskapazität

24 Voice over IP – technisch nicht näher definierte Sammelbezeichnung für Sprachübertragung mittels des Internet-Protokolls (IP), beispielsweise Skype oder SIP

25 Ein Nutzer eines klassischen Telefonanschlusses (mobil oder Festnetz) ruft eine Rufnummer an, die an eine Skype-Kennung vermittelt wird.

26 Ein Skype-Nutzer ruft aus dem Skype-Netz heraus eine klassische Telefonnummer an.

27 Session Initiation Protocol; Standard-Protokoll zur Einleitung von VoIP-Gesprächen.

28 Real-Time Transport Protocol; ein Protokoll zur Übertragung von audiovisuellen Daten (etwa VoIP) über IP-Netzwerke.

- unter Verwendung eines eigenen Telefonie-Servers
- Software kommerziell und als Open Source verfügbar
- Beispiele: Asterisk (freie SIP-Implementierung) oder Mumble (stark verschlüsselnde OpenSource-VoIP-Lösung, Clients u.a. für Mobilfunkgeräte verfügbar)
- Skype setzt dedizierte Skype-Clients ein, während es für SIP eine Vielzahl von Client-Anwendungen für alle aktuellen Betriebssysteme gibt
- SIP/RTP-Verkehr lässt sich optional auch verschlüsseln, etwa mittels zfone /ZRTP.

2. E-Mail-Dienste (Übertragung von Texten oder beliebigen Dateien)

- WWW-basiert (»Webmailer«)
  - mit transportbasiert verschlüsselter (HTTPS|[29]) oder unverschlüsselter (HTTP|[30]) Kommunikation zum Webmail-Server
  - regelmäßig erfolgt die Weiterleitung zum E-Mail-Server des Empfängers (also auf der Strecke zwischen beteiligten E-Mail-Servern via SMTP|[31]) unverschlüsselt
  - Kommunikation ist auch über bloßes Ablegen einer Nachricht in einem zwischen den Kommunikationspartnern geteilten Postfach möglich, sodass es technisch zu keiner E-Mail-Kommunikation im engeren Sinne, insbesondere keiner unverschlüsselten Übertragung zwischen den E-Mail-Servern von Absender und Empfänger kommt.
- unter Verwendung dedizierter eMail-Programme (»Clients«)
  - in Senderichtung: SMTP
  - unter Verwendung von Transportverschlüsselung (SMTP over SSL|[32]/TLS|[33])
  - ohne Transportverschlüsselung: »einfaches« SMTP (wie zwischen zwei SMTP-Servern)

29 Secure Hypertext Transfer Protocol.

30 Hypertext Transfer Protocol.

31 Simple Mail Transfer Protocol.

32 Secure Socket Layer; ein mit nahezu allen Übertragungsprotokollen (etwa HTTP, IMAP, SMTP, POP3) zu kombinierendes Verschlüsselungsverfahren auf Transportebene, das auf Zertifikaten aufbaut, die von Zertifizierungsstellen ausgestellt werden, denen wiederum der Nutzer (bzw. der Hersteller der verwendeten Software) vertraut.

33 Transport Layer Security; Nachfolger des (bekannteren) SSL; TLS Version 1.0 ist mit SSL Version 3.1 identisch. Die Begriffe werden auch oftmals synonym verwendet.

- in Empfangsrichtung: POP3 | [34]/IMAP | [35]
  - transportbasiert verschlüsselt (POP3S/IMAPS)
  - unverschlüsselt (POP3/IMAP)
- mit Inhaltsverschlüsselung z.B. mittels PGP | [36] / GPG | [37]
  - kann mit allen obigen Verfahren kombiniert werden, d.h. verschlüsselte Inhalte können über einen nochmals mit SSL verschlüsselten Transportweg gesendet werden
  - z.B. kann eine Webmail-Oberfläche mit HTTPS-Übertragung verwendet werden, um (nochmals) PGP-kryptierte Nachrichten auszutauschen- außerdem gibt es Zusatzprogramme zu E-Mail-Clients, die Kryptographie-Funktionen weitgehend in die normalen Arbeitsschritte bei der E-Mail-Kommunikation integrieren (z.B. Enigmail als benutzerfreundliche Oberfläche für PGP/GPG)

3. Chat / Instant Messenging

- kaum übersehbare Vielzahl von Protokollen, etwa IRC, ICQ, Skype Chat, AIM (AOL Instant Messenging), Microsoft Network / Windows live, Jabber, Yahoo Chat, Google Talk, Facebook Chat, Mail.ru, MySpace Chat, Twitter, ...
- inzwischen tausende unterschiedlicher Anwendungsprogramme für alle Desktop- und Mobiltelefon-Betriebssysteme, die oftmals mehrere der Protokolle unterstützen
- Chat-Lösungen bieten eine Vielzahl von Verschlüsselungsverfahren
  - transportbasiert (d.h. auf der Strecke zwischen Client und Gegenstelle)
  - inhaltsbasiert (d.h. im jeweiligen Client vor der Übertragung an die Gegenstelle)
  - beides kombiniert (verschlüsselte Inhalte über verschlüsselte Transportwege)
- außerdem gibt es populäre Chat-Systeme auf WWW-Basis, etwa Facebook Chat.

34 Post Office Protocol, Version 3; ein weit verbreitetes Übertragungsverfahren für das Abrufen von eMails von einem Server.

35 Internet Message Access Protocol; ein Übertragungsverfahren für die Verwaltung von eMails auf einem eMail-Server und das gezielte Herunterladen von eMails.

36 Pretty Good Privacy; ein asymmetrisches Verschlüsselungsverfahren für beliebige Dateien, das insbesondere bei eMail verbreitet ist.

37 Gnu Privacy Guard; eine weitgehend kompatible Open-Source-Alternative zu PGP.

4. Foren / Newsgroups

- »klassisch«, aber von rasch abnehmender Bedeutung: sogenanntes Usenet/ Newsgroups über das NNTP[38]-Protokoll
  - öffentlich
  - unverschlüsselt
- WWW-basierte Foren
  - sternförmige Struktur – alle Teilnehmer kommunizieren mit einem zentralen Server, auf dem die Mitteilungen abgelegt und meist in Form von sogenannten Gesprächsfäden (»Threads«) strukturiert werden
  - öffentlich oder mit Zugangskontrolle (Benutzername / Passwort, ggf. zusätzliche Sicherungsmittel: IP-basiert, VPN[39], ...)
  - Verbindung zwischen Nutzer und Server kann per HTTPS verschlüsselt sein (transportbasierte Verschlüsselung)
  - wiederum zusätzliche Inhaltsverschlüsselung etwa mittels PGP/GPG technisch möglich (mir sind aber keine Beispiele bekannt)

III. Überblick über die technischen Möglichkeiten der TKÜ bei verschiedenen Formen der TK

1. verschlüsselte und unverschlüsselte Kommunikationsformen

Sowohl die *Transportverschlüsselung*[40] (regelmäßig mittels SSL, z.B. in Form von HTTPS, IMAPS, POPS oder bei der VoIP-Lösung Skype) als auch die *Inhaltsverschlüsselung* etwa mittels PGP/GPG sind als solche nicht in realistischen Zeiträumen zu brechen, sofern der Schlüssel nicht bekannt ist. Eine inhaltlich zielführende Überwachung ist daher nicht möglich, soweit lediglich die kryptierte Kommunikation überwacht wird, was etwa bei einer TKÜ-Maßnahme beim Internet-Zugangs-Provider gem. § 100a Abs. 1 StPO der Fall wäre.

Dies betrifft in der Praxis die oben genannten Kommunikationsmittel mit Ausnahme von

- E-Mail ohne Einsatz von Verschlüsselungsverfahren (POP, IMAP SMTP)
- HTTP (WWW ohne Verschlüsselung)
- Usenet / Newsgroups / unverschlüsselte Chats
- klassische Telefonie (Festnetz und Mobil)

38 Network News Transport Protocol.

39 Virtual Private Network; Sammelbezeichnung für Verfahren zur sicheren Verbindung zweier Rechner oder Netzwerke über eine nicht vertrauenswürdige Verbindung, etwa das öffentliche Internet.

40 Zum verfassungsrechtlichen Hintergrund und zur Abgrenzung der Begriffe Transport- und Inhaltsverschlüsselung siehe unten Seite 166 ff.

Soweit diese zuletzt genannten Kommunikationsverfahren ohne Verschlüsselung eingesetzt werden, ist eine Kenntnisnahme der Inhalte mittels einer klassischen TKÜ gem. § 100 Abs. 1 StPO prinzipiell möglich. Die Rekonstruktion sinnhafter Kommunikation aus dem bei der TKÜ gewonnenen, zunächst vollkommen unstrukturierten Datenstrom kann allerdings je nach Kommunikationsform einen ganz erheblichen technischen Aufwand verursachen.

Soweit hingegen zeitgemäße Verschlüsselungsverfahren (gleich ob transport- oder inhaltsbasiert) eingesetzt werden, ist eine Kenntnisnahme der Inhalte nach gegenwärtigem Stand der Technik grundsätzlich nicht möglich. Zwar kann der digitale Datenstrom auch in diesem Fall ausgeleitet werden, allerdings ist ein Rückschluss auf die ursprünglich übertragenen Daten nicht möglich.

2. Möglichkeiten zur Überwachung verschlüsselter Kommunikation

Erfolgversprechende Angriffe gegen eine lediglich transportbasierte Verschlüsselung mittels SSL (z.B. HTTPS, IMAPS) sind allerdings durch sog. Man-in-the-middle-Attacken (MITM) möglich. Bei MITM-Attacken wird dem System der Zielperson mittels bestimmter technischer Manipulationen vorgespiegelt, es sei beispielsweise mit dem E-Mail-Server vom GMX verbunden, während es tatsächlich mit einem dazwischen geschobenen Server (deswegen »in the middle«) einer Ermittlungsbehörde kommuniziert. Da in diesem Falle die Verschlüsselung des Leitungsweges zwischen der Zielperson und dem MITM-Server abläuft und letzterer hoheitlich kontrolliert ist, kann der Klartext der Kommunikation an diesem Punkt abgefangen werden. Zwecks Verschleierung der Maßnahme wird es sich regelmäßig empfehlen, die Kommunikation vom MITM-Server noch zum eigentlich gewünschten Zielserver weiterzuleiten.

MITM-Attacken gegen SSL-Verbindungen erfordern einen erheblichen technischen Aufwand, da für jeden Server, mit dem die verschlüsselte Kommunikation abgefangen werden soll, von einer Zertifizierungsstelle ein separates SSL-Zertifikat ausgestellt werden muss. Unmöglich ist dies zwar nicht; in jüngerer Zeit haben sich etwa Anhaltspunkte dafür ergeben, dass der iranische Geheimdienst gezielt in Server eine niederländischen SSL-Zertifizierungsstelle eingebrochen ist, um falsche Zertifikate von E-Mail-Dienstleistern ausstellen zu können und so die iranische Oppositionsbewegung zu überwachen.[41] Für eine rechtsstaatlich ausgeführte MITM-Attacke jedoch müsste eine Zertifizierungsstelle gezwungen werden, zu hoheitlichen Zwecken falsche Zertifikate auszustellen, etwa für www.gmx.de oder www.hotmail.com.

41 http://www.spiegel.de/netzwelt/web/0,1518,784626,00.html.

Freiwillig dürfte mit einer Kooperation kaum zu rechnen sein, da im Falle des Bekanntwerdens die Zertifizierungsstelle ihrerseits als nicht mehr vertrauenswürdig eingestuft würde, sodass ihre Zertifikate seitens der Browser- bzw. E-Mail-Client-Hersteller gesperrt würden.

Zudem muss dem System der Zielperson mittels gezielt falscher Antworten auf seine Domain-Name-Abfragen (sog. »DNS Spoofing«) die IP-Adresse des hoheitlichen Überwachungsservers untergeschoben werden. Letzteres setzt eine gezielte Manipulation des Datenstroms zum Zielsystem voraus, also in der Praxis die Kooperation des jeweiligen Providers oder einen unmittelbaren Zugriff auf das System.

MITM-Attacken sind hingegen nicht zielführend, wenn allein oder zusätzlich zur Verschlüsselung auf Transportebene auch Verfahren zur Inhaltsverschlüsselung eingesetzt werden, da MITM wie gezeigt allein die Transport-Sicherheit von SSL / TLS aushebeln kann. Nicht sinnvoll einsetzbar sind diese Attacken daher etwa gegen E-Mail-Kommunikation, die mit PGP/GPG verschlüsselt ist. Gegen *Skype* können technisch anders konstruierte Formen von MITM-Attacken implementiert werden, die nicht auf manipulierten SSL-Zertifikaten basieren. | [42]

Eine Abwandlung desselben Grundgedankens für VoIP-Verkehr stellt ein Microsoft-Patent vom Dezember 2009 | [43] dar, das allerdings auf sehr abstraktem Niveau argumentiert, sodass sich konkrete Aussagen in Bezug auf einzelne VoIP-Netze auf dieser Grundlage allein nicht treffen lassen. Allerdings bietet das Skype-Netz Möglichkeiten zur Implementierung dieses Patents.

Kommunikationsformen, die sich mittels MITM grundsätzlich überwachen lassen, sind z.B. Kommunikation mit WWW-Servern über HTTPS (z.B. Foren, Webmail) oder E-Mail-Dienste mit SSL-Verschlüsselung auf dem Transportweg (etwa IMAPS, POPS).

Nach derzeitigem Kenntnisstand ist die Entschlüsselung eines mit zeitgemäßer Kryptographie verschlüsselten Datenstroms als solche hingegen nicht möglich. Auf Umgehungsmöglichkeiten wie MITM wurde bereits hingewiesen; dabei wird allerdings keine Verschlüsselung gebrochen, sondern über die Identität des Kommunikationspartners getäuscht und sodann eine verschlüsselte Verbindung zwischen dem Zielsystem und dem Überwachungssystem aufgebaut (s.o.).

42 Siehe unten Seite 11.

43 http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&co1=AND&d=PG01&s1=20110153809.PGNR.&OS=DN/20110153809RS=DN/20110153809

Die StPO bietet außerdem bereits in ihrer heutigen Fassung andere Erkenntnismöglichkeiten, die anstelle einer Quellen-TKÜ einen der unmittelbaren Überwachung der Kommunikation zumindest in Teilen vergleichbaren Erkenntnisgewinn ermöglichen. Zu denken ist etwa an den Zugriff auf bei der Zielperson gespeicherte E-Mails im Wege einer Hausdurchsuchung beim Beschuldigten (§§ 102, 105 StPO) oder auf die beim Provider gespeicherten E-Mails im Wege einer Hausdurchsuchung bei einem Dritten (§§ 103, 105 StPO), bei letzterem naheliegend mit Abwendungsklausel im Falle freiwilliger Herausgabe. In beiden Fällen wäre die Beschlagnahme der E-Mails gem. §§ 94, 98 StPO grundsätzlich möglich.[44] Beides lässt sich ggf. noch durch eine TK-Überwachung beim Provider ergänzen. Jedenfalls im Falle einer Maßnahme unmittelbar gegenüber der Zielperson würde dies allerdings möglicherweise ermittlungstaktische Nachteile mit sich bringen.

Soweit Gespräche über VoIP in Rede stehen, wäre – sofern die engeren rechtlichen Voraussetzungen vorliegen – auch eine akustische Wohnraumüberwachung bei der Zielperson zu prüfen (§ 100c Abs. 1 StPO).

3. insbesondere: Überwachung von Skype-In und Skype-Out

Aus technischer Sicht sind Skype-In- sowie Skype-Out-Gespräche nach denselben Prinzipien wie klassische Telefonie zu überwachen, da es jeweils einen Übergabepunkt zwischen dem Skype-Netz und dem klassischen Telefonnetz gibt, an dem ein klassisches, unverschlüsseltes Audio-Signal abgegriffen werden kann.

Die praktische Durchsetzbarkeit dieser Möglichkeit liegt in den Händen der Fa. Skype. Gelingt es, mit dieser die Einrichtung einer Abhörschnittstelle zu vereinbaren, so unterscheiden sich Skype-In- sowie Skype-Out-Gespräche nicht mehr von »normalen« Telefongesprächen. Eine andere Alternative wäre eine klassische TKÜ-Maßnahme gegen die jeweiligen Endpunkte im klassischen Telefonnetz, also bei Skype-In gegen den Anrufer, bei Skype-Out gegen den Angerufenen.

4. insbesondere: Alternativen zur Quellen-TKÜ bei klassischen Skype-Gesprächen

Es liegt eine Vielzahl von Indizien vor, die darauf hindeuten, dass Skype mit Ermittlungsbehörden zu Zwecken der TKÜ zusammenarbeitet. So lässt sich Skype in den der Nutzung ihres VoIP-Dienstes zugrundeliegenden AGB aus-

44 BVerfGE 124, 43, 58 f.

drücklich das Recht zur Zusammenarbeit mit Ermittlungsbehörden einräumen:[45]

> »Skype, der örtliche Skype-Partner oder der Betreiber bzw. Anbieter, der die Kommunikation ermöglicht, stellt personenbezogene Daten, Kommunikationsinhalte oder Verkehrsdaten Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung, die derartige Informationen rechtmäßig anfordern. Skype wird zur Erfüllung dieser Anforderung angemessene Unterstützung und Informationen bereitstellen, und Sie stimmen hiermit einer derartigen Offenlegung zu.«

Allerdings ist über die genaue Funktion der Skype-Software relativ wenig bekannt, denn sie betreibt einen ganz erheblichen, in dieser Form sonst hauptsächlich von Schadsoftware bekannten Aufwand, um die Analyse der Software und ihrer Funktionsweise möglichst zu verhindern.[46] Insbesondere ist nicht bekannt, welche kryptographischen Algorithmen genutzt werden und wie deren Qualität einzuschätzen ist. Es erscheint auch wenig wahrscheinlich, dass sich hier Definitives wird ermitteln lassen, zumal regelmäßig neue Programmversionen erscheinen.

Allerdings verfügt die Fa. Microsoft – die die Fa. Skype im Sommer 2011 übernommen hat – seit Dezember 2009 über das oben bereits erwähnte US-Patent zum Abhören von VoIP-Gesprächen.[47] In der Kurzbeschreibung des Patents heißt es:

> »Aspects of the subject matter described herein relate to silently recording communications. In aspects, data associated with a request to establish a communication is modified to cause the communication to be established via a path that includes a recording agent.«

Mit anderen Worten hat der heutige Skype-Betreiber bereits vor einiger Zeit ein technisches Verfahren zum Abhören von VoIP-Gesprächen durch gezielte Umleitung über einen »recording agent« entwickelt. Als möglicher Anwendungszweck wird Skype in der Patentschrift ausdrücklich genannt. Auch vor diesem Hintergrund erscheint es nicht unwahrscheinlich, dass die Fa. Skype über Möglichkeiten zur effektiven TK-Überwachung verfügt.

Schließlich kann auch aus dem Vorhandensein der Funktionen Skype-In und Skype-Out in der gegenwärtigen Fassung der Skype-Software geschlossen

45 Datenschutz-Richlinie der Fa. Skype, Ziffer 3, Absatz 7; abrufbar unter http://www.skype.com/intl/de/legal/privacy/general/.

46 *Biondi / Desclaux*, Silver Needle in the Skype, http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf.

47 Vgl. oben Fußnummer 43.

werden, dass die Implementierung einer Abhörschnittstelle auch für Gespräche innerhalb des Skype-Netzes aus Sicht des Netzanbieters Skype allenfalls minimale Änderungen an der Software erfordern würde, sofern eine solche Funktion nicht bereits implementiert ist (dies ist nicht öffentlich bekannt, s.o.). Denn sowohl bei Skype-In als auch Skype-Out werden die Gespräche jeweils über eine Schnittstelle der Fa. Skype zum klassischen Telefonnetz geleitet, wo sie unverschlüsselt abgeleitet werden können. Aus technischer Sicht wäre eine Abhörschnittstelle also durch simple Kombination einer Skype-In- und einer Skype-Out-Schaltung zu erreichen, indem beide an einer Verbindung beteiligte Skype-Clients im Überwachungsfall angewiesen werden, statt einer Direkt-Verbindung eine aus dem Skype-Netz heraus gerichtete bzw. von außen kommende Verbindung aufzubauen, und diese beiden Kanäle am Skype-Out-Gateway gleichsam zusammengeschaltet werden. Hier wiederum könnte – da das Audio-Signal am Gateway zwecks Weiterleitung ins klassische Telefonnetz ohnehin unverschlüsselt anliegt – eine klassische TKÜ-Maßnahme ansetzen.

Der Sache nach wäre dies eine praktische Implementierung des sehr abstrakt gehaltenen »Microsoft-Patents« bzw. eine spezifische MITM-Attacke gegen das Skype-Netzwerk. Aufgrund dessen dezentraler Struktur|[48] würde die gezielte Steuerung der Clients im genannten Sinne zwar einen gewissen Aufwand mit sich bringen. Jedenfalls dem Netzbetreiber aber wäre dies mit größter Wahrscheinlichkeit möglich: Im Kern erfordert das Re-Routing eines Skype-Anrufs lediglich ein Spoofing des Systems des Anrufers mit der Adresse und Port-Nummer des Gateways statt der des eigentlich angerufenen Systems. Dadurch würde der Skype-Client des Anrufenden – ohne dass es dem Nutzer bewusst würde – eine verschlüsselte Verbindung zum Gateway statt (unmittelbar) zum gewünschten Zielsystem aufbauen, die sodann zum eigentlich gewünschten Zielsystem weitergeleitet würde.

Aus verfassungsrechtlicher Sicht wäre die Ausgestaltung der Skype-Software in der Weise, dass die beschriebene Funktion genutzt werden könnte, wohl unbedenklich. Insbesondere läge allein in der Ausgestaltung der serienmäßigen Skype-Software in der Weise, dass die über sie geführten Gespräche auch Gegenstand einer TKÜ sein können, noch kein Eingriff in die Integrität und Vertraulichkeit des Systems (da die Software lediglich Eingriffe in Art. 10 Abs. 1 GG ermöglichen würde) oder in das Grundrecht aus Art. 10 Abs. 1 GG

48 Eine exakte Beschreibung ist bisher nicht öffentlich geworden, vgl. aber die aufschlussreiche Analyse von *Baset/Schulzrinne*, An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, http://www.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf.

(da es sich in Bezug auf dessen Schutzbereich lediglich um eine vorbereitende Maßnahmen handeln würde, weil noch keine Kenntnisnahme stattfindet). Damit stellt sich eine solche Maßnahme als das mildere Mittel gegenüber einer Quellen-TKÜ dar. Unter Verhältnismäßigkeitsgesichtspunkten ist diese Option daher zunächst ernsthaft zu prüfen und definitiv auszuschließen, ehe ein Zielsystem infiltriert werden darf.

IV. Zum Begriff der »laufenden Kommunikation« und zur Reichweite der der Quellen-TKÜ

Für die einfachgesetzliche Ausgestaltung einer Quellen-TKÜ ist die Abgrenzung dieser verfassungsrechtlich unter wesentlich weiteren Voraussetzungen zulässigen Maßnahme von der Online-Durchsuchung wesentlich. Da das BVerfG für diese Unterscheidung das Kriterium der »laufenden Kommunikation« vorgegeben hat, soll hier untersucht werden, was unter »*laufender Kommunikation*« im Sinne der OD-Entscheidung zu verstehen ist.

Gemäß Rn. 190 der OD-Entscheidung ist

> »Art. 10 Abs. 1 GG [...] der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer »Quellen-Telekommunikationsüberwachung«, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt.«

Daraus ergibt sich, dass das BVerfG die Privilegierung der Überwachung laufender Telekommunikation durch Infiltration eines informationstechnischen Systems als eine *Schutzbereichsausnahme* vom »IT-Grundrecht« definiert hat:[49] Zwar wäre der Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme grundsätzlich eröffnet, denn »mit der Infiltration [ist] die entscheidende Hürde genommen, um das System insgesamt auszuspähen«; es sind also beide Schutzbereichsdimensionen des IT-Grundrechts bereits berührt (Rn. 188). Gleichwohl sind Eingriffe allein an Art. 10 Abs. 1 GG zu messen, wenn sie ausschließlich die Überwachung laufender Telekommunikation ermöglichen und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist (Rn. 190).[50] Daraus ergibt sich zugleich, dass die *Schutzbereiche* beider Grundrechte in diesem Fall *komplementär* angelegt sind: Sobald die engen Grenzen der »laufenden Kommunikation« überschritten sind, also der verfassungsrechtlich zulässige Anwendungsbereich der Quellen-TKÜ verlassen wird, stellt sich der Eingriff ohne weiteres als Online-Durchsuchung dar.

49 Vgl. *Bäcker* in *Uerpmann-Wittzack* (Hrsg.), Das neue Computer-Grundrecht, S. 1, 21; *Hoffmann-Riem* JZ 2008, 1009, 1022.

Das Grundrecht aus Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs,[51] sein Schutzbereich erfasst daher Zugriffe auf derart übermittelte Inhalte,[52] aber auch auf die Umstände der Kommunikation.[53] Hintergrund dieses besonderen grundrechtlichen Schutzes ist die spezifische Verletzlichkeit der Vertraulichkeit der Kommunikation, sobald Informationen unter Einschaltung eines Kommunikationsmittlers über eine Distanz hinweg ausgetauscht werden.[54] Dabei hat das BVerfG zwar auch *Zugriffe »am Endgerät«* in den Schutzbereich des Art. 10 Abs. 1 GG einbezogen.[55] Dieses Grundrecht dient aber nicht dem Schutz vor Zugriffen auf *ehemalige oder zukünftige* Kommunikationsinhalte oder Kommunikationsumstände im Machtbereich der Kommunikationspartner:[56] Sobald der Kommunikationsinhalt beim Empfänger angekommen ist, endet der Schutz des Art. 10 Abs. 1 GG.[57] In den Fällen der Infiltration des Zielsystems führt dies aufgrund des zu Art. 10 Abs. 1 GG komplementären Schutzbereichs zur Eröffnung des Schutzbereichs des »IT-Grundrechts«, sobald der unmittelbare Übertragungsvorgang beendet ist: Soll auf bereits übermittelte oder zukünftig (möglicherweise) einmal zu übermittelnde Daten zugegriffen werden, so stellt dies einen Eingriff in das IT-Grundrecht dar, der einer entsprechenden Ermächtigungsgrundlage bedürfte.

Durch diese Abgrenzung, insbesondere die Einbeziehung des Endgeräts in den Schutzbereich des Art. 10 Abs. 1 GG, wird dessen Schutz gleichsam in den Machtbereich des Kommunikationspartners hinein erweitert. Wird ein informationstechnisches System selbst als Endgerät der Telekommunikation verwendet, so sind solche Datenverarbeitungsvorgänge auch im alleinigen Machtbereich eines Kommunikationspartners vom Grundrecht aus Art. 10 Abs. 1 GG erfasst, die noch als Teil dieser Verwendung als »Telefonie-Endgerät« angesehen werden können. Dies sind jedoch allein solche technischen Vorgänge, die *unmittelbar der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen* und sich somit als integraler Bestandteil der Telekommu-

50 Vgl. vertiefend zum Hintergrund dieser Differenzierung *Hoffmann-Riem* JZ 2008, 1009, 1021 f.

51 BVerfGE 115, 166, 182; 120, 274, 306 f.; 124, 43, 54.

52 BVerfGE 115, 166, 182.

53 BVerfGE 115, 166, 183; 124, 43, 54.

54 BVerfGE 115, 166, 182 f.; *Bäcker*, Die Vertraulichkeit der Internet-Kommunikation, in: Linien der Rechtsprechung des Bundesverfassungsgerichts, Band 1 (2009), S. 99, 103.

55 BVerfGE 106, 28, 37 f.; BVerfGE 115, 166, 186 f.; vgl. hierzu *Buermeyer* RDV 2008, S. 8 f., *Hornung* CR 2008, 299, 300.

56 BVerfGE 115, 166, 183 f.; 124, 43, 54. Das BVerfG schließt auch in der OD-Entscheidung (Rn. 189) »Daten ohne Bezug zur laufenden Telekommunikation« ausdrücklich aus dem Anwendungsbereich des Art. 10 Abs. 1 GG aus, ebenso *Bäcker* (oben Fn. 54); *Hoffmann-Riem* JZ 2008, 1009, 1022.

nikation im Sinne des Grundrechts aus Art. 10 Abs. 1 GG darstellen - auch wenn die spezifische Gefährdungslage auf der Übertragungsstrecke, vor der Art. 10 Abs. 1 GG klassischerweise schützen will, hier streng genommen bereits nicht mehr zu konstatieren ist.

Bildhaft gesprochen wird durch diese Auslegung des Telekommunikationsgeheimnisses durch das BVerfG die unter dem Schutz des Grundrechts aus Art. 10 Abs. 1 GG stehende Übertragungsstrecke gleichsam in das überwachte System hinein verlängert. Dies erscheint im Bereich der TKÜ per Trojaner auch insofern plausibel, als die Quellen-TKÜ letztlich dazu führt, dass die mangels effektiver Überwachungsmöglichkeit beim Provider fehlende »Verletzlichkeit« des Übertragungsweges, die wiederum die spezifische Gefährdungslage darstellt, vor der Art. 10 Abs. 1 GG schützen will,[58] durch Infiltration des Zielsystems am Ende der Übertragungsstrecke künstlich herbeigeführt wird. Dem korrespondiert es, diese - wenn auch synthetische - Verletzlichkeit der Kommunikation wiederum unter dem Schutz des Art. 10 Abs. 1 GG zu stellen.

Grenzt man den Schutzbereich des Art. 10 Abs. 1 GG in dieser Fallgruppe mit dem BVerfG wie dargelegt ab, so ergibt sich daraus zugleich eine *Definition* des »laufenden Kommunikationsvorgangs«: Dieser umfasst Datenverarbeitungsvorgänge,

- die sich entweder im Herrschaftsbereich eines Kommunikationsmittlers abspielen (klassischer Schutzbereich des Art. 10 Abs. 1 GG) *oder*
- die sich zwar im Herrschaftsbereich eines der Kommunikationspartner abspielen, die aber unmittelbar der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen und sich somit als integraler Bestandteil der Telekommunikation im Sinne des Grundrechts aus Art. 10 Abs. 1 GG darstellen (Zugriff »am Endgerät«[59]).

Nicht umfasst sind insbesondere solche Vorgänge im Machtbereich eines Kommunikationspartners, die nicht unmittelbar der Übertragung dienen, sondern lediglich der Vorbereitung von Daten auf eine mögliche spätere Kommunikation oder der Weiterverarbeitung bereits empfangener Kommunikation. Daran gemessen darf eine Quellen-TKÜ-Maßnahme beispielsweise erfassen:

57 BVerfGE 115, 166, 183 f.; 124, 43, 54.

58 Besonders instruktiv BVerfGE 115, 166, 186: »Der spezielle Schutz des Fernmeldegeheimnisses durch Art.10 GG schafft einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entsteht, und errichtet eine besondere Hürde gegen den vergleichsweise wenig aufwendigen Zugriff auf Kommunikationsdaten, den die Nutzung der Fernmeldetechnik ermöglicht.«

59 Entwickelt in BVerfGE 115, 166, 186 f.

- die aktuell laufende Kommunikation via VoIP,
- E-Mail-Kommunikation, sofern lediglich eine Verschlüsselung auf dem Transportweg (»Transportverschlüsselung«), also etwa SMTP/TLS, IMAPS oder POP3S, umgangen wird,
- die Inhalte aufgerufener WWW-Seiten, auch wenn die Übertragung z.B. mittels HTTPS verschlüsselt ist, etwa durch Zugriff auf die Netzwerkfunktionen des Betriebssystems (nicht aber per Screenshot / »Application Shot«,[60] s.u.),
- Internet-Chat, sofern nur die Verschlüsselung auf dem Transportweg umgangen wird.

Hingegen darf auch eine Quellen-TKÜ beispielsweise *nicht* erfassen, sodass eine solche Maßnahme eine Online-Durchsuchung erfordert, die wiederum an den Voraussetzungen des IT-Grundrechts zu messen wären (ohne Anspruch auf Vollständigkeit):

- E-Mail-Kommunikation oder Internet-Chat, wenn allein oder neben einer Transportwegverschlüsselung noch eine Inhaltsverschlüsselung (etwa per PGP / GPG) vorgenommen wird, da diese Verschlüsselung gerade nicht Teil der Kommunikation, sondern eine Vorbereitungsmaßnahme für mögliche spätere Kommunikation darstellt,
- allgemein Entwürfe etwaiger späterer Kommunikation,
- Dateien, die früher Gegenstand der Telekommunikation waren oder es zukünftig ggf. einmal sein werden,
- Bildschirminhalte, da sie stets auch Informationen enthalten, die nicht Gegenstand aktuell laufender Kommunikation sind,
- in WWW-Formulare eingegebene Daten, solange nicht der Knopf zum Absenden gedrückt wurde.

Der *Ausschluss von Inhaltsverschlüsselung* aus dem Anwendungsbereich der Quellen-TKÜ ergibt sich aus der oben hergeleitete Endgeräte-Analogie. Sofern der Kommunikationspartner etwa eine E-Mail vor dem eigentlichen Absenden an den Empfänger in einem eigenen technischen Vorgang verschlüsselt, so stellt dieser Vorgang selbst noch keine Kommunikation dar, sondern einen von der eigentlichen Kommunikation losgelösten, ihr vorgelagerten Prozess zur Vorbereitung von Daten auf eine mögliche spätere Kommunikation. Der PC oder das Smartphone wird insoweit also gerade noch nicht als Telekommunikations-Endgerät, sondern allgemein als informationstechnisches System eingesetzt. Insoweit ist folglich auch nicht der Schutzbereich des Art. 10 Abs. 1 GG, sondern derjenige des IT-Grundrechts eröffnet.

60 Ein ausschnittsweises Bildschirmfoto, dass nur das Fenster der zu überwachenden Anwendung (»Application«) erfasst.

Dass sich diese Differenzierung von vorgelagerter Inhaltsverschlüsselung (dann keine Kommunikation, Zugriff nur via Online-Durchsuchung) und Transportverschlüsselung (dann Quellen-TKÜ zulässig) aus der Abgrenzung von »IT-Grundrecht« und Art. 10 Abs. 1 GG durch das BVerfG zwingend ergibt, zeigen auch folgende Kontrollüberlegungen:

Bei einer Überwachung des Briefverkehrs durch Eingriff in Art. 10 Abs. 1 GG würden zwar Briefumschläge geöffnet werden können. Hat der Absender seinen Text jedoch vor dem Versenden eigens codiert, so ist die Kenntnisnahme des Inhalts im Klartext trotz der Überwachung des Postverkehrs nicht möglich. Ebenso würde das Brechen einer *vor* einer etwaigen Transportverschlüsselung (Briefumschlag) zusätzlich eingesetzten Inhaltsverschlüsselung (Codierung des eigentlichen Briefes) gerade nicht mehr die – bei der Quellen-TKÜ ohnehin synthetisch herbeigeführte – Verletzlichkeit der Übertragungsstrecke ausnutzen, sondern hierüber noch hinaus gehen. Bildhaft formuliert entspräche dies der Überwachung des Briefschreibers am heimischen Schreibtisch beim Codieren seiner Nachricht. Dies aber wäre ganz offenkundig keine Überwachung im Sinne des Art. 10 Abs. 1 GG.

Zudem ist es technisch rein zufällig, welcher Zeitraum zwischen einer Inhaltsverschlüsselung und dem eigentlichen Kommunikationsvorgang vergeht: Der Nutzer kann eine E-Mail zunächst nur verschlüsseln, dann aber das Versenden der verschlüsselten E-Mail noch hinausschieben oder auch ganz darauf verzichten – der Vorgang des Verschlüsselns wäre in beiden Fällen mangels Übertragungsakts nicht als Telekommunikation anzusehen. Der Nutzer könnte seiner E-Mail auch eine separat verschlüsselte Datei als Anhang hinzufügen – auch hier wäre die Verschlüsselung der Datei als solche noch kein in den Schutzbereich des Art. 10 Abs. 1 GG fallender Vorgang.

Beides macht deutlich, dass eine Inhaltsverschlüsselung im Gegensatz zur Transportverschlüsselung noch kein Vorgang der Telekommunikation – umso weniger der »laufenden« Kommunikation – ist und der Rechner insofern nicht als »Endgerät« eines TK-Vorgangs eingesetzt wird.

Wollte man hingegen eine Inhaltsverschlüsselung unter Ausblendung der technischen Zwischenschritte als bereits von der Quellen-TKÜ umfasst ansehen, so bliebe zur Abgrenzung zur Online-Durchsuchung nur die Alternative, auf einen wie auch immer begrenzten zeitlichen Zusammenhang zwischen Verschlüsselung und Übermittlung abzustellen. Das wiederum brächte notwendig willkürliche Abgrenzungen mit sich: Was wäre dann - zeitlich betrachtet - noch nahe genug an der eigentlichen Kommunikation? Außerdem würde dies in einem kaum aufzulösenden Spannungsverhältnis zur BVerfG-

Vorgabe stehen, dass nur laufende Kommunikation in den Schutzbereich des Art. 10 Abs. 1 GG fällt und gerade nicht zukünftige, um die es sich bei der vorgelagerten Inhaltsverschlüsselung allenfalls handeln mag.

Vorzugswürdig erscheint daher die hier im Anschluss an das BVerfG vertretene Auffassung, an die tatbestandlich klar zu erfassenden technischen Vorgänge anzuknüpfen und darauf abzustellen, ob die *Verschlüsselung einen integralen Teil der Übertragung selbst bildet* (dann Transportverschlüsselung → laufende TK → ggf. Quellen-TKÜ möglich) oder eine *zusätzliche Maßnahme des Nutzers vor der Übertragung* darstellt (dann Inhaltsverschlüsselung → keine TK → allenfalls Online-Durchsuchung möglich). Dies lässt sich auf die klare Frage herunterbrechen, ob sich technisch zwei Vorgänge (Verschlüsselung und Übertragung) unterscheiden lassen oder nicht.

Rechtlich kann es jedenfalls nicht darauf ankommen, wie viel Zeit zwischen einer Inhaltsverschlüsselung und dem Transport vergeht: Fällt beides aufgrund einer konkreten softwaretechnischen Umsetzung zeitlich nahe zusammen, etwa weil eine Schaltfläche in einem E-Mail-Programm zunächst eine Verschlüsselung des Inhalts auslöst und die verschlüsselte Nachricht sodann zeitnah versendet wird, so kann aus grundrechtlicher Perspektive nichts anderes gelten als im Falle der Einhaltung einer »Karenzzeit« zwischen Verschlüsselung und Versand.

V. Konkrete Anwendungsfälle zulässiger und unzulässiger Erhebungen

Im Rahmen der oben im einzelnen definierten Grenzen dessen, was als laufende Telekommunikation im Sinne der OD-Entscheidung anzusehen ist, dürften die folgenden Funktionen einer Quellen-TKÜ-Software mit der Definition des BVerfG kompatibel sein:

- Ausleitung von Audio-Daten unmittelbar aus eine VoIP-Software während eines laufenden Gesprächs,
- Ausleitung von Audio-Daten an der Mikrofon- bzw. Lautsprecher-Schnittstelle, sofern technisch sichergestellt ist, dass aktuell ein Gespräch mittels einer VoIP-Software geführt wird,
- Ausleitung von E-Mails unter Zugriff auf das jeweilige E-Mail-Programm, sofern dabei lediglich eine etwaige Transportverschlüsselung umgangen wird (s.o.).

Hingegen ist beispielsweise unzulässig:

- das Anfertigen von Screenshots bzw. »Application Shots«, da dabei wohl unvermeidlich (auch) Daten erhoben werden, die nicht Gegenstand der laufenden Kommunikation sind, etwa Entwurfsstadien von E-Mails oder Lesezeichen-Leisten in WWW-Browsern,
- das Auslesen von Dateien, die später möglicherweise verschlüsselt und versandt werden sollen oder die früher per Telekommunikation übermittelt wurden,
- das Auslesen von E-Mails, bei denen neben der Transportwegverschlüsselung noch Verschlüsselungsverfahren vor dem Versand eingesetzt werden, insbesondere also PGP / GPG.

VI. Zusammenfassung[61]

Die Entscheidung des BVerfG zur teilweisen Verfassungswidrigkeit des nordrhein-westfälischen Verfassungsschutzgesetzes[62] lässt die Erhebung laufender Telekommunikation (TK) mit den Mitteln einer Online-Durchsuchung (sogenannte »Quellen-TKÜ«) unter weniger strengen Voraussetzungen zu als eine Online-Durchsuchung,[63] die über die Erhebung laufender TK hinausgeht. Allerdings gestattet diese Ausnahme vom Schutzbereich des »IT-Grundrechts«[64] nicht die Erhebung der Inhalte früherer oder potentieller späterer Kommunikation. Als Quellen-TKÜ ist daher nur die Erhebung von Inhalten aus Datenverarbeitungsvorgängen zulässig, die unmittelbar der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen und sich somit als integraler Bestandteil der Telekommunikation im Sinne des Grundrechts aus Art. 10 Abs. 1 GG darstellen (Zugriff »am Endgerät«). Nicht umfasst sind insbesondere solche Vorgänge im Machtbereich der Kommunikationspartner, die nicht unmittelbar der Übertragung dienen, sondern lediglich der Vorbereitung von Daten auf eine spätere Übertragung oder ihrer Weiterverarbeitung nach einer Übertragung dienen sollen. Typische Beispiele hierfür sind separate Ver- oder Entschlüsselungen der Inhalte vor dem eigentlichen Übertragungsvorgang, etwa unter Verwendung von PGP/GPG.

61 Fundstellen sind unter II. bei der Herleitung der hier zusammengefasst dargestellten Thesen nachgewiesen. Der Verfasser dankt *Prof. Dr. Matthias Bäcker, LL.M.* (Mannheim) für weiterführende Diskussionen des hier behandelten Themenkreises.

62 Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 -, HRRS 2008 Nr. 160.

63 Zu den Begriffen vgl. *Buermeyer* HRRS 2007, S. 154 ff. sowie *Gercke* CR 2007, 245, 246 f.

64 Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, vgl. OD-Entscheidung, Leitsatz 1.

65 *Buermeyer/Bäcker* HRRS 2009, 433.