Universität Osnabrück
Fachbereich Rechtswissenschaften
Seminar: Straftaten und Strafverfolgung unter
Nutzung informationstechnischer Systeme
Leitung: Prof. Dr. Roland Schmitz
Wintersemester 2012/2013

Seminararbeit

Erlaubt die Regelung des § 110 Abs. 3 StPO eine „Online-Durchsuchung light“?

28.02.2013

LITERATURVERZEICHNIS

Bär, Wolfgang Transnationaler Zugriff auf Computerdaten
in: ZIS online
http://www.zis-online.com/dat/artikel/2011_2_525.pdf
zitiert als *Bär,* ZIS

Durchsuchungen im EDV-Bereich
in: CR 1995, 158 und 227.
zitiert als *Bär,* CR

Handbuch zur EDV-Beweissicherung im Strafverfahren
1. Auflage
Stuttgart 2007
zitiert als *Bär,* EDV-Beweissicherung im Strafverfahren

Bode, Thomas Verdeckte strafprozessuale Ermittlungsmaßnahmen
1. Auflage
Berlin, Heidelberg 2012
zitiert als *Bode*

Borges, Georg Rechtsfragen des Phishing – Ein Überblick
in: NJW 2005, S. 3313 bis 1317
zitiert als *Borges,* NJW 2005

Buermeyer,Ulf „Die Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme
in: HRRS 4/2007, S. 154 bis 166
zitiert als *Buermeyer*, HRRS 4/2007

Buermeyer, Ulf / Bäcker, Matthias Zur Rechtswidrigkeit der Quellen - Telekommunikations-überwachung auf Grundlage des § 100 a StPO
in: HRRS 10/2009, S. 433 bis 441
zitiert als *Buermeyer/Bäcker*, HRRS 10/2009

Engländer, Armin
Examens-Repetitorium Strafprozessrecht
5. Auflage
Heidelberg 2011
zitiert als *Engländer*, Strafprozessrecht

Graf, Jürgen Peter/
Allgayer, Peter
Graf – Kommentar zur Strafprozessordnung
2. Auflage
München 2012
zitiert als Graf/*Bearbeiter*

Hannich, Rolf
Karlsruher Kommentar zur Strafprozessordnung, mit GVG, EGGVG und EMRK
6. Auflage
München, 2008
zitiert als KK/*Bearbeiter*

von Heintschel-Heinegg, Bernd /
Stöckel, Heinz (Hrsg.)
KMR– Kommentar zur Strafprozessordnung
Kleinknecht/Müller/Reitberger
Loseblattsammlung, Heidelberg
zitiert als Heintschel-Heinegg/Stöckel

Herzog, Felix
Straftaten im Internet, Computerkriminalität und die Cyber Crime Convention
http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf

Holzner, Stefan
Die Onlinedurchsuchung: Entwicklung eines neuen Grundrechts
1. Auflage
Kenzingen 2009
zitiert als *Holzner*, Die Onlinedurchsuchung

Kasiske, Peter
Neues zur Beschlagnahme von Emails beim Provider
in: StraFo 2010, Heft 6, S. 228 bis 235
zitiert als *Kasiske*, StraFO 2010

Kretschmer, Joachim
§ 160 a StPO-eine gelungene oder misslungene Gesetzgebung?
in: HRRS 12/2010, S. 551 bis 558
zitiert als *Kretschmer*, HRRS 12/2010

Kudlich, Hans
Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme –
in: GA 2011, S. 193 bis 208
zitiert als *Kudlich,* GA 2011

Leupold, Andreas /
Glossner, Silke
Münchener Anwaltshandbuch zum IT-Recht
1. Auflage
München 2008
zitiert als *Leupold/Glossner*, IT-Recht

von Mangoldt, Hermann/
Klein, Friedrich/
Starck, Christian
Kommentar zum Grundgesetz
Band 1 und 2
6. Auflage
München 2010
zitiert als Mangoldt/Klein/Starck/*Bearbeiter*

Meyer-Goßner, Lutz
Kurz Kommentar zur Strafprozessordnung
54. Auflage
München 2011
zitiert als *Meyer Goßner*

Obenhaus, Nils
Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft
in: NJW 2010, S. 651 bis 655
zitiert als *Obenhaus,* NJW 2010

Palm, Franz/
Roy, Rudolf
"Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte"
in: NJW 1996, S. 1791 bis 1797
zitiert als *Palm/Roy*, NJW 1996

Pohl, Hartmut
Zur Technik der heimlichen Online-Durchsuchung
in: DuD 31 2007, S. 684 bis 688
zitiert als *Pohl* , DuD 2007

Radtke, Henning /
Hohmann, Olaf
Kommentar zur Strafprozessordnung
München 2011
zitiert als Radtke/Hohmann/*Bearbeiter*

Roggan, Frederik
Online-Durchsuchungen
1. Auflage
Berlin 2008
zitiert als *Bearbeiter*, Online-Durchsuchungen

Sankol,Barry
Überwachung von Internettelefonie
in: CR 2008, S. 13 bis 18
zitiert als *Sankol,* CR 2008

Schlegel, Stephan
„Beschlagnahme“ von E-Mail-Verkehr beim Provider
in: HRRS, 02/2007, S. 44 bis 51
zitiert als *Schlegel,* HRRS 2007

„Online-Durchsuchung-light“ – Die Änderung des § 110 III StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung
in: HRRS, 01/2008, S. 23 bis 30
zitiert als *Schlegel*, HRRS 2008

Schröder, Burkhard/
Schröder, Claudia
Die Onlinedurchsuchung – Rechtliche Grundlagen
Technik, Medienecho
1. Auflage
Hannover 2008
zitiert als *Schröder/Schröder,* Die Onlinedurchsuchung

Wolter, Jürgen Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK
Band 2
Köln 2010
zitiert als SK/*Bearbeiter*

Für Abkürzungen wird verwiesen auf:
Kirchner, Hildebert/ Butz, Cornelie Abkürzungsverzeichnis der Rechtssprache, 5. Auflage, Berlin 2003

Online – Quellenverzeichnis

Bundesministerium des Innern – Fragenkatalog des Bundesministeriums der Jusitz
zitiert: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf

GLIEDERUNG

A. Einleitung

„Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen“.[1]

Der Alltag findet immer mehr in der virtuellen Welt, im Internet, statt. Dies geschieht zum einen zum Zwecke der Kommunikation, zum anderen erscheint aber auch die Speicherkapazität des Internets schier unerschöpflich, was die Möglichkeit der Auslagerung von Daten mit sich bringt. Die Nutzung des Internets ist nicht mehr wegzudenken und erlangt einen immer größeren Stellenwert für die Menschen, was eine Virtualisierung der Gesellschaft zur Folge hat. Aus diesem Grund ist es auch für die Strafverfolgungsorgane notwendig und sinnvoll, sich dieses System zum Zwecke der Strafverfolgung zu Nutze zu machen da sie mit den klassischen und normierten Ermittlungsmethoden an ihre Grenzen stoßen. Dies kann zum einen über die Mobilisierung von Bürgern zur Mithilfe erfolgen, wie es z.B. durch die Polizei in sozialen Netzwerken bereits umgesetzt wird, als auch über einen Zugriff in Vorgänge und Daten, die im Internet ausgetauscht oder gelagert werden, um aus ihnen beweiserhebliche Informationen zu gewinnen.

Der erste Versuch in Deutschland, eine Ermächtigungsgrundlage für die Online-Durchsuchung zu schaffen, war 2006 die Verabschiedung einer Ermächtigungsgrundlage auf Länderebene im Verfassungsschutzgesetz NRW, die das heimliche Beobachten und Aufklären des Internets sowie einen heimlichen Zugriff auf informationstechnische Systeme ermöglichen sollte.[2] Gegen das im Dezember 2006 vom NordrheinWestfälischen Landtag beschlossene Gesetz wurde bereits kurze Zeit später, am 09. Februar 2007, Verfassungsbeschwerde eingelegt.

In seinem Urteil vom 27. Februar 2008 erklärte das Bundesverfassungsgericht diese Ermächtigungsgrundlage für verfassungswidrig und formulierte

---

[1] vgl. BVerfGE 109, 279 (314); BVerfG 1 BvR 370/07 und 595/07 vom 27.02.2008, Rn. 271.

[2] § 5 Abs. 2 Nr. 11 in Verbindung mit § 7 Abs. 1, § 5 Abs. 3, § 5a Abs. 1 und § 13 VSG NRW in der Fassung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW 2006, S. 620).

darüber hinaus ein neues Grundrecht, das Grundrecht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 I i.V.m. Art. 1 I GG.

Die heimlich erfolgende Online-Durchsuchung unterliegt aufgrund ihrer hohen Eingriffsintensität einer strengen Verhältnismäßigkeitsprüfung.

Auf der einen Seite steht das Interesse der Allgemeinheit an einer effektiven Strafverfolgung auf der anderen ein Eingriff in die Grundrechte eines Bürgers. Das Grundrecht auf Gewährsleitung von Vertraulichkeit und Integrität informationstechnischer Systeme hat vor allem wie Eingangs zitiert, zum Ziel, dass das Vertrauen des Bürgers in den Staat gewährleistet werden muss. Niemand soll befürchten müssen, dass es noch einmal dazu kommt, dass er sich einem Überwachungsstaat unterwerfen muss.

Im Rahmen dieser Arbeit soll herausgestellt werden, ob ein so schwerwiegender Eingriff dennoch unter einfacheren Voraussetzungen, ohne eine Verhältnismäßigkeitsprüfung, realisierbar wäre. In diesem Zusammenhang wird der § 110 III StPO, der die Durchsicht elektronischer Speichermedien und ferner auch ihnen angeschlossene externe Speichersysteme regelt, näher betrachtet. Um einen Überblick über die verschiedenen Vorgehensweisen einer Durchsuchung zu bekommen wird zunächst die Durchsuchung i.S.d. § 110 StPO und in Abgrenzung hierzu die heimliche Online-Durchsuchung vorgestellt. Um eine Vorstellung von der hohen Eingriffsintensität der Online-Durchsuchung zu erhalten, wird im Rahmen der Auseinandersetzung mit der Frage, ob § 110 III StPO eine Grundlage für einen solchen Eingriff darstellt, auch die Verhältnismäßigkeitsprüfung des neuen Grundrechts näher betrachtet.

B. Begriffe und Arten von (Online-)Durchsuchungen

I. Regelung des § 110 III StPO

Der § 110 StPO regelt die Durchsuchung elektronischer Speichermedien und wird durch den 3. Absatz dahingehend erweitert, dass eine Durchsicht auch auf solche Speichermedien erstreckt werden kann, die räumlich von dem durchsuchten Objekt getrennt sind. Er enthält somit eine Spezialregelung für den Zugriff auf Daten in Computernetzwerken.

1. räumlich getrennte Speichermedien

Unter dem Begriff der „räumlich getrennten Speichermedien“ sind programmierbare Systeme mit Eingabe-, Ausgabe- und Speichermöglichkeit zu verstehen, die nicht unmittelbar mit dem bei dem von der Durchsuchung Betroffenen befindlichen Speichermedium verbunden sind.[3]

2. Durchsicht von Papieren

Unter den in § 110 StPO genannten Papierbegriff ist alles zu verstehen, was aufgrund seines Gedankeninhalts Bedeutung hat und auf Papier geschrieben ist.[4] Als Papier werden ferner auch solche Unterlagen bezeichnet, für die ein anderes Material verwendet wurde[5], somit sind auch elektronische Datenträger unter diesen Begriff zu subsumieren

3. Zugriff

Um gemäß § 110 III StPO auf diese räumlich getrennten Speichermedien zugreifen zu können, ist zunächst erforderlich, dass ein solcher Zugriff von dem elektronischen Gerät aus erfolgt, das sich in den Räumlichkeiten des von der Durchsuchung Betroffenen befindet. Des Weiteren muss das System des Betroffenen derart konfiguriert sein, dass allein aufgrund seiner aktuellen Konfiguration eine Erweiterung der Durchsicht auf andere, daran angeschlossene, aber unabhängige Computersysteme erfolgen kann. Demzufolge ist es nicht erforderlich, dass sich das unabhängige Computersystem im Durchsuchungsobjekt befindet, es muss lediglich auf elektronischem Wege erreichbar sein. Das Erfordernis der Körperlichkeit wurde somit aufgehoben.

4. Durchsuchung

§ 110 III StPO ergänzt die allgemeine Bestimmung des § 110 I StPO, welcher sich auf die Papiere bezieht, die bei einer Durchsuchung im Rahmen der §§ 102, 103 StPO aufgefunden werden. Insofern geht auch der Durch-

[3] *Schlegel*, HRRS 01/2008, 23 (27).
[4] *Meyer/Goßner*, § 110, Rn. 1.
[5] *Meyer/Goßner*, § 110, Rn. 2.

sicht von Speichermedien eine Durchsuchung nach §§ 102, 103 StPO voraus.[6]

a) Durchsuchungsbegriff

Der allgemeine Durchsuchungsbegriff ergibt sich aus §§ 102, 103 StPO. Hiernach wird den Ermittlungsbehörden die Befugnis zuteil, Wohnungen oder andere Räumlichkeiten von Betroffenen sowie die Dritter zu durchsuchen und gegebenenfalls die gefundenen Beweise gemäß §§ 94 ff. StPO sicherzustellen oder zu beschlagnahmen. Der Begriff der Durchsuchung beschreibt die Tätigkeit, eine Sache aufzuspüren, sie detailliert zu untersuchen und zu durchforschen, sich darum zu bemühen, etwas aufzufinden, indem ein Objekt bis zum letzten Winkel abgesucht wird.[7] Bei der Durchsuchung nach §§ 102, 103 StPO handelt es sich um Maßnahme, die auf eine offene und somit für den Betroffenen erkennbare Ausführung angelegt ist.[8]

b) Durchsuchung beim Verdächtigen gemäß § 102 StPO

Die Durchsuchung gemäß § 102 StPO darf sowohl zur Ergreifung des Verdächtigen, als auch zur Beweissicherung durchgeführt werden.[9] Hierbei sind nicht nur die Wohnung oder andere Räumlichkeiten von umfasst, sondern auch die Person des Verdächtigen und seine Sachen, für deren Durchsuchung es nicht erforderlich, dass diese im Eigentum des von der Durchsuchung Betroffenen stehen. Denn „ihm gehörend“ ist nicht Gleichbedeutend mit in seinem (Mit-) Eigentum stehend. § 102 StPO umfasst somit Besitz, Gewahrsam und Mitgewahrsam.[10]

c) Durchsuchung bei anderen Personen gemäß § 103 StPO

Die Durchsuchung gemäß § 103 StPO ist auf die Ergreifung des Beschuldigten und das Auffinden bestimmter Gegenstände und Spuren beschränkt. Zwar ist von § 103 StPO nur die Durchsuchung von Räumlichkeiten erfasst, doch wird nach h.M. auch eine Personendurchsuchung zugelassen.[11]

---

[6] *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, § 29, S. 413.
[7] Vgl. *Bär*, EDV-Beweissicherung im Strafverfahren, 2007, Rn. 361.
[8] *Engländer,* Strafprozessrecht, § 7; Rn. 146; *Schlegel*, HRRS 2008, S. 26..
[9] *Meyer/Goßner*, § 102, Rn. 12 f. .
[10] *Meyer/Goßner*, § 102, Rn. 10; BGH wistra 07, 28.
[11] *Meyer/Goßner*, § 103, Rn. 3.

5. Durchsicht von Papieren i.S.d. § 110 StPO

Die Durchsicht von Papieren stellt eine inhaltliche Kenntnisnahme dar, deren Zweck es ist, festzustellen, ob das gesichtete Material als Beweismittel in Betracht kommt.[12] Ist dies der Fall, so müssen die aufgefundenen Papiere gemäß § 98 StPO richterlich beschlagnahmt werden. Für den Fall, dass sich bei der Durchsicht herausstellt, dass sie zu keinem Ergebnis führt bzw. das aufgefundene Material nicht beweiserheblich ist, ist die Durchsicht zu beenden und das aufgefundene Material an den Betroffenen zurückzugeben.[13]
Aus § 110 III S.1 StPO geht hervor, dass die Sichtung und Sicherung von Daten der Verhinderung von Beweismittelverlusten dient. Gemäß § 110 III S. 1 StPO darf die Sichtung und eventuelle Sicherung von Daten vorgenommen werden, sofern andernfalls der Verlust dieser zu besorgen ist. Hieraus folgt, dass für eine Sichtung und eventuelle Sicherung von ausgegliederten Daten die potenzielle Gefahr Ihres Verlustes gegeben sein muss.[14]

a) zur Durchführung der Durchsicht befugter Personenkreis

In § 100 III StPO wird kein Personenkreis genannt, der zur Durchführung einer solchen Durchsicht befugt ist. Da Absatz 3 einen Sonderfall der Durchsicht von Papieren gemäß § 110 I StPO darstellt, wird vertreten, dass hier dieselben Bestimmungen gelten sollen.[15] Die Befugnis für die Durchsicht von Papieren hat in erster Linie der Staatsanwalt.[16] Diese Befugnis wurde im Rahmen des 1. JuModG und mit Blick auf eine Verfahrensbeschleunigung dahingehend erweitert, dass die Staatsanwaltschaft eine Durchsicht nunmehr auch auf ihre Ermittlungspersonen übertragen kann (§ 152 GVG).[17] Ferner ist es gemäß § 110 II StPO auch möglich, andere Beamte hinzuzuziehen. Dies erfordert allerdings eine Genehmigung des Inhabers der Beweisgegenstände. Darüber hinaus können auch Sachverständige und Dolmetscher hinzugezogen werden. Dies kommt für den Fall in Betracht, dass der Inhalt der Papiere oder Daten in einer Fremdsprache abge-

---

[12] *Meyer/Goßner*, § 110, Rn. 2.
[13] *Meyer/Goßner*, § 110 Rn. 2
[14] *Meyer/Goßner*, § 110, Rn. 7.
[15] *Schlegel*, HRRS 2008, S. 26.
[16] SK/*Wohlers*, § 102, Rn. 15.
[17] *Meyer/Goßner*, § 110, Rn. 3.

fasst oder ohne Sachkenntnisse für die Ermittlungspersonen nicht nachvollziehbar ist.[18]

b) Zwischenergebnis

Die Dursuchung gemäß § 110 III stellt eine offene Maßnahme dar, der eine Durchsuchung gemäß §§ 102, 103 StPO vorausgeht. Hieraus resultiert auch, dass der Betroffene Kenntnis von der Durchsuchung erlangt, zumal er gemäß § 106 StPO auch das Recht hat, der Durchsuchung beizuwohnen.

II. Reichweite des § 110 III StPO

Der 3. Absatz erweitert die Durchsicht auf elektronischen Speichermedien und auf hiervon getrennte Speichermedien, sofern auf diese vom Zielsystem aus zugegriffen werden kann. Demnach kann nicht davon ausgegangen werden, dass es für die Ermittlungspersonen einwandfrei erkennbar ist, ob sie mit der Ausweitung der Durchsuchung auf getrennte Speichermedien nicht eventuell in die Sphäre eine Dritten eingreifen. In diesem Fall könnte es sich für diesen so darstellen, als wäre er von einer (heimlichen) Online-Durchsuchung betroffen.

Um erörtern zu können, ob § 110 III StPO eine Ermächtigungsgrundlage für einen solchen Eingriff sein kann, muss zunächst eine Abgrenzung der o.g. Durchsuchung zu einer Online-Durchsuchung stattfinden.

1. Vorgehensweise bei einer Online-Durchsuchung

Bei der Online-Durchsuchung handelt es sich im Vergleich zur o.g. Durchsuchung nach §§ 102, 103 StPO um einen heimlichen Zugriff auf ein informationstechnisches System. Ihr Ziel ist die heimliche Erfassung von Daten eines IT-Systems, das von einer verdächtigen Person genutzt wird. Sie hat ebenso wie die Durchsuchung nach §§ 102, 103 StPO die Sichtung und gegebenenfalls die Sicherstellung von beweiserheblichen Informationen als Ziel. Für ihre Durchführung bedient man sich verschiedener technischer Verfahren, wobei zwischen einer aktiven und passiven Durchsuchung unterschieden wird.

---

[18] SK/*Wohlers,* § 110, Rn. 19.

a) aktive Online-Durchsuchung

Damit eine aktive Online-Durchsuchung stattfinden kann, ist es erforderlich, das zu durchsuchende System zuvor zu infiltrieren. Hierunter ist der Zugriff der ermittelnden Personen auf das IT-System des Betroffenen zu verstehen.[19] Dieser kann auf verschiedene Wege erfolgen.

aa) physischer Zugriff

Eine Infiltration mittels eines physischen Zugriffs erfolgt in dem die Ermittler in die Räumlichkeiten des Betroffenen eindringen, wo sich auch das zu durchsuchende Zielsystem befindet.[20] Hierbei wird entweder eine Soft- oder Hardwarekomponente auf das Zielsystem installiert, worüber zukünftig eine Datenerfassung erfolgen kann. Eine andere Möglichkeit des physischen Zugriffs ist die Image-Kopie (bitidentische Kopie) der Festplatte, deren Untersuchung dann später im forensischen Labor erfolgt.[21] Mittels der Image-Kopie ist es den Ermittlern möglich, eine auf diese Festplatte angepasste Software zu entwickeln, die mittels eines weiteren Eindringens in die Räumlichkeiten dann auf dem Zielsystem installiert werden kann, um ab diesem Zeitpunkt die Daten zu erfassen. Diese Softwarekomponenten können sowohl einen schreibenden, als auch lesenden Zugriff auf das Zielsystem haben.

bb) Zugriff über das Internet

aaa) "Zero-Day-Exploits"

Bei einer Infiltration über das Internet bedient man sich ebenfalls einer Softwarekomponente, die das Zielsystem ausspähen soll. Diese Form des Zugriffs kann auf verschiedenen Wegen erfolgen. Zum Beispiel kann eine bereits installierte Software als Einfallstor genutzt werden, wenn diese etwa Sicherheitslücken aufweist (sog. Zero-Day-Eploits[22]).[23]

---

[19] *Leupold/Glossner*, IT-Recht, Rn. 409.
[20] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 135.
[21] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 135.
[22] „Zero-Day-Exploits" sind Sicherheitslücken, die gerade erst vom Hersteller entdeckt wurden, „Less-Than-Zero-Day-Exploits" hingegen bezeichnen solche Hintertüren von denen der Hersteller selbst noch keine Kenntnis erlangt hat.

bbb) ”Less-Than-Zero-Day-Exploits”

Die Less-Than-Zero-Day-Exploits unterscheiden sich im Vergleich zu den Zero-Day-Eploits dahingehend, dass sie Sicherheitslücken eines IT-Systems ausnutzen, die dem Hersteller noch nicht bekannt sind.[24] Aufgrund dieser Unkenntnis ist der Nutzen dieser Sicherheitslücken für eine Online-Durchsuchung größer als der der Zero-Day-Eploits. Aber auch wenn noch keine Gegenmaßnahmen seitens des Herstellers und des Nutzers eingeleitet wurden, besteht dennoch die Gefahr, dass die Lücke während des Zugriffs erkannt und geschlossen wird.

ccc) “Man-in-the-middle” - Zugriff

Zum anderen besteht auch die Möglichkeit, Daten während der Übertragung über das Internet zu manipulieren. Diese in Echtzeit erfolgende Manipulation sorgt dafür, dass beim abrufenden IT-System andere Daten ankommen, als vom Zielsystem abgeschickt wurden.[25]

ddd) „Trojaner“

Eine weitere Methode, um einen Zugriff auf das Zielsystem zu erhalten bedarf der (unfreiwilligen) Mithilfe der Zielperson bzw. einer Person die an dem zu durchsuchenden Objekt tätig wird. Diese Art der Infiltration erfolgt dann z.B. über eine Email, die den Betroffenen dazu verleiten soll, eine angehängte Datei zu öffnen. In dieser befindet sich dann die für die Online-Durchsuchung erforderliche Software.

eee) „Backdoor“

Ferner gibt es Meinungen, die der Ansicht sind, dass vom Hersteller implementierte Hintertüren in einer Hard- oder Software bestehen könnten, die einen heimlichen Zugriff auf das Zielsystem ermöglichen. Diese Ansicht stellt jedoch lediglich eine Vermutung dar.[26]

---

[23] *Pohl*, DuD 2007, 684 (685).
[24] *Pohl,* DuD 2007, 684 (685).
[25] *Borges*, NJW 2005, 3313 (3314).
[26] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 136 f..

fff) Kritik

Hinsichtlich des Zugriffs über Kommunikationsnetze wird häufig angeführt, dass nicht ausgeschlossen werden kann, dass versehentlich ein anderes, als das beabsichtigte Zielsystem, implementiert wird oder/und dass aufgrund der evtl. dort befindlichen Sicherheitslücken auch schon Dritte das Zielsystem erfolgreich angegriffen haben. Somit wird die Zurechnung der gewonnenen Daten zum Nutzer des Zielsystems nicht selten in Frage gestellt.[27]

b) passive Online-Durchsuchung

Für die passive Online-Durchsuchung ist ein unmittelbarer Zugriff auf das Zielsystem nicht erforderlich. Die Durchsuchung erfolgt lediglich durch das Beobachten der auf einem IT-System ausgeführten Aktionen. Die Informationsgewinnung erfolgt über die Auswertung physischer Abstrahlungen, die von dem Zielsystem erfolgen. Hierunter fallen sowohl optische Signale, wie z.B. die Reflexion eines Monitorbildes, als auch akustische Signale, die z.B. aus der Bedienung einer Tastatur gewonnen werden können, da jede Taste einen anderen Klang hat.[28]

Ferner kann eine solche Informationsgewinnung auch über die messbare Abstrahlung von elektromagnetischen Signalen erfolgen, die von den im IT-System eingebauten Komponenten, wie z.B. der Grafik- oder Soundkarte, der Hauptplatine oder der CPU (central processing unit – deutsch: Hauptprozessor) ausgehen.[29]

Im Gegensatz zur aktiven Online-Durchsuchung, der eine Infiltration des zu durchsuchenden Systems vorausgeht, ist bei dieser Methode die Gefahr entdeckt zu werden, wesentlich geringer. Ein weiterer Vorteil der passiven Durchsuchung ist, dass die hierdurch gewonnenen Informationen sich auf Daten beschränken, die der Nutzer direkt in das Zielsystem eingibt oder abruft und somit auch ihm direkt zugeordnet werden können.

Ferner stellt diese Form der Online-Durchsuchung auch eine geeignete Vorbereitung für eine eventuell später erfolgende offene Durchsuchung mit Beschlagnahme des IT-Systems dar, da mit Hilfe der passiven Onlinedurchsu-

---

[27] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 136.
[28] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 134.
[29] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 134.

chung gewonnene Daten, wie z.B. Passwörter, einen einfacherer Zugang zu verschlüsselten Daten ermöglichen und diese dann beweisfest und ohne forensisch zu beanstandenden Methoden ausgewertet werden können.[30]

c) Zugriff auf ausgelagerte Datensysteme

Eine Online-Durchsuchung ist wie oben beschrieben nicht nur auf den Rechner des Betroffenen beschränkt sondern kann ebenso auch IT-Systeme betreffen, auf die der Betroffene von dem Zielrechner aus Zugriff hat. So läge es z.B. bei der Nutzung des „Cloud-Computing".

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. definiert das „Cloud Computing" als eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen welche in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet werden.[31] Es bietet Gleichgesinnten die Möglichkeit des einfachen Datenaustausches und stellt darüber hinaus auch eine Möglichkeit der Datenspeicherung dar. Insofern handelt es sich bei dem „Cloud-Computing" um keinen Kommunikationsvorgang sondern lediglich um die Auslagerung von Daten. Es stellt somit eine Erweiterung der in dem Rechner befindlichen Festplatte.

Die Lokalisierung der sogenannten „Cloud Systeme" bzw. ihrer Server stellt sich u.a. deswegen als besonders schwierig dar, da sie sich oftmals im Ausland befinden. Die jeweiligen Spuren, die man anhand von IP-Adressen, Top-Level-Domains und Länderkennungen verfolgt haben heute mehr Indizwirkung, als das hieraus auf den Standort des Speichersystems geschlossen werden kann.[32]

Ausgelagerte Server bringen somit neue rechtliche Fragestellungen mit sich, insbesondere ob mit der Beschlagnahme beweiserheblicher Daten aus dem Ausland eventuell ein Beweisverwertungsverbot einhergeht.

Damit ein solcher Zugriff nicht zu einer Verletzung fremder Souveränitätsrechte oder zum Unterlaufen von Rechtshilfeübereinkommen führt, bedient man sich entsprechender Regelungen. Im genaueren ergeben sich diese aus der Cyber-Crime-Konvention.

---

[30] *Hansen/Pfitzmann*, Online-Durchsuchungen, S. 134.
[31] http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf
[32] *Bär,* ZIS, 2/2011, S. 54.

aa) Cyber-Crime-Konvention

Bei der Cyber-Crime-Konvention (Convention on Cybercrime / ETS N° 185 (European Treaties Series)) handelt es sich um ein auf Initiative des Europarates zurück gehendes Abkommen (völkerrechtlichen Vertrag) im Kampf gegen die Computer- und Internetkriminalität, das neben Instrumenten zur Koordinierung der internationalen Zusammenarbeit einen Normkatalog enthält, der bestimmte Formen von Internetkriminalität zu systematisieren versucht.[33]

Diese Konvention wurde am 8. November 2001 durch das Ministerkomittee des Europarats in Budapest verabschiedet und ist am 01.07.2004 in Kraft getreten. Zu den insgesamt 46 Mitgliedsstaaten der Cyber-Crime-Convention zählen sowohl einige Länder der Europäischen Union, als auch einige nicht-europäische Staaten wie Kanada, Japan, Südafrika und die USA an.[34] Diese Konvention hat den Zweck eine gemeinsame Strafrechtspolitik mit dem Schwerpunkt des Schutzes der Gesellschaft vor Computerkriminalität zu verfolgen.[35] Hierbei findet u.a. auch die Gefahr, dass Rechnernetze und elektronische Informationen auch zur Begehung von Straftaten benutzt und Beweismaterial für Straftaten über solche Netze gespeichert und übermittelt werden können, Berücksichtigung.[36]

bb) Artikel 29 und Artikel 32 der Cyber-Crime-Konvention

Für den o.g. Fall, dass es sich bei dem ausgelagerten System um einen Server im Ausland handelt, finden die Regelungen der Art. 29 und Art. 32 der Cyber-Crime-Konvention Anwendung.[37]

aaa) Artikel 32 Cyber-Crime-Konvention

Art. 32 der Cyber-Crime-Konvention regelt den „Grenzüberscheitenden Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich sind“. Hiernach ist der Zugriff auf im Ausland (einer Vertragspar-

---

[33] *Herzog*, http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf.
[34] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?CL=GER&CM=&NT=185&DF=12/27/2006&VL=
[35] Vgl. Präambel der Konvention, http://conventions.coe.int/treaty/ger/treaties/html/185.htm
[36] Vgl. Präambel der Konvention, http://conventions.coe.int/treaty/ger/treaties/html/185.htm
[37] *Bär*, ZIS, 2/2011, S. 54.

tei der Cyber-Crime-Konvention) gespeicherten Computerdaten in zwei Fällen möglich. Entweder muss es sich gemäß Art. 32 a) um öffentlich zugängliche Computerdaten handeln oder gemäß Art. 32 b) eine rechtmäßige und freiwillige Zustimmung der Person vorliegen, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems weiterzugeben.
Sollte diese Möglichkeit nicht bestehen, so kann eine beschleunigte Sicherung ausländischer Daten nach Maßgabe des Artikels 29 Cyber-Crime-Konvention erfolgen.

bbb) Artikel 29 Cyber-Crime-Konvention

Gemäß Art. 29 Cyber-Crime-Konvention kann die beschleunigte Sicherung ausländischer Daten ohne vorheriges förmliches Ersuchen erfolgen.[38] Es ist lediglich vorerst ein Ersuchen nach den Voraussetzungen des Art. 29 II Cyber-Crime-Konvention erforderlich, bevor dann nach vorläufiger Sicherung der Daten für mindestens 60 Tage ein erneutes Ersuchen für weitere Maßnahmen an die jeweilige Vertragspartei gestellt werden muss. Für den Fall, dass der Staat des Speicherortes ein solches Ersuchen ablehnt, muss zwar von einer Verwertung der Daten abgesehen werden, aber immerhin erlaubt diese vorläufige Maßnahme eine zügige Sicherung beweisrelevanter Daten, die viel schneller und effektiver als traditionelle Rechtshandlungen ist.[39]

cc) Zwischenergebnis

Nach den Maßgaben der Artikel 29 und 30 der Cyber-Crime-Konvention ist es somit möglich auf ausgelagerte Daten im Ausland zuzugreifen.

2. Abgrenzung der (Online-)Durchsuchung zur Quellen-TKÜ und Email-Überwachung

Im Zusammenhang mit der Online-Durchsuchung wird man unter anderem auch mit dem Email-Verkehr und anderen Vorgängen konfrontiert, die durch den Gebrauch eines IT-Systems vom Nutzer getätigt werden. Auch im Rahmen der Durchsicht nach § 110 III StPO ist ein Eingriff in diese Sphäre nicht ausgeschlossen.

---

[38] *Bär,* ZIS, 2/2011, S. 55.
[39] *Bär,* ZIS, 2/2011, S. 55; Radtke/Hohmann/*Ladiges*, § 110, Rn. 19.

Hierbei handelt es sich jedoch um rechtlich und technisch anders geartete Bereiche. Um eine Abgrenzung der jeweiligen Bereiche zur Online-Durchsuchung darzustellen, ist es notwendig eine Einordnung der Email-Überwachung und der Quellen-TKÜ vorzunehmen.

a) Email – Kommunikation

Beim Kommunikationsvorgang mittels des Email-Verkehrs werden verschiedene Phasen durchlaufen. Die erste Phase stellt das Versenden der Email an den Emailprovider dar.[40] Die zweite Phase bezeichnet den Zeitraum während die Email beim Provider zwischengelagert wird und die dritte Phase beinhaltet das Abrufen der Email durch den Empfänger.[41] Einige Ansichten in der Literatur unterteilen den Email-Kommunikationsvorgang darüber hinaus auch noch in eine vierte Phase, die die Speicherung der Email beim Empfänger beinhaltet.[42]

Die Unterteilung in verschiedene Phasen ist insbesondere für die Vornahme einer Email-Beschlagnahme wichtig, da für die verschiedenen Phasen durchaus unterschiedliche rechtliche Grundlagen Anwendung finden. Die ersten beiden Phasen werden als Kommunikationsvorgänge eingestuft und fallen somit unter den Schutzbereich des Art. 10 I GG.[43] Fraglich ist allerdings auf welcher rechtlichen Grundlage ein Zugriff auf Emails erfolgen kann, die nach ihrer Kenntnisnahme durch den Empfänger beim Provider abgelegt bzw. gespeichert sind.

Die Reichweite des Schutzes durch Art. 10 GG geht über die Übermittlung der Nachricht zum Endgerät hinaus, da die von Art. 10 GG geschützte Vertraulichkeit der Kommunikation auch dann betroffen ist, wenn ein Zugriff auf das Endgerät erfolgt.[44] Ein Ende für den Kommunikationsvorgang wird aber dann angenommen, wenn der Empfänger die Nachricht erhalten hat und der Übertragungsvorgang beendet ist.[45] Begründet wird dieser Zeitpunkt damit, dass der Empfänger nach dem Empfang der Email die Möglichkeit hat, selbst zu entscheiden, ob er die Nachricht liest, speichert oder

---

[40] *Schlegel,* HRRS 2007, 44 (47).
[41] *Palm/Roy,* NJW 1996, 1791.
[42] *Schlegel,* HRRS 2007, 44 (47).
[43] *Bär,* EDV-Beweissicherung im Strafverfahren, Rn. 103.
[44] *Schlegel,* HRRS 2/2007, 44 (46); Vgl. BVerfGE 106, 28, 37.
[45] BVerfG NJW 2006, 976 (Bargatzky-Entscheidung).

löscht und somit mit der Email genauso verfahren kann, wie mit anderen Daten, die sich in seiner Privatsphäre befinden.[46] Somit fallen die gespeicherten Emails, nicht mehr in den Bereich des Kommunikationsvorgangs. Hierfür spricht auch, dass der Bereich des Telekommunikationsvorgangs insbesondere deshalb in den Schutzbereich des Art. 10 GG fällt, da die Nachricht vor Eingang beim Empfänger dem Risiko des erleichterten Zugriffs Dritter ausgesetzt ist. Eben dieses Risiko besteht nicht mehr (oder nicht mehr in dem Maße), wenn sich die Nachricht in der Sphäre des Empfängers befindet, die auch schon für den Fall angenommen werden kann, in dem der Empfänger noch keine Kenntnis von dem Empfang der Nachricht hat, aber potenziell selbst entscheiden könnte, wie er mit ihr verfährt.[47]

Eine andere Ansicht stellt darauf ab, dass der Zweck des Art. 10 GG der Schutz des Empfängers gegenüber Dritten sei und deshalb eine Abschluss des Telekommunikationsvorgangs erst dann angenommen werden könne, wenn die Nachricht nicht mehr beim Provider sondern allenfalls nur noch auf dem Endgerät des Empfängers gespeichert sei.[48] Da Angestellten eines Providers das Postfach des Nutzers regelmäßig offensteht kann der Zugriff eines Dritten nicht ausgeschlossen werden, ebenso kann nicht ausgeschlossen werden, dass der Provider im Rahmen einer Datensicherung die Emails des Nutzers abspeichert. Eine Unterteilung der Emails in solche, die noch ungeöffnet sind und somit noch nicht abgerufen wurden und solche, die schon geöffnet sind, erscheint für die Praxis undenkbar, da nicht verhindert werden kann, dass somit auch Informationen betroffen sind, die dem Fernmeldegeheimnis unterliegen, da auch bereits abgerufene Emails die Verkehrsdaten anderer ungeöffneter Nachrichten enthalten können.[49]

Insofern unterliegen auch geöffnete Emails, die beim Provider lagern, den Schutzbereich des Fernmeldegeheimnisses aus Art. 10 I GG.

Folglich können als Ermächtigungsgrundlage für den Zugriff auf beim Provider befindlichen Emails nur die §§ 100 a ff. StPO gelten.

Fraglich ist, wie es sich mit solchen Emails verhält, die der Nutzer über ein auf dem Computer installiertes Programm direkt abruft. Im Rahmen der

---

[46] *Schlegel,* HRRS 2/2007, 44 (47).
[47] Mangoldt/Klein/Starck/*Gusy,* Band I, Art. 10, Rn. 19.
[48] *Schlegel,* HRRS 2/2007, 44 (48).
[49] *Schlegel,* HRRS 2/2007 44 (49).

Durchsicht nach § 110 III StPO wird für die Fälle, in denen das Passwort gespeichert ist, und somit ein direkter Zugriff auf die Emails des Betroffenen stattfinden kann, angenommen, dass diese von der Durchsicht mit umfasst sind.[50] Auch wenn diese Nachrichten durch das Abrufen auf dem Computer des Betroffenen gespeichert werden, so wären auch jene Emails von der Durchsuchung betroffen, die noch ungelesen sind. In diesem Fall wäre es angebracht, den Versuch der Differenzierung zwischen gelesenen und ungelesenen Emails erneut vorzunehmen. Auch wenn die Ermittlungspersonen durch das vorinstallierte Email-Programm direkten Zugriff auf die Nachrichten haben, so aktualisiert sich dieses nur dann, wenn es auf dem Zielrechner geöffnet wird oder wenn ein weiterer „Button" betätigt wird. Demnach sind es die durchsuchenden Personen, die die neuen Emails beim Provider abrufen. Da es Ziel des Art. 10 GG ist, den Empfänger vor dem Zugriff Dritter – und somit auch des Staates – zu schützen, kann ein Beenden des Kommunikationsvorgangs nur dann angenommen werden, wenn der Betroffene selbst die Emails abruft. Denn dann steht es ihm auch frei, die neuen Emails zu speichern oder zu löschen, also mit diesen ebenso zu verfahren, wie mit anderen Daten auf seinem Computer. Diese Möglichkeit würde ihm durch die Ermittlungspersonen genommen werden. Anders stellt es sich dar, wenn sich bei den durch den Betroffenen abgerufenen Emails auch welche befinden, die noch ungelesen sind. Hier hatte der Nutzer die Möglichkeit der Entscheidung und hat durch das selbständige Abrufen die Nachricht auf seinem Computer gespeichert, wodurch diese wiederum in den Anwendungsbereich des § 110 III StPO fallen.

b) Quellen-TKÜ

Unter einer Quellen-TKÜ versteht das Bundesverfassungsgericht einen Vorgang, bei dem ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert wird.[51] Die Abgrenzung der Quellen-TKÜ zur Online-Durchsuchung wird damit vollzogen, dass sich

[50] SK/*Wohlers,* § 110, Rn. 10; *Schlegel,* HRRS 1/2008, 23 (28); BVerGE 124, 43, 58.
[51] *BVerfG,* Urt. v. 27.02.2008 – 1 BvR 370/07.

die Quellen-TKÜ allein auf Telekommunikationsdaten und die Onlinedurchsuchung auf alle andere Arten von Daten beschränkt.[52]

Die Aufzeichnung der Daten erfolgt direkt an der Quelle, bevor diese, wie für den Vorgang üblich, verschlüsselt an den Empfänger übermittelt werden.[53] Der technische Vorgang der Quellen-TKÜ vollzieht sich mittels einer Quellen-TKÜ-Software, die diejenigen Datenquellen auslesen soll, die vermutlich zur Telekommunikation genutzt werden.[54] Wenn man bedenkt, dass für diesen technischen Vorgang erforderlich ist, dass die Software nur anhand zusätzlicher Daten des infiltrierten Zielsystems analysieren kann, ob und wie ein Telekommunikationsvorgang gerade stattfindet[55], erscheint eine Abgrenzung zwischen Quellen-TKÜ und Onlinedurchsuchung nicht eindeutig. Des Weiteren spricht für ein Überlappen der beiden Vorgehensweisen, dass bei einer Onlinedurchsuchung immer die Möglichkeit des Zugriffs auf alle Datenquellen beim Zielsystem besteht, was auch Telekommunikationsdaten und ihre zugehörigen Verbindungsdaten nicht ausschließt. Werden im Rahmen einer Online-Durchsuchung durch die angewandte Software Bildschirmfotos angefertigt, so kann nicht ausgeschlossen werden, dass der von der Durchsuchung Betroffene seinen Bildschirminhalt mittels einer Bildschirmübertragungssoftware (z.B. während einer Skype-Konversation) mit seinem Gesprächspartner teilt. Demnach sind die Quellen-TKÜ und die Online-Durchsuchung softwaretechnisch identisch. Ferner stellt die Quellen-TKÜ eine Form der Onlinedurchsuchung dar, die sich lediglich auf einen laufenden Kommunikationsvorgang beschränken soll.

Umstritten ist ferner, auf welcher rechtlichen Grundlage eine Quellen-TKÜ möglich sein soll. Lange Zeit stand § 100a StPO als mögliche Ermächtigungsgrundlage im Fokus; dies wurde jedenfalls für den Fall verneint, wenn für eine Quellen-TKÜ die Installation einer Software auf dem Zielsystem erforderlich ist.[56] Daher scheidet § 100a StPO als rechtliche Grundlage für eine Quellen-TKÜ aus und die Möglichkeit der Quellen-TKÜ zum repressiven Zweck wäre rechtswidrig.

---

[52] Drucksache 16/6535, Antwort auf Frage 14.
[53] *Sankol,* CR 2008, 13.
[54] Bundesministerium des Innern-Fragenkatalog des Bundesministeriums der Justiz, S. 8 f..
[55] Bundesministerium des Innern-Fragenkatalog des Bundesministeriums der Justiz, S. 8 f..
[56] *Buermeyer/Bäcker*, HRRS 10/2009, S. 440.

Ihre Anwendung ist lediglich für den präventiven Zweck durch §§ 201 II, 20 k BKAG gedeckt.

c) Zwischenergebnis

In den Anwendungsbereich des § 110 III StPO fallen nur solche Emails, die vom Zielsystem aus direkt heruntergeladen werden können und zum Zeitpunkt des Zugriffs durch Ermittlungspersonen schon geöffnet sind. Ungeöffnete Nachrichten sind nur dann von der Durchsicht im Rahmen des § 110 III StPO mit umfasst, wenn diese vom Betroffenen selbst auf seinem Computer gespeichert wurden. Die beim Provider befindlichen Emails hingegen fallen in den Bereich des § 100 a StPO, da für sie der Telekommunikationsvorgang noch andauert.

3. verfassungsrechtliche Rechtfertigung der Online-Durchsuchung

Ein heimlicher Zugriff auf ein informationstechnisches System, stellt nach dem vom Bundesverfassungsgericht zu Grunde gelegten Verständnis eine technische Infiltration dar, die es – unter Ausnutzung von bestehenden Sicherheitslücken des Zielsystems oder nach Installation eines Spähprogramms – ermöglicht, die Nutzung zu überwachen, die Speichermedien durchzusehen oder das Zielsystem fernzusteuern.[57] Charakteristisch für eine Onlinedurchsuchung ist, dass diese heimlich erfolgt. Da diese staatliche Maßnahme in Grundrechte eingreift ist es erforderlich, dass die ihr zugrunde liegende Ermächtigungsgrundlage den Anforderungen der Normenbestimmtheit und Normenklarheit genügt.[58] Darüber hinaus ist es erforderlich, dass der Eingriff einer Verhältnismäßigkeitsprüfung nach den Grundsätzen der Geeignetheit, Erforderlichkeit, Verhältnismäßigkeit und des Kernbereichschutzes unterliegt.[59]

---

[57] *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07 und 595/07; *Holzner,* Die Onlinedurchsuchung: Entwicklung eines neuen Grundrechts, S.4.
[58] BVerfG 1 BvR 370/07 und 595/07.
[59] Mangoldt/Klein/Starck/*Sommermann,* Bd.2, Art. 20 III GG, Rn. 308.

a) Geeignetheit

Das Mittel ist geeignet, wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann.[60]

Im Rahmen der Geeignetheitsprüfung bezüglich einer Onlinedurchsuchung sieht es das Bundesverfassungsgericht als nicht gefordert an, dass die Maßnahme Erfolg versprechend ist.[61] Dies begründet es damit, dass nicht unterstellt werden kann, dass die mögliche Zielperson bestehende Schutzmöglichkeiten gegen einen solchen Angriff nutzt.[62] Die Geeignetheit wird schon darin gesehen, dass durch den heimlichen Zugriff auf informationstechnische Systeme „ die Möglichkeiten der Verfassungsschutzbehörde zur Aufklärung von Bedrohungslagen erweitert“ werden.[63] Bei einem so weit gefassten Begriff der Geeignetheit kann im Grunde regelmäßig von der Geeignetheit einer Onlinedurchsuchung ausgegangen werden, da die Möglichkeit der Kenntnisnahme näherer Informationen grundsätzlich nicht ausgeschlossen werden kann.

b) Erforderlichkeit

Erforderlich wäre die Online-Durchsuchung, wenn es kein milderes Mittel gäbe, dass weniger in das Grundrecht eingreift und genauso effektiv wäre.[64]
Auch hinsichtlich dieses Prüfungspunktes steht dem Gesetzgeber wieder ein weitreichender Einschätzungsspielraum zu, sodass auch die Erforderlichkeit gegeben ist.[65]

c) Verhältnismäßigkeit

Im Prüfungspunkt der Verhältnismäßigkeit muss mittels einer Gesamtabwägung das Verhältnis zwischen staatlichem Handeln und dem Grundrechtseingriff erfolgen.

Bei diesem Prüfungspunkt erfolgt insbesondere im Vergleich zu den beiden Prüfungspunkten der Geeignetheit und Erforderlichkeit eine sehr differenzierte Betrachtung. Dies resultiert daraus, dass die Datenerhebung aus in-

---

[60] BVerfGE 30, 292 (316).
[61] *Schröder/Schröder,* Die Onlinedurchsuchung, S. 114.
[62] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 220.
[63] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 221.
[64] BVerfGE 30, 292 (316).
[65] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 224.

formationstechnischen Systemen ein beträchtliches Potenzial für die Erforschung des Betroffenen aufweist und ein Eingriff in diesen Bereich eine beträchtliche Intensität hat.[66] Gerade die Benutzung solcher Systeme zur Speicherung von persönlichen Daten und sensiblen Informationen lässt schon einen Vergleich zu einem Tagebuch zu.[67] Des Weiteren ist zu berücksichtigen, dass die Erhebung solcher Daten das Vertrauen der Bürger in eine unbefangene Kommunikation stören könnte und diese sich in einen Überwachungsstaat versetzt fühlen.[68] Ferner spricht für eine genaue Abwägung, dass nicht garantiert werden könne, ob die Infiltration eines Systems nicht eventuell zur Schädigung eines solchen führen kann. Insbesondere das Prinzip der Rechtsstaatlichkeit muss dahingehend gewahrt werden, dass eine heimliche Maßnahme wie die Onlinedurchsuchung nicht die Regel wird und stets eine Ausnahme bleibt.

Die erhöhte Intensität des Eingriffs wird u.a. auch darin gesehen, dass dem Betroffenen keine Möglichkeit zusteht, sich im Wege des Rechtsschutzes gegen diese Maßnahme zu wehren.[69]

Hinsichtlich der starken Eingriffsintensität fordert das Bundesverfassungsgericht in der Abwägung der sich widersprechenden Interessen besondere materiellrechtliche Anforderungen für die Rechtfertigung einer Onlinedurchsuchung.[70] Diese liegen u.a. darin, wenn eine konkrete Gefahr für ein überragend wichtiges Rechtsgut gegeben ist.[71] Zu dem Begriff der überragend wichtigen Rechtsgüter zählen Leib, Leben und Freiheit der Person und solche Güter der Allgemeinheit, deren Bedrohung die Grundlage und den Bestand des Staates oder die Grundlage der Existenz der Menschen berühren.[72] Nach Ansicht des Bundesverfassungsgerichts ist eine Gefahr dann konkret, „wenn die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für Schutzgüter der Norm durch bestimmte Personen verursacht wird“.[73] Hinsichtlich der Interessen des von der Maßnahme Betroffenen fordert das Bundesverfassungs-

---

[66] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 230.
[67] *Schröder/Schröder*, Die Onlinedurchsuchung, S. 118.
[68] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 233.
[69] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 238.
[70] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 245 f..
[71] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 249 f..
[72] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 247.
[73] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 251.

gericht eine verfahrensrechtliche Absicherung. Diese erfolgt in Form eines Richtervorbehalts, der die eingehende Überprüfung und die schriftliche Fixierung der Entscheidungsgründe zum Inhalt hat.[74] Dies soll dem Zweck dienen, dass eine unabhängige und sachverständige Instanz dafür Sorge trägt, dass auf die Interessen des Betroffenen Rücksicht genommen wird, da er diese aufgrund der Heimlichkeit der Maßnahme nicht selbst wahrnehmen kann.[75] Einzige Ausnahme bildet die Eilregelung bei Gefahr im Verzug, welche aber nur dann zugelassen wird, wenn eine nachträgliche Überprüfung durch eine neutrale Stelle gewährleistet ist und die verfassungsrechtlichen Anforderungen für die Annahme eines Eilfalles vorliegen.[76]

d) Kernbereichsschutz

Der Kernbereichsschutz soll verhindern, dass der Mensch zum bloßen Objekt der Staatsgewalt wird.[77] Neben der Wahrung der Menschenwürde sieht dieser Schutz auch vor, dass bei der staatlichen Beobachtung ein unantastbarer Kern privater Lebensgestaltung zu wahren ist.[78] Zu diesem unantastbaren Kern zählen die Möglichkeit innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen ohne Angst davor haben zu müssen, dass staatliche Stellen dies überwachen.[79]

e) Zwischenergebnis

Die oben genannten Voraussetzungen der Verhältnismäßigkeitsprüfung zeigen insbesondere im Rahmen des Prüfungspunktes der Verhältnismäßigkeit auf, welchen hohen Anforderungen eine Onlinedurchsuchung unterliegt. Es bleibt festzuhalten, dass es nicht ohne weiteres möglich sein dürfte einen solchen Grundrechtseingriff auf andere Rechtsgrundlagen, die von ihrer Natur aus keine heimliche Maßnahme darstellen, zu übertragen.

---

[74] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 259.
[75] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 257, 259 f..
[76] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 261.
[77] *Schröder/Schröder,* Die Onlinedurchsuchung, S. 125; BVerfG 116, 279.
[78] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 118.
[79] BVerfG 1BvR 370/07; BVerfG 1 BvR 595/07, Rn. 271; BVerfG 09, 279 (314).

C. Fazit

Zusammenfassend lässt sich feststellen, dass die Online-Durchsuchung als heimliche Maßnahme keine Ermächtigungsgrundlage in den Regelungen der StPO findet. Somit lässt auch § 110 III StPO keine Online-Durchsuchung-light zu, auch wenn der Verwendung des Begriffs der „ausgelagerten Computersysteme“ diesen Schluss beim Lesen der Norm zulässt.

Zum einen hat das Vorausgehen einer Durchsuchung nach §§ 102, 103 StPO den offenen Charakter der Norm betont, zum anderen macht ein Blick auf die Verhältnismäßigkeitsprüfung, der die Durchführung einer Online-Durchsuchung unterläge, deutlich, dass der Gesetzgeber es nicht zulassen würde, eine so hohe Hürde durch andere Normen zu unterlaufen und somit das Prinzip der Rechtstaatlichkeit zu gefährden.

Nach dem geltenden Recht ist eine Online-Durchsuchung nur zum präventiven Zweck, im Rahmen der Gefahrenabwehr möglich und findet ihre Grundlage in § 20 K BKAG. Insofern kann der Bürger sein Vertrauen in die Integrität informationstechnischer Systeme fortsetzen, wenn auch dies nur im Hinblick auf staatliche Eingriffe gilt. Nicht zu unterschätzen ist dennoch die Gefahr, die von Dritten herrührt, die es aufgrund des leichtfertigen Umgangs mit sensiblen Daten im Rahmen der Internetkommunikation immer einfacher haben, dem Nutzer Schaden zuzufügen.