# [H]DIE ONLINE-DURCHSUCHUNGSMASSNAHME IN DER DEUTSCHEN RECHTSORDNUNG MIT GESETZESÄNDERUNGEN VOM 25.05.2018 UND 24.08.2017 UND DIE DURCHFÜHRBARKEIT DIESER MASSNAHME IN DER TÜRKİSCHEN RECHTSORDNUNG

***Dr. Öğr. Üyesi Çiler Damla BAYRAKTAR****

**Abstract**

*The secret infiltration of an information technology system by means of which the use of the system of a criminal can be monitored by the investigating authorities and its storage media can be read is ordered as a criminal measure in the Art. 49 Code of The Federal Criminal Police Office (BKAG) and in the Art. 100b Code of Criminal Procedure (StPO).*

*In this study these provisions are examined as the legal basis for this criminal measure and the findings in decisions of the Federal Constitutional Court (BVerfG) on the subject of the criminal measure „The secret infiltration of an information technology system" are stressed. Furthermore the seriousness and the quality of interference by this measure is determined and it is searched whether such a criminal measure is permitted in türkish legal system.*

**Keywords**

*The secret infiltration of an information technology system, the right to informational self-determination, fundamental right to the guarantee of the confidentiality and integrity of information technology systems*

---

H Hakem incelemesinden geçmiştir.

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Anabilim Dalı Öğretim Üyesi (e-posta: cilerdamla.bayraktar@asbu.edu.tr) ORCID: https://orcid.org/0000-0002-7611-5088 (Makalenin Geliş Tarihi: 09.08.2018) (Makalenin Hakemlere Gönderim Tarihleri: 16.08.2018-29.08.2018/Makale Kabul Tarihleri: 11.09.2018-31.08.2018)

# 25.5.2018 VE 24.8.2017 TARİHLİ YASA DEĞİŞİKLİKLERİYLE ALMAN HUKUKUNDAKİ ONLINE ARAMA TEDBİRİ (ONLINE-DURCHSUCHUNG) VE BU TEDBİRİN TÜRKİYE'DE UYGULANABİLİRLİĞİ


## Öz

*Soruşturma birimlerinin suçluların bilgisayar kullanımını denetlemesini ve bilgisayarda kayıtlı dosyalara ulaşılmasını sağlayan online arama tedbiri bir ceza hukuku tedbiri olarak Federal Kriminal Büro Kanunu'nun (BKAG) 49. maddesinde ve Ceza Muhakemesi Kanunu'nun (StPO) 100b maddesinde düzenlenmiştir.*

*Bu çalışmada online arama tedbirinin yasal temelini oluşturan bu hükümler ve Alman Anayasa Mahkemesi'nin (BVerG) kararlarında bu tedbire ilişkin ortaya koyduğu tespitler incelenmiştir. Ayrıca online arama tedbirindeki müdahalenin niteliği ve ağırlığı tespit edilmiş ve böyle bir ceza hukuku tedbirinin Türk hukukunda uygulanıp uygulanamayacağı hususu araştırılmıştır.*



## Anahtar Kelimeler

*Online arama, virüs göndererek bilgisayarda arama, bilgilerin kaderini belirleme hakkı, bilgi teknolojisi sistemlerinin gizliliğini ve bütünlüğünü sağlama hakkı*

Bei der Online-Durchsuchung greifen die staatlichen Behörden unbemerkt von dem potenziellen Straftäter auf die in seinem IT-System gespeicherten Daten über einen Internetzugang zu[1]. Dafür wird auf dem Rechner der Betroffenen gezielt während seiner Internet-Nutzung Software, ein sog. „Bundes-Trojaner oder Backdoor-Programme“[2], installiert[3], die dann die auf den Speichermedien des Computers abgelegten Daten und die verwendeten Programme online – also gleichfalls über das Internet – auf einen Rechner der Ermittlungsbehörde lesen, überspielen und übermitteln[4]. Auf diesem Weg können jederzeit, soweit der mit dem sog. „Bundestrojaner“ infizierte PC mit dem Internet verbunden ist, die dort gespeicherten Daten und möglicherweise verfahrensrelevante Daten und E-Mails eingesehen und zur Beweissicherung heruntergeladen werden, unabhängig davon, an welchem Ort sich der PC befindet und über welche Technik er mit dem Internet verbunden ist und ohne dass der Verdächtige hiervon erfährt[5].

---

1 BGH, Beschluss vom 31.01.2007 - StB 18/06, MMR 2007, S. 237, 237; BGH, Beschluss vom 25.11.2006 - 1 BGs 184/06, MMR 2007, S. 174, 174 ; **Conelius**, Kai, Teil 10. Besonderheiten des Straf- und Strafprozessrechts, in: Münchener Anwaltshandbuch IT-Recht, Andreas Leupold/Silke Glossner (Herausgeber), 3. Auflage, 2013, Rn. 471; vgl. auch **Obenhaus**, Nils, “Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft”, NJW, 2010, S. 651 ff.

2 „Backdoor-Programme (auch als trojanische Viren bezeichnet) sind Programme, die es einer dritten Person erlauben, einen Computer über eine TCP/IP-Verbindung zu steuern. Auf einem lokalen LAN oder über das Internet (diese benutzen TCP/IP-Verbindungen) gibt ein Backdoor-Programm seinem Benutzer die vollständige Kontrolle über einen infizierten PC“, vgl. hierzu www.kacees.de/Sicherheit_bei_der_Nutzung_desInternet_Backdoor_vh.htm (Stand vom 10.12.2017); vgl. auch **Fauß**,Patrick, „Viren-Schwemme auf einen Klick“, in: Stern, Veröffentlichung: 05.08.2007, abrufbar unter http://www.stern.de/digital/computer/drive-by-download-viren-schwemme-auf-einen-klick-594430.html (Stand vom 20.03.2018).

3 BGH, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237, 241; **Leipold**, Klaus, “Die Online-Durchsuchung”, NJW-Spezial Heft, 3/2007, S. 135; In der Diskussion über den Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA wurde die Befugnis zum „heimlichen Betreten von Wohnungen zwecks Infiltration informationstechnischer Systeme“ zwar gefordert, im Gesetzgebungsverfahren aber nicht umgesetzt, vgl. hierzu **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 139; **Roggan**, Fredrik, “Das neue BKA-Gesetz- Zur weiteren Zentralizierung der deutschen Sicherheitsarchitektur”, NJW, 2009, S. 261; **Soiné**, Michael, “Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder”, NVwZ, 2012, S. 1589 f.

4 **Kemper**, Martin, “Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten”, ZRP, 2007, S. 107; für die Deinstallation der Remote Forensic Software nach Beendigung des Eingriffs vgl. **Soiné**, Michael, “Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder”, NVwZ, 2012, S. 1589.

5 **Tinnefeld**, Marie-Theres, “Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner”, MMR, 2007, S. 139; **Hirsch**, Burkhard, “Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822,” NJOZ, 2008, S. 1909.

Hier ist zu bestimmen, dass bei einer solchen Maßnahme die Ermittlungsbeamten an die auf einem PC gespeicherten Daten über den Weg der offenen Wohnungsdurchsuchung, der Beschlagnahme des PCs und der anschließenden Datenauswertung nicht gelangen[6]. Insbesondere ist zu betonen, dass die Durchsuchung des Computers beim Beschuldigten nach § 110 III StPO von der „Online-Durchsuchung" zu unterscheiden ist.

Zwar werden die darauf abgelegten Daten von der Staatsanwaltschaft oder Polizei auch im Rahmen einer gewöhnlichen Hausdurchsuchung bzw. Beschlagnahme des PCs erlangt, aber aufgrund ihrer Heimlichkeit und der langfristigen Durchführbarkeit hat die Online-Durchsuchung als verdeckte Maßnahme den Vorteil, dass sie weiterführende, Erfolg versprechende Ermittlungsmaßnahmen ermöglicht[7].

In dieser Arbeit werden erst die gesetzliche Grundlage dieser Maßnahme in der deutschen Rechtsordnung und die Feststellungen des BVerfG zur Online-Durchsuchung dargelegt. Danach werden die Eingriffsschwere und die Qualität des Eingriffs bei der Online-Durchsuchung erwähnt und festgestellt, ob in der türkischen Rechtsordnung eine Ermächtigungsgrundlage für diese Maßnahme vorliegt, bzw. ob eine solche Ermittlungsmaßnahme nach der türkischen Rechtsordnung zulässig wäre.

## I. GESETZLICHE GRUNDLAGE DER ONLINE-DURCHSUCHUNG IN DER DEUTSCHEN RECHTSORDNUNG

### A. Im Bundeskriminalamtgesetz (BKAG)

#### 1. Die Feststellungen des BVerfG zur Präventiven Online-Durchsuchung

Wann eine heimliche Infiltration eines informationstechnischen Systems zum Zwecke der Überwachung seiner Nutzung und zur Auslesung seiner Speichermedien – also die heimliche Ausforschung der auf einem Computer gespeicherten Daten durch Sicherheitsbehörden vermittels spezieller „Spionage"-Software-zulässig ist, hat das BVerfG durch seine Online-Durchsuchung-Entscheidung vom 27.02.2008 zum VerfassungsschutzG NRW bestimmt[8].

Nach dem BVerfG darf dieser Eingriff durchgeführt werden, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr" für ein „überragend

---

6 Vgl. BGH, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237ff.

7 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 122.

8 BVerfG, Urteil vom 27.02.2008, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

wichtiges Rechtsgut“ vorliegen[9]. Bei seiner Rechtsprechung hat das Gericht zu diesen beiden Voraussetzung Folgendes erwähnt:

„*Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt*[10]*. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen. Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird*.“[11]

„*Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose*[12] *tragen. Diese Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein. “*[13]

Diese Bestimmungen weisen auf den Ausnahmecharakter des Eingriffs hin und tragen demzufolge dem Verhältnismäßigkeitsgrundsatz Rechnung.

Jedoch sind die Bestimmungen des BVerfG, die den Anwendungsbereich der Maßnahme ferner auf das Gefahrenvorfeld ausdehnen[14], in diesem Zusammenhang kritisch zu beurteilen.

Nach dem BVerfG kann der hier zu beurteilende Zugriff auf das informationstechnische System gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in

---

9 BVerfG, Urteil vom 27.02.2008, Rn. 247, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

10 **Kutscha**, Martin, “Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte”, LKV, 2008, S. 485; **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 140.

11 BVerfG, Urteil vom 27.02.2008, Rn. 247 f., abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

12 Vgl. auch **Gusy**, Christoph, “Gefahraufklärung zum Schutz der öffentlichen Sicherheit und Ordnung”, JA, 2011, S. 647.

13 BVerfG, Urteil vom 27.02.2008, Rn. 249 ff., abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

14 **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 140; **Holzner**, Stefan, „Rheinland-Pfalz: Online-Durchsuchung und weitere Maßnahmen der TK-Überwachung geplant“, MMR-Aktuell, 2010, 302767.

näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen[15], obwohl die konkrete Gefahr durch drei Kriterien – Einzelfall, zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und Bezug auf individuelle Personen als Verursacher – bestimmt wird[16].

Im Gefahrenvorfeld setzt das Gericht aber daneben Folgendes voraus: Die *„Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.“*[17]

### 2. §49 BKAG - Verdeckter Eingriff in informationstechnische Systeme

Die Entscheidung des BVerfG vom 27.02.2008[18] zum VerfassungsschutzG NRW hat klargestellt, dass eine Online-Durchsuchung nach der unter Beachtung einiger Kriterien geschaffenen gesetzlichen Ermächtigungsnorm angeordnet werden kann[19]. Dementsprechend wurde am 25.12.2008 im Bundesgesetzblatt

---

15 BVerfG, Urteil vom 27.02.2008, Rn. 251, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

16 Vgl. auch **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 140; **Soiné**, Michael, “Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder”, NVwZ, 2012, S. 1588; **Schäuble**, Wolfgang, “Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts”, ZRP, 2007, S. 213.

17 BVerfG, Urteil vom 27.02.2008, Rn. 251, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018); **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 140; BVerfG, Urteil vom 27.02.2008, Rn. 252: „Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.“ Abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

18 Für die Zusammenfassung dieses Urteils vgl. **Tepe**, Ilker, „Federal Alman Anayasa Mahkemesinin Online Araştırmalara İlişkin 28 Şubat 2008 Tarihinde Verdiği Karar“, CHD, Band: 8, 2008, S. 177 ff.

19 Demgegenüber hat Bayern mit Änderungsgesetzen vom 08.07.2008 das bayerische Polizeiaufgabengesetz (Bay GVBl 2008, 365; vgl. hierzu auch Bay LT-Drs 15/10998) sowie das Bayerische Verfassungsschutzgesetz (Bay GVBl 2008, 357; vgl. hierzu auch Bay LT-Drs 15/10999) mit Inkrafttreten ab 01.08.2008 geändert; für Informationen über die verfassungsrechtlichen Implikationen vor dem Hintergrund der Forderung nach der Schaffung einer gesetzlichen Grundlage für diese Ermittlungsmaßnahme vgl. **Warntjen**, Maximilian, “Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online- Durchsuchung”, Jura, 2006, S. 581 ff.

(BGBl I 3083) das die Voraussetzungen eines präventiven verdeckten Eingriffs durch das Bundeskriminalamt in informationstechnische Systeme nach § 20k BKAG regelnde Reformgesetz[20] verkündet und damit wurde die Online-Durchsuchung in dem § 20k BKAG in das Gesetz implementiert. Allerdings wurde die Ausgestaltung dieser Vorschrift (§20k BKAG) im Hinblick auf den Verhältnismäßigkeitsgrundsatz vom BVerfG kritisiert und wurde festgestellt, dass § 20k mit dem Grundgesetz nicht vereinbar ist.[21] Insofern wurde diese Maßnahme mit dem Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1 Juni 2017, in Kraft getreten am 25. Mai 2018, im § 49 BKAG wieder angeordnet.

Nach §49 BKAG darf das Bundeskriminalamt ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, soweit „*bestimmte Tatsachen die Annahme rechtfertigen*", dass eine Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, vorliegt[22], oder soweit bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung dieser Rechtsgüter eintritt oder das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums diese Rechtsgüter schädigen wird (§ 49 Abs. 1 BKAG).

Nach § 49 Abs. 1 Satz 3 BKAG ist die Anordnung der Online-Durchsuchungsmaßnahme möglich, wenn sie für die Aufgabenerfüllung zur Abwehr von Gefahren des internationalen Terrorismus (nach §5) erforderlich sind und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

Zuletzt darf diese Maßnahme nach dem § 49 Abs. 3 BKAG sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist, d.h. diese Maßnahme darf sich nur gegen eine Person richten, die eine Gefahr verursacht oder, wenn sie noch nicht vierzehn Jahre alt, die zur Aufsicht über sie verpflichtet ist, zudem gegen eine Person, die eine andere Person, die die Gefahr in Ausführung der Verrichtung verursacht, zu einer Verrichtung bestellt hat (§ 17 des Bundespolizeigesetzes). Zweitens darf diese Maßnahme auch gegen solche Personen angeordnet werden, die Inhaber der

---

[20] Für die Kritik, dass diese eine schwer kontrollierbare Befugniserweiterung für bestimmte Organe des Staates darstellen würde, vgl. **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 110.

[21] Für die Anforderungen des BverfG vgl. BverfG, Urteil des Ersten Senats vom 20.04. 2016, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html (Stand vom 09.08.2018).

[22] Für die detaillierten Informationen darüber vgl. **Bayraktar**, Çiler Damla, Eingriffe in die Privatsphäre durch technische Überwachung Ein deutsch-türkischer Vergleich anhand Art. 8 EMRK, Hamburg 2017, S. 521 ff.

tatsächlichen Gewalt, die Eigentümer oder andere Berechtigte sind oder die das Eigentum an der Sache aufgegeben haben, wenn die Gefahr von einem Tier oder einer Sache ausgeht (§ 18 des Bundespolizeigesetzes). Danach könnten die Besitzer und Betreiber informationstechnischer Systeme Ziel der Maßnahme sein[23].

Hier ist hervorzuheben, dass diese Bestimmungen im Hinblick auf die Vorgaben des BVerfG zu kritisieren sind, als dass der Gesetzgeber nicht unbedingt übernommen hat, was das BVerfG vorsieht. Schließlich, obwohl der Gesetzgeber die Vorgaben des BVerfG über das Gefahrenvorfeld in § 49 I BKAG übernommen hat[24], hat er die Vorgaben über den Personenkreis nicht übernommen und in § 49 Abs. 3 BKAG auf den Verhaltens- und Zustandsstörer abgestellt[25], was den Personenkreis weniger eng zieht, als es das *BverfG* tut[26], und in diesem Sinne die Verhältnismäßigkeit beeinträchtigt. Schließlich kritisieren *Baum/Schantz* dies insofern, als dass Zustandsverantwortlichkeitsfälle schwer vorstellbar sind, sodass eher der Verdacht besteht, dass hierüber die Besitzer und Betreiber informationstechnischer Systeme Ziel der Maßnahme sein könnten, die nach der Definition des BverfG Drittbetroffene wären[27].

### B. In der Strafprozessordnung (StPO)

#### 1. Die Feststellungen des BGH zur Repressiven Online-Durchsuchung

Im Jahre 2006 bestand innerhalb des Bundesgerichtshofs Uneinigkeit über die rechtssichere Anwendbarkeit von Online-Durchsuchungen. Im Februar 2006

---

23 **Baum**, Gerhart Rudolf/**Schantz**, Peter, "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 140. Insofern ist diese Vorschrift im Hinblick auf die Verhältnismäßigkeit bedenklich, als dass der Gesetzgeber hier auf den Verhaltens- und Zustandsstörer abgestellt und die Personengruppen weit begrenzt hat. Vgl. hierzu **Soiné**, Michael, "Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder", NVwZ, 2012, S. 1588 und **Baum**, Gerhart Rudolf/**Schantz**, Peter, "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 140. Für die Feststellungen von Roggan, dass die Maßnahme mangels Übersehbarkeit der konkreten Umgebung des auszuforschenden Systems das Gerät eines unbeteiligten Dritten betreffen könnte vgl. **Roggan**, Fredrik, "Das neue BKA-Gesetz- Zur weiteren Zentralizierung der deutschen Sicherheitsarchitektur", NJW, 2009, S. 262.

24 Vgl. Oben mit dem Untertitel „Die Feststellungen des BVerfG zur Präventiven Online-Durchsuchung"; vgl. hier auch **Baum**, Gerhart Rudolf/**Schantz**, Peter, "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 140; **Nazari-Khanachayi**, Arian, "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 765.

25 Vgl. hierzu **Soiné**, Michael, "Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder", NVwZ, 2012, S. 1588.

26 **Baum**, Gerhart Rudolf/**Schantz**, Peter, "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 140.

27 **Baum**, Gerhart Rudolf/**Schantz**, Peter, "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 140.

hat ein Richter am Bundesgerichtshof die Zulässigkeit der Online-Durchsuchung nach § 100a StPO (Telekommunikationsüberwachung) bejaht allerdings nur den einmaligen Zugriff auf die Mailbox – mit der Begründung, weil sich bei der Maßnahme Elemente des § 100a stopp mit solchen der Durchsuchung überschneiden würden und wegen der sachlichen Nähe zur Durchsuchung keine dauernde Überwachung der Mailbox, sondern nur ein einmaliger Zugriff auf die darin gespeicherten Daten zulässig sei – gestatten[28].

Allerdings hat ein anderer Richter am Bundesgerichtshof im November 2006 einen Antrag des Generalbundesanwalts für eine weitere Online-Durchsuchung abgelehnt: Der Generalbundesanwalt hat in Deutschland beim Ermittlungsrichter des BGH beantragt, gem. §§ 102, 105 Abs. 1, 94, 98, 169 Abs. 1 Satz 2 StPO die Durchsuchung des von dem Beschuldigten benutzten PC/Laptops, insb. der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien, und deren Beschlagnahme anzuordnen und den Ermittlungsbehörden zur verdeckten Ausführung dieser Maßnahme zu gestatten, ein hierfür konzipiertes Computerprogramm dem Beschuldigten zur Installation zuzuspielen, um die auf den Speichermedien des Computers abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen[29]. Der Ermittlungsrichter verweigert[30] die richterliche Genehmigung einer „Online-Durchsuchung“ in der deutschen Rechtsordnung mit der Begründung, dass es für diesen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung in Deutschland keine gesetzliche Grundlage gebe. Gegen diese Entscheidung hatte der Generalbundesanwalt dann eine Beschwerde eingelegt.

Der 3. Strafsenat des BGH hatte über diese Beschwerde des Generalbundesanwalts zu urteilen.

Diese klaren Beschlüsse des *Ermittlungsrichters beim BGH* zur Reichweite der strafprozessualen Ermittlungsbefugnisse wurde vom *3. Strafsenat des*

---

28 *BGH*, Beschluß vom 21.02.06 abrufbar unter https://www.jurion.de/urteile/bgh/2006-02-21/3-bgs-31_06/ (Stand vom 09.08.2018); *Hofmann* findet diese Entscheidung des *Ermittlungsrichters* des *BGH* zwar bedenklich, weil sie zwei unterschiedliche Ermittlungsmaßnahmen miteinander vermischt. Er hebt aber hervor, dass die Online-Durchsuchung in Deutschland unter den Voraussetzungen der §§ 102 (Durchsuchung bei Beschuldigten) und 103 (Durchsuchung bei anderen Personen) StPO rechtlich zulässig ist, wobei weiteres rechtliches Erfordernis ist wegen der Heimlichkeit der Maßnahme jedoch, dass als Anlasstat der Verdacht einer Straftat von erheblicher Bedeutung vorliegt und der Einsatz anderer Ermittlungsmethoden erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre vgl. hierzu: **Hofmann**, Manfred, “Die Online-Durchsuchung - staatliches „Hacken” oder zulässige Ermittlungsmaßnahme?”, NStZ, 2005, S. 125ff.

29 vgl. *BGH*, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237, 237.

30 BGH-Ermittlungsrichter, Beschluss vom 25.11.2006 – 1 BGs 184/2006, Nichtabhilfebeschluss auf die Beschwerde der Generalanwältin am 28.11.2006 (1 BGs 186/2006).

*BGH*[31] folgendermaßen bestätigt[32], als dass für die „verdeckte Online-Durchsuchung“ insbesondere nicht auf § 102 StPO (Durchsuchung bei Beschuldigten) i.V.m. § 110 StPO (Durchsuchung von Papieren, auch von elektronischen Speichermedien)gestützt werden könne, weil diese Vorschrift eine auf heimliche Ausführung angelegte Durchsuchung nicht gestattet, sowie nicht auf § 100a StPO (Telekommunikationsüberwachung) gestützt werden könne, weil es bei der Online-Durchsuchung des Computers des Beschuldigten an einer Überwachung eines Kommunikationsvorganges mit einem Dritten mangelt[33]. Durch diesen Beschluss des BGH vom 31.01.2007 ist dabei insoweit Rechtssicherheit geschaffen worden, als die geltende deutsche Strafprozessordnung einen solchen Eingriff zur Verfolgung von Straftaten nicht zulässt[34].

### 2. § 100b StPO - Online-Durchsuchung

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017, in Kraft getreten am 24.08.2017, wurde die Online-Durchsuchung in dem § 100b StPO in das Gesetz implementiert, bzw. im Ermittlungsverfahren die „Online-Durchsuchung“ eingeführt.

Nach dem § 100b StPO darf ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung). Nach dieser Vorschrift ist die Anordnung einer Online-Durchsuchung nur möglich, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in dem Straftatenkatalog aufgezählte besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat, die Tat auch im Einzelfall besonders schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre (100b StPO Abs.1).

Die Katalogstraftaten, die der Gesetzgeber für die Anordnung der „Online-Durchsuchung“ voraussetzt, sind im § 100b Abs. 2 aufgezählt. Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des

---

31 BGH StB 18/06 – Beschluss vom 31.01.2007, abrufbar unter http://www.hrr-strafrecht.de/hrr/3/06/stb-18-06.php (Stand vom 09.08.2018).

32 Vgl. hierzu **Tinnefeld**, Marie-Theres, “Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner”, MMR, 2007, S. 139, vgl. hierzu auch **Ihlenfeld**, Jens, „BGH: Verdeckte Online-Durchsuchung unzulässig“, in: golem.de, Veröffentlichung: 05.02.2007, abrufbar unter http://www.golem.de/0702/50334.html (Stand vom 09.08.2018).

33 **Kemper**, Martin, “Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten”, ZRP, 2007, S. 108.

34 **Kemper**, Martin, “Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten”, ZRP, 2007, S. 106.

Landesverrats und der Gefährdung der äußeren Sicherheit, Bildung krimineller Vereinigungen und terroristischer Vereinigungen, Geld- und Wertzeichenfälschung, Mord und Totschlag sind dazuzuzählen.

Nach dem §100b Abs. 3 darf diese Maßnahme sich nur gegen den Beschuldigten richten. Allerdings ist ein Eingriff in informationstechnische Systeme anderer Personen zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte informationstechnische Systeme der anderen Person benutzt, und die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird. Zudem darf diese Maßnahme auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

## II. DIE EINGRIFFSSCHWERE UND DIE QUALITÄT DES EINGRIFFS BEI DER ONLINE-DURCHSUCHUNG

### A. Eingriffsschwere

Zwar ist die Effizienz dieses Mittels bei Schwerkriminalität und Terrorismus dadurch bedenklich, dass „Online-Durchsuchungen" nur bei solchen Computernutzern einen Erfolg verspricht, die auf den Schutz ihrer Festplatte vor privaten oder staatlichen „Hackern" vertrauen und ihre Daten nicht „verstecken", was aber dem gemeingefährlichen Straftäter nicht entspricht, weil bei diesem Fall der Straftäter mit der heimlichen Ausforschung seines Computers rechnet und die ermittlungsrelevanten Daten verschlüsselt oder verschließet, oder einfach auf einen externen Speicher wie Diskette oder Stick übertragt, der nur durch die klassische Durchsuchung der Wohnung aufgefunden werden kann[35]. Aber mit der Weiterentwicklung der Technologie werden immer mehr Daten elektronisch gespeichert und übermittelt. Insofern ist es denkbar, dass die heimliche „Online-Durchsuchung" durch Polizei und Nachrichtendienste zum Ermittlungsinstrument der Zukunft wird[36], besonders angesichts des Offenheitsmissgriffs der „klassischen Durchsuchung der Wohnung", wonach der Betroffene erfährt, dass gegen ihn ermittelt wird, und deswegen möglicherweise andere Ermittlungsansätze „endgültig verschüttet" werden[37].

---

35 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1172 f.

36 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1170; auf der anderen Seite, bei der Abwägung der Maßnahmen im Hinblick auf deren Rolle in der Praxis der Sicherheitsbehörden, vgl. **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 487, und **Kutscha**, Martin, "Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung - nichts Neues aus Karlsruhe?", NJW, 2005, S. 23.

37 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1172.

Jedoch hat diese Maßnahme gravierende Auswirkungen.

Angesichts dessen, dass jeder Bürger, der im Besitz eines Computers mit Internetanschluss ist, zumindest theoretisch von solchen Überwachungen betroffen sein kann[38], und dass der privat genutzte PC heute so etwas wie ein „ausgelagertes Gehirn“[39] ist, tritt durch die Anwendung dieser Maßnahme die Gefahr auf, dass sich der Staat durch einen einzigen Zugriff auf einen Rechner ein nahezu komplettes Bild über einen Bürger verschaffen kann[40].

Besonders wenn eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht, sind Umfang und Vielfältigkeit des Datenbestands, der durch einen derartigen Zugriff erlangt werden kann, noch erheblich größer als bei einer einmaligen und punktuellen Datenerhebung, wobei das Gewicht des Grundrechtseingriffs von besonderer Schwere ist[41].

Durch den sinkenden Preis der technologischen Produkte ist es einfacher geworden, über solche Geräte zu verfügen bzw. sie in Gebrauch zu nehmen, wie bspw. Computer, die bei vielen Menschen längst die Rolle des klassischen Aktenordners eingenommen haben, weil sie dem jeweils berechtigten Nutzer ein hohes Speichervolumen zur Verfügung stellen und es dadurch ermöglichen, persönliche Aufzeichnungen, private Film- oder Tondokumente, Schriftstücke und zahlreiche sensible Daten, zum Beispiel über die Behandlung von Krankheiten, persönliche Finanzen oder das Sexualleben, aber auch digitale Fotos etc. aufzubewahren[42]. Bei der Online-Durchsuchung kommt so ein schwerer Eingriff in Betracht, da ein umfassendes Persönlichkeitsprofil erstellt werden kann[43].

---

38 **Kemper**, Martin, “Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten”, ZRP, 2007, S. 106.

39 **Tinnefeld**, Marie-Theres, “Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner”, MMR, 2007, S. 137 f.; **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 139.

40 **Baum**, Gerhart Rudolf/**Schantz**, Peter, “Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik”, ZRP, 2008, S. 139.

41 BVerfG, Urteil vom 27.02.2008, Rn. 234 f., abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

42 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171; BVerfG, Urteil vom 27.02.2008, Rn. 272, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

43 BVerfG, Urteil vom 27.02.2008, NJW 2008, S. 830, Rn. 231 f.; BGH: Online-Durchsuchung eines Computers, MMR 2007, S. 237, 239: „[…] die in den Speichermedien eines Computers abgelegten Daten im Einzelfall ähnlich sensibel und schutzwürdig sein können wie das in einer Wohnung nichtöffentlich gesprochene Wort und dass die Maßnahme wegen der Durchsicht einer Vielzahl unterschiedlicher Daten als ein besonders schwerwiegender Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung erscheinen

Auf der anderen Seite ist folgende Ausführung zu beachten, die im Rahmen der Online-Durchsuchung häufig angeführt wird: „wenn sich ein Nutzer derartig im Internet bewegt und er dann auch noch einen ‚ungeschützten' Computer hat, dann kann der Computerbenutzer durch seine Teilnahme am Internet-Verkehr sein System selbst öffnen bzw. konkludent seine Daten dem allgemeinen Zugriff über das Netz preisgeben; dabei nimmt er die Gefahren einer Infizierung seines Computers in Kauf"[44] und muss *„sich fast so behandeln lassen, als würde er seine Daten freiwillig herausgeben"*[45]. Daraus ließe sich das Fazit ziehen, dass der Eingriff der Online-Durchsuchung nicht so schwer wiegt. Aber wie bereits dargelegt wurde, sollte man hier den Willen der Betroffenen nicht übersehen. Die mittels ihres Computers mit der Außenwelt verbundene und dadurch E-Mails verschickende oder im Internet surfende Person möchte keineswegs ihre auf der Festplatte gespeicherten höchstpersönlichen Informationen dem Zugriff anderer preisgeben, und daneben hebt sie durch die Installation von Sicherheitsmaßnahmen, eben sogenannter Anti-Viren- und Firewall-Programme, hervor, dass sie von „Hacker"-Angriffen verschont zu bleiben hofft[46].

Außerdem wird hier zwar auch durch einen Vergleich zwischen der klassischen Durchsuchung und der Online-Durchsuchung behauptet, dass die Schwere des Eingriffs der Online-Durchsuchung nicht überschätzt werden darf[47]. Die insofern geprüfte Eingriffsschwereabwägung zwischen diesen Eingriffen führt uns aber zu der Folgerung, dass die Eingriffsschwere der Online-Durchsuchung folgendermaßen intensiver ist als die der klassischen Durchsuchung.

Wenn man tatsächlich den heimlichen Charakter der Online-Durchsuchung nicht berücksichtigt, könnte zu Recht behauptet werden, dass die Online-

---

mag"; **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171; **Tinnefeld**, Marie-Theres, "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 138; *Kemper* weist insofern darauf hin, dass das Gesetz bei der Durchsuchung von EDV-Anlagen keinen anderen Maßstab anlegt als etwa bei der Durchsuchung eines Schreibtischs oder einer Lagerhalle. Insofern stellt er infrage, ob nicht das allgemeine rechtliche Instrumentarium zur Durchsuchung von EDV-Anlagen einer Überarbeitung bedarf, vgl. **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 106.

44 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125.

45 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 110; **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171.

46 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171; **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125.

47 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125.

Durchsuchung gegenüber der klassischen Durchsuchung sogar die mildere Maßnahme darstellt, weil erstens dabei nicht die gesamte Wohnung des Betroffenen, sondern lediglich die Festplatte des Computers durchsucht wird[48], und zweitens weil während der klassischen Durchsuchung *regelmäßig* die Beschlagnahme und Mitnahme sämtlicher Datenträger erfolgt und dies zur Folge hat, dass der Betroffene diese Anlage für eine teilweise erhebliche Zeit nicht mehr nutzen kann[49], anders als wenn die Daten im Rahmen der Online-Durchsuchung nur kopiert werden, sodass der Betroffene sein elektronisches Datenverarbeitung-System ohne Beschränkungen weiter nutzen kann[50].

*Rux* hebt hervor, dass, ungeachtet auf welche Weise ein Zugriff erfolgt, es keinen Unterschied mache, ob mittels einer Online-Durchsuchung die auf einem privaten Rechner gespeicherten Daten erfasst werden sollen oder durch eine konventionelle Wohnungsdurchsuchung, bei welcher die auf der Computerfestplatte befindlichen Daten beschlagnahmt werden, weil die Belastungen des Betroffenen gleich sind[51].

Auf der anderen Seite ist zu akzeptieren, dass solche Maßnahmen wegen ihrer Verdecktheit gegenüber der offenen Durchsuchung der Räume nach § 102 StPO gravierendere und „intensivere" Grundrechtseingriffe in die Rechte des davon Betroffenen darstellen[52], wie der BGH richtig bemerkt[53], obwohl die klassische Durchsuchung als der schwerste Eingriff in das Wohnungsgrundrecht eingreift, während die Online-Durchsuchung darin keinen Eingriff darstellt[54].

### B. Die Qualität des Eingriffs bei der Online-Durchsuchung

#### 1. Überlegung im Rahmen des Wohnungsgrundrechts

Die Frage, ob diese Maßnahme das Grundrecht aus Art. 13 GG berührt, ist umstritten und sehr wichtig bei der Gewichtung der Eingriffsschwere, weil dieses Grundrecht vergleichsweise so viel schwerer wiegt als andere. Während

---

48 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125.

49 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125; **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 109.

50 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 109; für die Beschlagnahmefähigkeit von Daten, vgl. dort S. 108-109.

51 **Rux**, Johannes, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsgrundlagen der ‚Online-Durchsuchung'", Juristen-Zeitung, 2007, S. 292.

52 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 108; **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1172.

53 *BGH*, NJW 2007, S. 930.

54 Vgl. Unten mit dem Untertitel „Überlegung im Rahmen des Wohnungsgrundrechts".

das Recht auf informationelle Selbstbestimmung nach der Rechtsprechung des BverfG lediglich einem Gesetzesvorbehalt untersteht, statuiert Art. 13 GG in Absätzen 3 ff. bestimmte Voraussetzungen sowohl materiell-rechtlicher als auch verfahrensrechtlicher Art (Richtervorbehalt)[55] für die Überwachung von Wohnungen und errichtet damit eine wesentlich höhere Hürde für Eingriffe in dieses Grundrecht[56], was auch die schwere Gewichtung des Grundrechts widerspiegelt.

Es ist bei dieser Abwägung zuerst festzustellen, ob die Berührung dieses Grundrechtes nur bei dem Eingriff in Betracht kommt, der durch die Betretung einer Wohnung stattfindet, nämlich, ob unmittelbar festgelegt werden kann, dass die Online-Durchsuchungsmaßnahme eventuell gar nicht in Art. 13 GG eingreift, weil dabei der Raum, in welchem sich der Computer befindet, weder betreten, noch besichtigt oder akustisch überwacht wird[57].

Das BVerfG hat bei seiner Entscheidung zum Großen Lauschangriff[58] durch die Feststellung über den Schutzbereich des Grundrechts das Grundrecht auf Grund moderner Ermittlungsmaßnahmen durch die sich an dem sachlichen Schutzbereich des Grundrechts orientierenden Interpretation fortschrittsgewandt ausgelegt[59]. Anwendung findet diese Methodik auch bei der Feststellung, ob die Online-Durchsuchung in Art 13 GG eingreift: Das BVerfG hat in seinem Urteil vom 03.03.2004 zum sogenannten Lauschangriff den Schutzgehalt des Art. 13 GG im Lichte der fortschreitenden technischen Entwicklung offener ausgestaltet[60] und betont, dass das Grundrecht der Unverletzlichkeit der Wohnung seine Schutzwirkung unter den heutigen Bedingungen nicht nur gegenüber körperlicher Ingerenz entfaltet. Danach „diente das Grundrecht des Art. 13 I GG primär dem Schutz des Wohnungsinhabers vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt. Seitdem sind neue Möglichkeiten für Gefährdungen des Grundrechts hinzugekommen. […] Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer

---

55 Vgl. hierzu: **Gusy**, Christoph, "Überwachung der Telekommunikation unter Richtervorbehalt Effektiver Grundrechtsschutz oder Alibi?", ZRP, 2003, S. 276 f.

56 Vgl. hierzu **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1170.

57 BGH, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237, 241.

58 BVerfG, Urteil vom 03.03.2004, abrufbar unter https://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898 (Stand vom 09.08.2018).

59 Vgl. hierzu **Werkmeister**, Christoph/**Pötters**, Stephan, "Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen"", JuS, 2012, S. 227; vgl. hierzu **Möllers**, Christoph, "Wandel der Grundrechtsjudikatur Eine Analyse der Rechtsprechung des Ersten Senats des BVerfG", NJW, 2005, S. 1974.

60 **Buermeyer,** Ulf, „Die „Online-Durchsuchung" Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS, 8/2007, S. 332, abrufbar unter http://www.hrr-strafrecht.de/hrr/archiv/07-08/index.php?sz=7, (Stand vom 09.08.2018).

Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre."[61]

In diesem Zusammenhang ist darauf hinzuweisen, dass nach dieser Entscheidung des BVerfG bei diesem Grundrecht nicht nur das körperliche Eindringen in die Wohnung, sondern auch die Entscheidungsbefugnis des Einzelnen darüber geschützt wird, welche Informationen aus dem Bereich seiner „Wohnung" der Betroffene Dritten zugänglich machen will[62]. Behauptet wird, dass die die Wohnung unangetastet lassende Online-Durchsuchung in Art 13 GG eingreift[63], weil durch die Online-Durchsuchung die im Einklang mit der Entscheidung des BVerfG räumlich geschützte Privatsphäre „nach außen" vermittels moderner Technik ohne Wissen des Betroffenen geöffnet wird[64].

Dass durch eine Online-Überwachung – im Gegensatz zum Großen Lauschangriff – nicht aber der gesamte räumliche Schutzbereich der Wohnung und damit auch nicht der gesamte Rückzugsbereich des Einzelnen negiert werde, bedeutet nicht, dass durch diese Maßnahme das Wohnungsgrundrecht aus Art. 13 GG nicht berührt wird, weil auch durch eine optische Überwachung gezielt nur der Schreibtisch überwacht wird, wenn nur dieser Gegenstand in der Wohnung Relevanz für die Ermittlungsbeamten hat; auch dadurch wird jedoch das Wohnungsgrundrecht beeinträchtigt – zwischen den Fällen macht eine Betroffenheit körperlicher Gegenstände keinen Unterschied[65].

---

61 BVerfG, Urteil vom 03.03.2004, Rn.105, abrufbar unter https://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898 (Stand vom 09.08.2018); **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171; dazu im Einzelnen **Denninger**, Erhard, "Verfassungsrechtliche Grenzen des Lauschens - Der „große Lauschangriff" auf dem Prüfstand der Verfassung", ZRP, 2004, S. 101; **Gusy**, Christoph, "Lauschangriff und Grundgesetz", JuS, 2004, S. 457; **Werkmeister**, Christoph/**Pötters**, Stephan, "Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen"", JuS, 2012, S. 227; **Nazari-Khanachayi**, Arian, "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 763; **Kudlich,** Hans, „Zur Zulässigkeit strafprozessualer Online-Durchsuchungen", HFR, 2007, S. 206, abrufbar unter http://www.humboldt-forum-recht.de/deutsch/19-2007/beitrag.html (Stand vom 09.08.2018).

62 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171.

63 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171; **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 122.

64 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171.

65 **Buermeyer,** Ulf, „Die „Online-Durchsuchung" Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS, 8/2007, S. 333, abrufbar unter http://www.hrr-strafrecht.de/hrr/archiv/07-08/index.php?sz=7 (Stand vom 09.08.2018).

Auf der anderen Seite spricht es auch für einen Eingriff in das Wohnungsgrundrecht, dass durch diese Maßnahme eine Vielzahl von den sich im räumlichen Bereich einer Wohnung bzw. eines Geschäftsraums befindlichen Daten auf der Festplatte des betroffenen Computers ausgeforscht werden[66], besonders wenn man darauf Rücksicht nimmt, dass durch die ersatzweise Benutzung von Computern gegenüber des klassischen Aktenordners zahlreiche sensitive Daten – zum Beispiel über die Behandlung von Krankheiten, über die persönlichen Finanzen oder das Sexualleben, aber auch digitale Fotos etc. wegen des großen Speichervolumens der Festplatten und seines nur dem jeweils berechtigten Nutzer zur Verfügung stehenden Charakters – in PCs aufbewahrt werden[67].

Dagegen wird hier übersehen, dass erstens durch die Online-Durchsuchung gerade nicht in die durch räumliche Abschottung begründete private Lebenssphäre des Betroffenen eingedrungen wird, weil vielmehr für den Eingriff und seine Auswirkungen auf den Betroffenen der Standort des zu durchsuchenden Computers gleichgültig ist[68], wie sich etwa beim Zugriff auf ein außerhalb einer Wohnung befindliches Notebook zeigt, was aber für die Tangierung in dieses Grundrecht durch den von außen eingesetzten Einsatz technischer Mittel im Sinne des Merkmals „Überwachung von innerhalb der Wohnung stattfindenden Vorgängen“ wie etwa bei der akustischen oder optischen Wohnraumüberwachung als mangelhaft gesehen werden soll[69].

Zweitens würde zwar ein staatlicher Fernzugriff auf die gespeicherten Daten eines Rechners zugleich in den Schutzbereich des Grundrechts eingreifen, soweit er sich innerhalb einer Wohnung im Sinne des Art. 13 Abs. 1 GG befindet[70], es ist aber nicht möglich, genau festzustellen, wo der PC sich befindet.

---

66 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171; **Werkmeister**, Christoph/**Pötters**, Stephan, “Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen“”, JuS, 2012, S. 227.

67 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171 f.

68 Vgl. hierzu **Martini**, Mario, “Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts”, JA, 2009, S. 841; **Eifert**, Martin, “Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen”, NVwZ , 2008, S. 522; **Kemper**, Martin, “Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten”, ZRP, 2007, S. 107; vgl. hierzu **Werkmeister**, Christoph/**Pötters**, Stephan, “Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen“”, JuS, 2012, S. 229; vgl. Sie auch: **Nazari-Khanachayi**, Arian, “Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen”, JA, 2010, S. 763.

69 **Hofmann**, Manfred, “Die Online-Durchsuchung - staatliches „Hacken” oder zulässige Ermittlungsmaßnahme?”, NStZ, 2005, S. 125

70 **Buermeyer,** Ulf, „Die „Online-Durchsuchung“ Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme“, HRRS, 8/2007, s. 332 f., abrufbar

Tatsächlich ist die Online-Durchsuchung prinzipiell auch dann möglich, wenn der Computer zwar mit dem Internet verbunden ist[71], allerdings ist es nicht erforderlich, dass der Computer in einer Wohnung steht[72], was aber hinsichtlich der Eingriffsfeststellung in Art. 13 GG vorausgesetzt wird.

Gegenüber dieser Frage, woher der Ermittlungsbeamte wissen könne, ob sich der Rechner in Wohnräumen befindet[73], wird dargelegt, dass bis zur Feststellung, dass sich der Rechner nachweislich außerhalb der Wohnung befindet, angenommen wird, dass der PC in einer Wohnung steht; danach handelnde staatliche Behörde haben dabei jedoch die bestehenden verfassungsrechtlichen oder einfachgesetzlichen Eingriffsvoraussetzungen einzuhalten, da sie bei ihrem Handeln nicht genau wissen, ob sie in ein bestimmtes Grundrecht eingreifen[74]. Eine gegensätzliche Einstellung würde dazu führen, dass der Grundrechtschutz der großen Mehrheit der Bürger, die ihren Computer weiterhin innerhalb der Wohnung nutzen und diesem Umfeld eine entsprechend hohe Vertraulichkeitserwartung entgegenbringen, wegen der zunehmenden Mobilität von PCs verkürzt wird[75].

Zwar führt die Argumentation zu einer stückweiten Klärung im Rahmen des Feststellungsproblems, es stellt jedoch immer noch ein Problem dar, dass „durch die Online-Durchsuchung gerade nicht in die durch räumliche Abschottung begründete private Lebenssphäre des Betroffenen eingedrungen

---

unter http://www.hrr-strafrecht.de/hrr/archiv/07-08/index.php?sz=7, (Stand vom 09.08.2018); **Hirsch**, Burkhard, "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822," NJOZ, 2008, S. 1913.

71 **Tinnefeld**, Marie-Theres, "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 139.

72 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107.

73 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107; *Kemper* hebt erstens hervor, dass das Internet nicht an den deutschen Staatsgrenzen endet und das völkerrechtliche Territorialprinzip selbstständige Ermittlungshandlungen im Ausland durch deutsche Beamte schlicht nicht zulässt. Dann weist er auf den Fall hin, wenn die Beamten gar nicht wissen, wo der Rechner eingeloggt ist, vgl. hierzu **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107.

74 **Kudlich,** Hans, „Zur Zulässigkeit strafprozessualer Online-Durchsuchungen", HFR, 2007, S. 207, abrufbar unter http://www.humboldt-forum-recht.de/deutsch/19-2007/beitrag.html (Stand vom 09.08.2018); **Sachs**, Michael/**Krings**, Thomas, "Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"", JuS, 2008, S. 484.

75 **Buermeyer,** Ulf, „Die „Online-Durchsuchung" Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS, 8/2007, S. 333, abrufbar unter http://www.hrr-strafrecht.de/hrr/archiv/07-08/index.php?sz=7 (Stand vom 09.08.2018); **Schantz**, Peter, "Verfassungsrechtliche Probleme von „Online-Durchsuchungen"", KritV, 2007, S. 317; **Thiel**, Markus, Die „Entgrenzung" der Gefahrenabwehr, Tübingen, 2011, S. 292.

wird“, was sowohl beim Vergleich der Online-Durchsuchung und des Großen Lauschangriffs als auch bei der vergleichsweisen Übertragung der Feststellungen des BVerfG in der Entscheidung zum Großen Lauschangriff auf die Online-Durchsuchung maßgebend ist.

Außerdem spricht diese Kritik insoweit gegen den Eingriff in das Wohnungsgrundrecht durch die Online-Durchsuchung, als dass man, soweit man „online gehe“, auf den Schutz des Wohnungsgrundrechtes nicht länger vertrauen könne, weil durch seine Teilnahme am Internet-Verkehr der hiervon betroffene Computerbenutzer sein System selbst öffne[76]. Dagegen lässt sich zurecht darlegen, dass der PC-Benutzer durch die Installation von Sicherheitsmaßnahmen (Firewall[77], Virenschutz, Installation von aktuellen Sicherheitsupdates) einen Zugriff auf höchstpersönliche Informationen durch Dritte zu verhindern versucht[78] und das „Ausspähen von Daten“, die gegen unberechtigten Zugang besonders gesichert sind, gem. § 202a StGB unter Freiheitsstrafe bis zu 3 Jahren gestellt ist[79].

Vielmehr lässt sich anführen, dass der PC-Benutzer, der sich beim Surfen im Internet mit Sicherheitsmaßnahmen zu schützen sucht, im gleichen Maße mit einem Zugriff auf höchstpersönliche Daten rechnet, wie der Mensch, der vor dem Schlafengehen seine Tür abschließt, um einen Diebstahl zu verhindern. Wird die Tür nicht abgeschlossen, so verwirkt der Hausherr seine Rechte ebensowenig wie der PC-Benutzer, der ohne Sicherheitsmaßnahmen surft. Er verzichtet hier nicht auf seine Rechte.

Allerdings bedeutet dies nicht, dass durch die Online-Durchsuchung ein Eingriff in das Wohnungsgrundrecht stattfindet, obwohl durch die Online-Durchsuchung (im Einklang mit der Entscheidung des BVerfG[80]) die räumlich geschützte Privatsphäre „nach außen“ vermittels moderner Technik ohne Wissen des Betroffenen angeblich geöffnet wird. Bemerkenswert ist in diesem Zusammenhang auch die Bestimmung des BVerfG, dass der *„Schutzzweck der*

---

76 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171.

77 Eine Firewall ist Software oder Hardware, die die aus dem Internet oder einem Netzwerk eingehenden Daten überprüft und diese dann je nach den gewählten Einstellungen blockiert oder zum Computer gelangen lässt, vgl. hierzu https://www.teialehrbuch.de/Kostenlose-Kurse/Einblick-in-Windows-7/4.7.4-Beispiel-158-Status-der-Firewall-pr%C3%BCfen.html (Stand vom 09.08.2018).

78 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171.

79 **Kutscha**, Martin, “Verdeckte “Online –Durchsuchung” und Unverletzlichkeit der Wohnung”, NJW, 2007, S. 1171; **Hofmann**, Manfred, “Die Online-Durchsuchung - staatliches „Hacken” oder zulässige Ermittlungsmaßnahme?”, NStZ, 2005, S. 126.

80 Vgl. BVerfG, Urteil vom 03.03.2004, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/03/rs20040303_1bvr237898.html (Stand vom 09.08.2018).

*Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre"*; kritisiert wird jedoch, dass „durch die Online-Durchsuchung gerade nicht in die durch räumliche Abschottung begründete private Lebenssphäre des Betroffenen eingedrungen wird". Dagegen wird die bei der Großer-Lauschangriff-Entscheidung gestellte Feststellung zur Online-Durchsuchungsmaßnahme geltend gemacht, infolgedessen zu dem Schluss gelangt wird, dass bei der Online-Durchsuchung ein Eingriff in das Wohnungsgrundrecht in Betracht kommt[81].

Allerdings hat das BVerfG in seiner Rechtsprechung zur Online-Durchsuchung einen Eingriff in das Wohnungsgrundrecht durch diese Maßnahme folgendermaßen verneint: *„Art. 13 I GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet. Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone."*[82]

### 2. Überlegung im Rahmen des Fernmeldegeheimnisgrundrechts

Umstritten ist weiterhin auch, ob die Online-Durchsuchung die Grundrechte aus Art. 10 GG tangiert.

Im Hinblick auf das Fernmeldegeheimnis des Art. 10 GG ist zunächst festzustellen, dass das Fernmeldegeheimnis des Art. 10 GG nur solche Telekommunikationsdaten erfasst, die aus dem Herrschaftsbereich des Telekommunikationsdienstleisters erhoben werden[83].

---

81 **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1171; **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 122.

82 BVerfG, Urteil vom 27.02.2008, Rn. 194, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

83 Vgl. **Günther**, Ralf, "Zur strafprozessualen Erhebung von Telekommunikationsdaten - Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlichunkalkulierbares Wagnis?", NStZ, 2005, S. 493.

Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers (also auf dem eigenen Telefon oder Computer) gespeicherten E-Mails oder Verkehrsdaten unterstehen nach Auffassung des *BVerfG* allerdings nicht mehr dem Schutz des Fernmeldegeheimnisses gem. Art. 10 GG[84], und selbstverständlich ist zwar ein Zugriff auf die empfangenen Nachrichten, die weiter auf dem Handy oder Computer gespeichert bleiben, kein Eingriff mehr in Art. 10 GG[85], weil die auf dem PC abgespeicherten E-Mails keine „Telekommunikation" sind[86]. Daraus ergibt sich, dass die Online-Durchsuchung keinen Eingriff in das Fernmeldegeheimnis nach Art. 10 GG darstellt[87], weil die Online-Durchsuchung auf dem PC abgespeicherte Daten angreift und darin auch keine Telekommunikation in Betracht kommt[88].

Die Literatur stimmt mit dieser Ansicht größtenteils überein: In Bezug darauf, dass die Online-Durchsuchung keinen Eingriff in das Fernmeldegeheimnis nach Art. 10 GG darstellt, heben *Werkmeister/Pötters* hervor, dass Art. 10 I GG nur vor Zugriffen auf laufende Kommunikationsvorgänge schützt[89].

---

84 **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 486; *BverfGE* 115, 166, abrufbar unter http://www.servat.unibe.ch/dfr/bv115166.html (Stand vom 09.08.2018); für den Zugriff auf empfangene Nachrichten, vgl. **Bär**, Wolfgang, "Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen Gesetzliche Neuregelungen zum 1.1.2008", MultiMedia und Recht, 2008, S. 219.

85 **Bär**, Wolfgang, "Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen Gesetzliche Neuregelungen zum 1.1.2008", MultiMedia und Recht, 2008, S. 219; BVerfG Urteil vom 02.03.2006, Leitsatz 1, MMR 2006, S. 217 [das Urteil ist abrufbar auch unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2006/03/rs20060302_2bvr209904.html (Stand vom 09.08.2018)]; für Information über diesbezügliche BVerfG- und BGH-Entscheidungen vgl. **Günther**, Ralf, "Zur strafprozessualen Erhebung von Telekommunikationsdaten - Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlichunkalkulierbares Wagnis?", NStZ, 2005, S. 488 ff.; vgl. hierzu auch **Sachs**, Michael/**Krings**, Thomas, "Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"", JuS, 2008, S. 484; **Nazari-Khanachayi**, Arian, "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 763.

86 **Tinnefeld**, Marie-Theres, "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 138.

87 Obwohl einige Ansichten dagegen sprechen: *Hofmann* hebt hervor, dass die Online-Durchsuchung jedoch die Grundrechte aus Art. 10 GG tangieren kann, vgl. **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 122.

88 **Gusy**, Christoph, "Gefahraufklärung zum Schutz der öffentlichen Sicherheit und Ordnung", JA, 2011, S. 650; vgl. auch **Huber**, Bertold, "Trojaner mit Schlapphut - Heimliche „Online-Durchsuchung " nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz", NVwZ, 2007, S. 883.

89 Vgl. hierzu **Werkmeister**, Christoph/**Pötters**, Stephan, "Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen"", JuS, 2012, S. 229.

*Martini* unterstützt diese Ansicht und stellt fest, dass Art. 10 I GG vor den Gefahren räumlich distanzierter Kommunikation über das Medium drahtloser oder drahtgebundener elektromagnetischer Wellen schützt, gleichsam die Privatheit auf Distanz, wobei die Online-Durchsuchung aber nicht notwendig an einen laufenden Telekommunikationsvorgang anknüpft[90].

*Eifert* weist insofern auch darauf hin, dass Art. 10 GG als Schutz der spezifischen Gefahren räumlich-distanzierter Kommunikation insbesondere nicht die schützenswerten Daten erfassen kann, die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeichert bleiben[91].

Dazu, dass Art. 10 I GG durch die Online-Durchsuchung nicht tangiert ist, stellt *Werkmeister* folgendermaßen fest, dass der durch Art. 10 I GG bewirkte Schutz in diesem Fall nicht besteht, da die bloße Überwachung der Nutzung eines informationstechnischen Systems keine laufenden Kommunikationsvorgänge betrifft, außerdem hebt er hervor, dass bei dem Online-Zugriff letztlich nur die Computer kommunizieren, nicht aber grundrechtsberechtigte Personen, wobei Art. 10 I GG nicht die „Kommunikation“ zwischen technischen Geräten, sondern nur die Kommunikation zwischen Personen schützt[92].

Diese Ansichten werden jedoch von *Kutscha* und *Huber* folgendermaßen nicht vertreten:

*Huber* stellt heraus, dass das uneingeschränkte, nachträgliche Auslesen des Inhalts von E-Mail-Korrespondenz im Wege der „Online-Durchsuchung“ gegen Art. 10 I GG verstößt, da sich hierdurch Kenntnis von einer – wenn auch bereits abgeschlossenen – Telekommunikation verschafft wird[93].

*Kutscha* weist auch darauf hin, dass die gespeicherten Daten unabhängig davon, ob die Daten bei einem Telekommunikationsunternehmen bzw. Internet-Provider oder im Mobiltelefon oder Personalcomputer des Teilnehmers gespeichert sind, detaillierte Aufschlüsse über das Kommunikationsverhalten und damit auch über die Sozialbeziehungen geben. Insofern hebt er hervor, dass dem Schutzzweck des Art. 10 GG nur dann hinreichend Rechnung getragen

---

90 Vgl. hierzu **Martini**, Mario, “Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts”, JA, 2009, S. 841.

91 Vgl. hierzu **Eifert**, Martin, “Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen”, NVwZ, 2008, S. 522.

92 Vgl. hierzu **Werkmeister**, Christoph/**Pötters**, Stephan, “Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen“”, JuS, 2012, S. 225 und 228.

93 Vgl. hierzu **Huber**, Bertold, “Trojaner mit Schlapphut - Heimliche „Online-Durchsuchung ” nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz”, NVwZ, 2007, S. 884.

wird, wenn sämtliche individualbezogenen Verkehrsdaten unabhängig vom Ort ihrer Speicherung einbezogen werden[94].

### 3. Überlegung im Rahmen des Rechts auf informationelle Selbstbestimmung und des Computergrundrechts

Es liegt auf der Hand, dass die Online-Durchsuchung in das Recht auf informationelle Selbstbestimmung eingreift[95], das aus Art. 2 I in Verbindung mit Art. 1 I GG abgeleitet wird und als „Befugnis des Einzelnen definiert ist, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[96].

Nach der Auffassung des BVerfG geht die durch diese Maßnahme stattgefundene Beeinträchtigung des Interesses des Betroffenen folgendermaßen sogar noch über den Schutzbereich des Rechts auf informationelle Selbstbestimmung hinaus: *„Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus."*[97]

Weil dieses Recht den Persönlichkeitsgefährdungen durch die Nutzung moderner informationstechnischer Systeme nicht vollständig Rechnung trägt und eine Schutzlücke darstellt,[98] hat das BVerfG[99] ein neues Grundrecht aus

---

94 Vgl. hierzu **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 486.

95 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 122; **Martini**, Mario, "Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts", JA, 2009, S. 841f.

96 **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 483; **Tinnefeld**, Marie-Theres/**Petri**, Thomas/**Brink**, Stefan, "Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz Eine erste Analyse und Bewertung", MMR, 2010, S. 728; **Erdem**, Mustafa Ruhan, Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri, (Dissertation), S. 109 ff.

97 BVerfG, Urteil vom 27.02.2008, Rn. 200, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018); **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 485; **Hirsch**, Burkhard, "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822," NJOZ, 2008, S. 1911.

98 BVerfG, Urteil vom 27.02.2008, Rn. 200, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018); für die Ansicht, dass Art. 2 I i.V.m. Art. 1 I

dem allgemeinen Persönlichkeitsrecht[100] aus Art. 1 I GG i.V.m. Art. 2 I GG in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[101] entwickelt[102] und festgestellt, dass diese Maßnahme in eben dieses eingreift[103]. Begründet würde dies mit dem Umstand, dass das neue Grundrecht in Betracht kommt, wenn eine Eingriffsermächtigung informationstechnische Systeme wie etwa PCs betrifft oder solche Mobiltelefone oder elektronische Terminkalender erfasst, die mittels ihrer großen Funktionsumfänge „allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“[104]. Demnach stelle die Online-Durchsuchung zu Recht eine solche Eingriffsermächtigung dar[105].

Jedoch wurde diesem neuen Grundrecht in der Literatur, entgegen der Ansicht von *Sachs*[106]*, nicht* ohne Einwände Anerkennung gezollt.

---

GG die Schutzlücke schließt, vgl. hierzu **Martini**, Mario, “Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts”, JA, 2009, S. 841; *Eifert* vertritt diese Ansicht ebenfalls, vgl. hierzu **Eifert**, Martin, “Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen”, NVwZ , 2008, S. 522.

99 Vgl. BVerfG, Urteil vom 27.02.2008, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

100 Für Informationen zum allgemeinen Persönlichkeitsrecht des Beschuldigten im Strafverfahren vgl. **Trüg**, Gerson, “Medienarbeit der Strafjustiz – Möglichkeiten und Grenzen”, NJW, 2011, S. 1042; *Martini* hebt hervor, dass „Vertraulichkeit und Integrität informationstechnischer Systeme“ unter den Schutzbereich des allgemeinen Persönlichkeitsrecht fallen, vgl. **Martini**, Mario, “Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts”, JA, 2009, S. 841 f.

101 Vgl. BVerfG, Urteil vom 27.02.2008, NJW 2008, S. 822, Rn. 166 ff.; *Hoeren/Gräbig* legen die Literatur zum Thema Online-Durchsuchung dar, vgl. hierzu **Hoeren**, Thomas/**Gräbig**, Johannes, “Entwicklung des Internet- und Multimediarechts im Jahr 2009”, MMR-Beil., 2010, S. 33.

102 **Soiné**, Michael, “Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder”, NVwZ, 2012, S. 1587.

103 Vgl. auch **Hirsch**, Burkhard, “Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822”, NJOZ, 2008, S. 1915 f.

104 Vgl. BVerfG, Urteil vom 27.02.2008, NJW 2008, S. 828, Rn. 203; **Kutscha**, Martin, “Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte”, LKV, 2008, S. 485.

105 Vgl. hierzu **Sachs**, Michael/**Krings**, Thomas, “Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”“, JuS, 2008, S. 483.

106 Vgl. hierzu **Sachs**, Michael/**Krings**, Thomas, “Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”“, JuS, 2008, S. 484.

Angesichts der Feststellung des BVerfG, dass es sich bei dem informationellen Selbstbestimmungsrecht um den Schutz einzelner Informationen handelt, nicht aber um die Ausforschung einer Persönlichkeit durch das Eindringen in ein informationstechnisches System, auf dessen Nutzung der Einzelne angewiesen ist und in dem er unausweichlich zahllose Spuren hinterlassen muss[107], kritisiert *Sachs* diese Aussage des *BVerfG* und hält sie für bloße petitio principii[108]. Er hebt hervor, dass das Recht auf informationelle Selbstbestimmung, das Informationen unabhängig davon schützt, ob sie bereits ihrer Art nach sensibel sind oder nicht, zum Schutz informationstechnischer Systeme nicht ausreichen soll und die Begründung mit dem großen Umfang des Datenbestandes, den ein Zugriff auf ein solches System ermöglicht, und dem besonderen Gewicht eines so weitreichenden Eingriffs für die Persönlichkeit nicht überzeugen kann, denn diese Gegebenheiten sind vom Schutzgegenstand der informationellen Selbstbestimmung unabhängig. Er schlägt vor, dass dem besonderen Gewicht der Beeinträchtigung eines grundrechtsgeschützten Interesses durch entsprechend strenge materielle Anforderungen im Rahmen der Verhältnismäßigkeitsprüfung oder auch durch solche an das Verfahren im Rahmen der objektivrechtlichen Grundrechtsgehalte Rechnung getragen werden kann.

*Kutscha* hebt hervor, dass das Recht auf informationelle Selbstbestimmung durchaus auch vor intensiven Persönlichkeitsgefährdungen durch die gezielte Erfassung und Auswertung auch hochsensibler personenbezogener Daten schützt, die in unterschiedlichen informationstechnischen Systemen gespeichert sind, und weist darauf hin, dass in der Tat sich der Schutzbereichs des Rechts auf informationelle Selbstbestimmung schon nach dem Volkszählungsurteil des *BverfG* auf alle Formen der „Verwendung“ personenbezogener Daten, mithin auch auf jegliche Form der Zweckentfremdung ohne Wissen und Einwilligung des Betroffenen (insbesondere auch durch eine „Online-Durchsuchung”), erstreckt[109].

*Eifert* hebt hervor, dass hinreichender Schutz durch die informationelle Selbstbestimmung gewährleistet werde und das neue Grundrecht insgesamt letztlich unnötig und tendenziell zu breit angelegt sei[110]. Insofern weist er darauf

---

107 Vgl. hierzu **Hirsch**, Burkhard, “Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822,” NJOZ, 2008, S. 1915; BVerfG, Urteil vom 27.02.2008, NJW 2008, S. 827 ff., Rn. 198 ff.

108 Vgl. hierzu **Sachs**, Michael/**Krings**, Thomas, “Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”“, JuS, 2008, S. 484 f.

109 Vgl. hierzu **Kutscha**, Martin, “Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte”, LKV, 2008, S. 485.

110 Vgl. hierzu **Eifert**, Martin, “Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen”, NVwZ, 2008, S. 522f.

hin, dass, soweit es also um die Gewährleistung der Vertraulichkeit der in einem informationstechnischen System gespeicherten Daten geht, keine Schutzlücke vorliegt, sondern nur die Notwendigkeit, im Rahmen der Verhältnismäßigkeitsprüfung auf die besonders hohe Eingriffsintensität mit entsprechend hohen Schutzanforderungen zu reagieren. Insofern hält er die dabei liegende Gefahr für eine Annexgefahr, der nicht selbstständig begegnet werden muss, sondern der beim Schutz der Daten immer zugleich hinreichend Genüge getan wird. Außerdem weist er darauf hin, dass gerade die Notwendigkeit, das neue Grundrecht zukünftig gegenüber der informationellen Selbstbestimmung abzugrenzen, die Gefahr mit sich bringt, dass es sich letztlich eher zu einem apersonalen, technikorientierten Grundrecht entwickelt, als dass es den Schutz der Persönlichkeitsentfaltung unter den Bedingungen des Internets sicherstellt.

*Sachs* stellt infrage, ob es sinnvoll ist, die Zahl der Grundrechte dadurch zu vermehren, dass einzelne Persönlichkeitsinteressen nicht nur als „Ausprägungen" des allgemeinen Persönlichkeitsgrundrechts, sondern gleich als eigenständige Grundrechte gehandelt werden, und hebt die Kritik hervor, dass der Schutzgegenstand von diesem Grundrecht unklar ist und das geschützte Interesse des Bürgers nur wenig präzise bestimmt wird[111].

Dagegen steht *Nazari-Khanachayi* hinter dem BVerfG und hebt hervor, dass die besonderen Ausprägungen des allgemeinen Persönlichkeitsrechts aus Art. 2 I i.V.m. Art. 1 I GG in Form des Schutzes der Privatsphäre bzw. des Rechts auf informationelle Selbstbestimmung nicht vermögen, die Schutzlücke zu schließen, und begründet dies damit, dass die Entstehung der Daten, ihre Verknüpfungspunkte miteinander und die Unüberschaubarkeit ihrer Relevanz anhand eines Datums ausschlaggebend dafür sind, dass die Infiltration nicht nur private, sondern (schlicht) alle Daten umfassen kann, die in ihrer Gesamtheit zu einem umfassenden Bild des Nutzers führen können[112]. Insofern weist er darauf hin, dass der Schutz der Privatsphäre die Lücke nicht zu schließen vermag. Außerdem stellt er heraus, dass der Nutzer aufgrund der komplexen informationstechnischen Systeme kaum erfassen kann, welche personenbezogenen bzw. seine Persönlichkeit betreffenden Daten bei dem Nutzungsvorgang generiert, wo und wie lange sie festgehalten und in welchen Verwendungskontexten sie durch wen genutzt werden. Demzufolge ist es praktisch nicht möglich, sein Selbstbestimmungsrecht auszuüben. Zudem hebt er das geschützte Interesse des Bürgers hervor. Danach wird der Nutzer auf der einen Seite dahingehend geschützt, dass ihm die Vertraulichkeit der von einem

---

111 Vgl. hierzu **Sachs**, Michael/**Krings**, Thomas, "Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"", JuS, 2008, S. 484 f.

112 Vgl. hierzu **Nazari-Khanachayi**, Arian, "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 763 f.

vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten zugesichert wird. Auf der anderen Seite wird der Nutzer vor Zugriffen auf das System, namentlich die Integrität, geschützt, wenn „dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können", da hierdurch eine „entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen" wird.

*Werkmeister/Pötters* unterstützen die Ansicht des BVerfG insofern, als dass auch die bisher in der Rechtsprechung des *BVerfG* anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistungen des Schutzes der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht in ausreichendem Maße genügen, weil bei der bloßen Infiltration des Computersystems noch keine Daten erhoben werden, sodass auch die informationelle Selbstbestimmung nicht zwingend einschlägig ist.[113] Zudem haben sie den Schutzbereich des neuen Grundrechts gegen Art. 10 und 13 GG so abgegrenzt, dass das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nur subsidiär greift, dieses ist aber in den nicht von Art. 10, 13 GG erfassten Fällen ebenfalls verletzt[114]. Insofern stellen sie fest, dass, soweit sich der infiltrierte Rechner in einer Wohnung befindet, im Hinblick auf diese Maßnahme Art. 13 I GG einschlägig ist. Allerdings ist für den Fall, dass der Standort des Computers offen ist, Raum für das sonst subsidiäre Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorhanden.

## III. DURCHFÜHRBARKEIT DIESER MASSNAHME IN DER TÜRKISCHEN RECHTSORDNUNG

Bei einer „Online-Durchsuchung" wird auf Dateien auf dem PC eines Beschuldigten, auf denen sich möglicherweise verfahrensmäßig relevante Daten und E-Mails befanden[115], eingegriffen[116]. Für diesen schwerwiegenden Eingriff

---

113 **Werkmeister**, Christoph/**Pötters**, Stephan, "Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen"", JuS, 2012, S. 225 ff.; vgl. hier auch **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107 (Sachbeschädigung).

114 Vgl. auch **Sachs**, Michael/**Krings**, Thomas, "Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"", JuS, 2008, S. 483 f.

115 **Tinnefeld**, Marie-Theres, "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 139.

116 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107; der Antrag des Generalbundesanwalts an den Ermittlungsrichter beim *BGH,* der der neuen Entscheidung des *BGH* zu Grunde liegt vgl. *BGH*, NJW 2007, 930.

in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausdruck des allgemeinen Persönlichkeitsrechts und selbstverständlich auch in das Recht auf informationelle Selbstbestimmung ist nach Art. 13 TGG[117] eine gesetzliche Ermächtigungsgrundlage erforderlich.

Zu überprüfen ist, ob in der Türkei nach der derzeitigen Fassung der CMK[118] und Polizeigesetz eine Online-Durchsuchung durchgeführt werden kann.

Insofern werden zuerst die Regelungen der Überwachung der Telekommunikation nach Art. 135 CMK[119] und nach Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes geprüft[120].

In diesem Zusammenhang ist es möglich, die unbewusste, durch das eingesetzte Computervirus verursachte Datenübertragung an die ermittelnde Stelle als Telekommunikation i.S.d. Art. 135 CMK, bzw. Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes anzusehen, weil der Betroffene durch die Internetnutzung den Telekommunikationsvorgang an sich willentlich in Gang setzt[121], wobei zurecht für eine Telekommunikation eine sämtlich mit dem Willen des Betroffenen stattgefundene Übermittlung nicht erforderlich ist, sondern es ausreicht, dass der Betroffene die Telekommunikationsanlage selbst willentlich in Betrieb gesetzt oder betriebsbereit gehalten hat[122].

Andererseits spricht der Umstand, dass die angegriffenen Daten schon gespeichert sind, also sich nicht mehr im Übermittlungsfluss befinden, gegen die Behauptung, dass diese durch das eingesetzte Computervirus verursachte Datenübertragung an die ermittelnde Stelle eine Telekommunikation i.S.d. Art.

---

117 Das türkische Grundgesetz. Vgl hier auch **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015, S.71 ff.

118 Die türkische Strafprozessordnung.

119 Hier wird der Einsatz technischer Mittel, „kleine Lauschangriff" § 140 CMK nicht erörtert, weil bei der Online-Durchsuchung es nicht um das Abhören gesprochener Worte geht, sondern um die Durchsuchung eines Computers.

120 Die repressive Telekommunikationsüberwachungsmaßnahme ist in CMK angeordnet, während die präventive Telekommunikationsüberwachungsmaßnahme in Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes angeordnet. In Hinblick auf die Zwischenfrage, ob nach den Telekommunikationsüberwachungsvorschriften eine Online-Durchsuchung durchgeführt werden kann vgl. **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 123 ff.

121 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 123 f.

122 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S.123 f. Für die gegenseitige Ansicht vgl. **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015, S. 56 und 118; **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 533.

135 CMK, bzw. Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes darstellt[123], weil nach der Definition des Begriffs der Telekommunikation[124] im Art. 1 Telegraf und Telefon Gesetz[125] „das Aussenden, Übermitteln und Empfangen von Zeichen, Symbolen, Tönen und Bildern sowie jegliche andere Arten von verwandelbaren Daten mittels Telekommunikationsanlagen" für eine Telekommunikation erforderlich ist. Es wäre ohne Bedeutung, dass die Dateien, auf die sich die Maßnahme bezieht, bereits vor deren Beginn auf dem Zielcomputer gespeichert worden sind, weil die Online-Durchsuchung technisch nur möglich ist, wenn der Computernutzer das Internet nutzt und dabei die durch das aufgespielte Computervirus ausgelesenen Daten insoweit nur als Bestandteil des durch den Online-Status ohnehin bestehenden Datenstroms und damit Bestandteile der Telekommunikation nach Art. 135 CMK, bzw. nach Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes angesehen werden sollen[126]; kritisch ist dabei anzumerken, dass dies eine übersteigernde Interpretation der Vorschrift im Art.1 Telegraf und Telefon Gesetz darstellt, weil eine solche Interpretation, im Rahmen der Internetnutzung bzw. beim Datenstrom die schon im PC gespeicherten Daten als einen Bestandteil der Telekommunikation zu qualifizieren, dem Wille des Gesetzgebers nicht entsprechen werde.

Erwähnenswert ist zuletzt, dass bei dieser Online-Durchsuchungsmaßnahme keine Telekommunikation zwischen dem Tatverdächtigen und einem Dritten überwacht wird[127]- also keine „Überwachung" im Sinne des Art.135 CMK, bzw. des Absatz 2 der Zusatzbestimmung 7 des Polizeigesetzes vorliege - denn hier nimmt der Staat als Dritter am zu kontrollierenden Kommunikationsvorgang nicht teil[128], sondern stellt die Verbindung erst selbst her und greift durch die

---

123 Vgl. **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015, S. 47 ff.; **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 533.

124 Vgl. hierzu auch: **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 413; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar /**Tepe**, İlker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 456; **Kunter**, Nurullah/ **Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 716 **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 533; **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015, S. 51 und 144.

125 Türkisches Telefon- und Telegraphengesetz mit der Gesetznummer 406.

126 Vgl. **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 123 f.

127 *BGH,* NJW 2007*,* 930*; BVerfG*, Urteil vom 27. 02. 2008, BverfG, NJW 2008, 822*,* 825.

128 Vgl. **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 455; **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan Iletisimin Denetlenmesi, 4. Auflage, 2015, S. 53.

Telekommunikationsleitung auf bereits gespeicherte Daten zu, welche u.U. noch nicht einmal frühere Kommunikationsdaten sein müssen[129] und veranlasst eine Übermittlung der auf dem Zielcomputer gespeicherten Daten an die ermittelnde Stelle[130].

Es liegt auch nahe, dass die Vorschrift über die Durchsuchung beim Computer[131] im Art. 134 CMK[132] für eine Online Durchsuchung eine Ermächtigungsgrundlage darstellen könnte[133], wonach eine Durchsuchung des Computers, das Kopieren der durch die Computer-Durchsuchung erlangten Daten, und das Ausdrucken derselben durch Richterliche Anordnung zulässig ist, wenn es nicht möglich ist, auf eine andere Weise Nachweise zu finden. Hier ist jedoch bedenklich, dass die Computer-Durchsuchung nach Art. 134 CMK eine offene Maßnahme ist (Art. 134 CMK i.V.m. Art.120 CMK), deren Kennzeichen in der physischen Anwesenheit der Ermittlungsbeamten am Ort der Durchsuchung liegt[134], während die Online-Durchsuchung eine verdeckte Form der Durchsuchung von elektronischen Datenverarbeitung-Anlagen[135] darstellt.

In diesem Zusammenhang ist zuerst festzustellen, ob Offenheit ein konstitutives Merkmal des Durchsuchungsbegriffs ist.

Tatsächlich stellt der strafrechtliche Durchsuchungsbegriff nach ganz herrschender Meinung das ziel- und zweckgerichtete Suchen staatlicher Organe nach einem bestimmten abgrenzbaren Bereich oder Objekt dar[136]; daraus ergibt

---

129 **Heinrich**, Bernd/**Reinbacher**, Tobias, Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018).

130 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 123 f.

131 Vgl. sie hier auch **Şen**, Osman Nihat, „Ceza Hukukunda Bilgisayar Araştırmaları", Ceza Hukuku Dergisi, Band 1, Zahl. Nr. 1, Oktober 2006, S. 375 ff.

132 Die Maßnahme der Durchsuchung beim Computer wird im Polizeigesetz nicht angeordnet.

133 In Hinblick auf die Zwischenfrage, ob nach den Art. 110 StPO (Durchsuchung von Papieren, auch von elektronischen Speichermedien) eine Online-Durchsuchung durchgeführt werden kann, vgl. *BGH,* Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237, 237.

134 **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 505; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 428; **Kunter**, Nurullah/**Yenisey**, Feridun/ **Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 988; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 389 f.; vgl. auch **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 124.

135 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 106.

136 **Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S.972; **Bacaksız**, Pınar/**Özbek**, Veli Özer, "Ceza Muhakemesi Hukukunda Arama", Ceza Hukuku Dergisi, Band 1, Zahl Nr. 1, September

sich nicht, dass die strafprozessuale Durchsuchung weder ein offenes Handeln noch eine körperliche Anwesenheit von Ermittlungsbeamten am Durchsuchungsort voraussetzt.

Außerdem setzt Art.157 CMK voraus, dass die Art und Weise der Prozedur beim Ermittlungsprozess soll heimlich sein soll, es sei denn der Gesetzgeber schließt einen solchen Fall aus oder dieser verstößt gegen die Schutzrechte[137]. Diese Vorschrift beruft sich darauf, dass die Ermittlungen in Heimlichkeit nach der Pflicht zur Erforschung der Wahrheit und zur Gewährleistung der effektiven Strafverfolgung ein Gebot darstellen[138].

Übrigens ist wieder hervorzuheben, dass die Vorschriften dynamisch und nach den heutigen Realitäten ausgelegt werden sollen[139]. Durch eine solche zeitgemäße, den veränderten technischen Gegebenheiten angepasste Auslegung[140] könnte man sagen, dass die Subsumtion der Online-Durchsuchung unter Computer-Durchsuchung nach Art.134 CMK zulässig wird.

Zweitens sind die Vorschriften über die Art und Weise der Durchführung der Durchsuchungsmaßnahme nach Art. 134 CMK zu überprüfen.

Der Computer kann, wenn das Passwort nicht ermittelt und er nicht freigeschaltet werden kann, nach Art.134 CMK Abs. 2 der Beschlagnahme unterliegen, „wenn die Daten aus dem Computer nicht kopiert werden". Nach Abs. 3 sollen bei der Durchführung der Beschlagnahme des Computers „die

---

2006, S. 145 ff.; **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 124*;* **Baytar**, Serdal, *„*Koruma Tedbirlerinden Doğan Zararin Karşilanmasi", TBB Dergisi, Zahl Nr. 61, 2005, S. 366, abrufbar auch unter http://tbbdergisi.barobirlik.org.tr/m2005-61-190 (Stand vom 09.08.2018).

137 Im Hinblick auf das deutsche Strafrecht hat *BGH* ausdrücklich festgestellt, dass den strafprozessualen Vorschriften über das Ermittlungsverfahren ein Grundsatz der Offenheit des staatlichen Handelns nicht zu entnehmen ist und die Heimlichkeit der Ermittlungshandlungen nicht zu ihrer Unzulässigkeit führt (BGHSt 42, 139, 150) vgl. hierzu: **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 124 f.

138 **Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 137 und 593; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 103; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/ **Doğan**, Koray/**Bacaksız**, Pınar /**Tepe**, Ilker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 269; **Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 531; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 489; **Kaymaz,** Seydi, Ceza Muhakemesinde Telekommunikasyon Yoluyla Yapılan Iletisimin Denetlenmesi, 4. Auflage, 2015, S. 341.

139 **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 37.

140 **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 124.

gesamten Daten im System des PCs vorrätig gespeichert werden"; nach Abs. 4 werden diese gespeicherten Vorratsdaten kopiert, dieser Umstand protokolliert und zum Schluss von den Betroffenen unterschrieben werden[141]. Außerdem setzt der 134 CMK Abs. 5 voraus, dass „ohne eine Beschlagnahme die Daten auch kopiert werden können. Diese kopierten Daten sollen ausgedruckt werden, der Status quo soll protokolliert und von den Betroffenen unterschrieben werden." Diese Absätze dienen dem Rechtsschutz für den Betroffenen, weil sie durch die Erforderlichkeit der Anwesenheit und der Unterschrift der Betroffenen während der Durchsuchung Schutzmaßnahmen zu Gunsten des Beschuldigten darstellen[142].

Die Vorschriften bei diesen Absätzen können jedoch nicht vollständig vollgezogen werden, weil die Online-Durchsuchung eine heimlich durchgeführte Maßnahme ist und demzufolge der Computerbesitzer dieses Protokoll nicht unterschreiben kann. Dadurch wird der Rechtsschutz für den Betroffenen beeinträchtigt, wenn die Online-Durchsuchung unter der Computerdurchsuchungsvorschrift subsumiert wird. Diese Absätze stehen einer Anwendung der Onlinedurchsuchungsmaßnahme unter Art.134 CMK entgegen.

Der Rechtsschutz für den Betroffenen wird jedoch nicht endgültig beeinträchtigt, weil die Folge der Einschränkung im weitergehenden Stadium des Ermittlungsprozesses dadurch kompensiert wird, dass der Beschuldigte auch nach Abschluss der Online-Durchsuchung gegen deren Anordnung Beschwerde einlegen und gegen die Art und Weise ihrer Durchführung einen Antrag entsprechend Art. 267 CMK[143] stellen kann.

---

141 Für die detaillierten Ausführungen über diese Vorschriften Vgl. **Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/ **Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 506 f.; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S.449; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar/**Tepe**, İlker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 424 f.; **Kunter**, Nurullah/ **Yenisey**, Feridun/**Nuhoğlu**, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S.1023 f.; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S.409 f.

142 Im Hinblick auf das deutsche Strafrecht vgl. **Heinrich**, Bernd/**Reinbacher**, Tobias, Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018).

143 Nach 267 Abs.1 CMK kann man gegen den richterlichen Beschluss Beschwerde einlegen und nach 134 CMK wird die Computer Durchsuchung durch einen richterlichen Beschuss angeordnet, für die detaillierte Information vgl.: **Aydın**, Devrim, „Ceza Muhakemesi Kanunu'nda itiraz", TBB Dergisi, Zahl Nr. 65, 2006, S.61 ff. abrufbar unter http://tbbdergisi.barobirlik.org.tr/m2006-65-238 (Stand vom 09.08.2018); vgl. Sie hier auch **Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 670; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 450 und 830; **Özbek**, Veli Özer/**Kanbur**,

Auf der anderen Stelle könnte hier im Hinblick auf die Vorschriften über die Art und Weise der Durchführung der Durchsuchungsmaßnahme nach Art. 134 CMK teilweise behauptet werden, dass es sich hierbei nur um reine Ordnungsvorschriften handle, aus deren Verletzung keine Rechtsfolgen hergeleitet werden können[144], so dass deren auf die Folge nicht-einwirkenden Verstöße im Art. 302 Abs. 2 CMK nicht als Widerlegungsgrunde gesehen werden[145], und zwar könnte behauptet werden, dass die Vorschriften über die Art und Weise der Durchführung der Computer-Durchsuchung nach Art. 134 Absatz 4 und 5 CMK dadurch einer Anwendung des § 134 CMK bei der Durchführung der Online- Durchsuchung nicht entgegenstehen und dadurch die Online-Durchsuchung unter der Vorschrift der Computerdurchsuchung subsumiert werden kann.

Allerdings setzt Art. 120 Abs.1 CMK voraus, dass der Betroffene selbst, bei Unmöglichkeit seiner Anwesenheit ein Vertreter […] oder Nachbar während der Durchsuchung anwesend sein soll[146]. Angesicht dieses Falls könnte statuiert

---

Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar /**Tepe**, Ilker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 425 und 806 ff.; **Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 1394 ff.; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 768 ff.; **Kaymaz,** Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015, S. 419. In Deutschland können nach Abschluss der Durchsuchung gegen deren Anordnung Beschwerde eingelegt und gegen die Art und Weise ihrer Durchführung einen Antrag entsprechend § 98 II 2 StPO gestellt werden, vgl. hierzu: **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125.

144 Im Hinblick auf das deutsche Strafrecht vgl. **Heinrich**, Bernd/**Reinbacher**, Tobias, Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018); **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 125. Der BGH hat diese Ansicht zu Recht ablehnt und stattdessen annimmt, dass die Durchsuchung im Sinne der §§ 102 ff. StPO ihrem Wesen nach nicht heimlich sei (BGHSt 51, 211), vgl. hierzu: **Heinrich**, Bernd/**Reinbacher**, Tobias, Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018).

145 Vgl. **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 800; **Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 1425 f.; **Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan/**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 739; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 843; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar /**Tepe**, Ilker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 872.

146 Für die detaillierten Informationen über diese Vorschrift vgl. **Öztürk**, Bahri/**Tezcan**, Durmus/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/ **Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 505; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**,

werden, „dass die Beachtung des Art. 120 CMK dadurch gewährleistet wird, dass die Maßnahme - wie bereits ausgeführt - nur möglich ist, wenn der Betroffene mit seinem Computer „online" und damit während der Maßnahme zugegen ist. Dass er die Maßnahme nicht bemerkt, ändert an seiner Anwesenheit nichts". Allerdings würde dieses eine übersteigernde Interpretation der Vorschrift des Art. 120 darstellen, weil durch eine solche Interpretation der Schutzzweck der Norm ausgehöhlt werde.

Schließlich ist insofern zu akzeptieren, dass die Durchsuchung bei Abwesenheit dieser Personen nicht zulässig ist und die gesammelten Beweise insoweit auch nicht angewandt werden dürfen. Schließlich sind sie als unter Verstoß gegen die Normen der CMK erlangte Beweismittel rechtswidrig (Art. 38 Abs. 6 TGG, Art. 217 Abs. 2 CMK)[147].

Zum Schluss ist hervorzuheben, den im Art. 134 liegenden Widerspruch – wie oben darstellt wurde - zu beseitigen und zu erreichen, dass die Heimlichkeit der Online-Durchsuchung, deren Subsumtion unter die Computer-Durchsuchung nicht entgegensteht, stellt eine übersteigernde Interpretation der Vorschrift des Art. 134 dar; dies besonders angesichts des Falls, dass solche Maßnahmen, bei denen der Eingriff ohne die Kenntnis des Inhabers erfolgt, der Betroffene also weder um die Anordnung noch um das Kopieren seiner Daten weiß[148], wegen ihrer Verdecktheit einen anderen und „intensiveren" Eingriff[149] in die Rechte

---

Pınar/**Tepe**, İlker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 401; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 428; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 389 ff.

147 Vgl. hierzu **Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan /**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015, S. 505, 419; **Özbek**, Veli Özer/ **Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar/**Tepe**, Ilker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 415 f.; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 235; **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 61 ff. und 390; **Gülşen**, Recep, „Yargıtay Kararları Işığında Hukuka Aykırı Aramada Elde Edilen Delillerin Ceza Muhakemesinde Değerlendirilmesi", CHKD, 2015, Band 3, Zahl Nr. 2, S. 244 ff. Für die gegenseitige Ansicht vgl. Großer Strafsenat beim Kassationshof, Urteil vom 26.6.2007, Nr. E.2007/7-147, K.2007/159, abrufbar unter http://bilgibankasi.istanbulbarosu.org.tr/karar/hukuka-aykiri-arama-omutlak-delil-yasaklari-onispi-delil-yasaklari-o-degerlerin-tartimi-ilkesi/e1dM (Stand vom 09.08.2018); **Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008, S. 1079 ff.

148 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107.

149 Das heimliche Ausspähen dieser Daten vermittels einer „Online-Durchsuchung" ist sogar noch durch eine höhere Eingriffsintensität gegenüber der offenen Durchsuchung der Räume nach den §§ 102ff. StPO gekennzeichnet, vgl. Sie hierzu: **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1172; *BGH* sieht nun gerade wegen der Heimlichkeit der Maßnahme das Fehlen einer formell-gesetzlichen Befugnisnorm für eine Online-Durchsuchung, denn das Bild der Strafprozessordnung von einer rechtmäßigen Durchsuchung sei dadurch geprägt, dass

des davon Betroffenen darstellen, als eine herkömmliche offene Durchsuchung nach Art. 134 CMK. In diesem Sinne muss akzeptiert werden, dass die Heimlichkeit der Online-Durchsuchung der Zulässigkeit der Subsumtion entgegensteht[150], weil die Computer-Durchsuchung i.S. des Art. 134 CMK gerade durch das offene Vorgehen und die körperliche Anwesenheit der Ermittlungsbeamten am Ort der Durchsuchung gekennzeichnet ist. Hier ist auch nicht vergessen werden, dass bei der Ermittlungsmaßnahmen Analogieverbot vorhanden[151].

***Fazit***

1- Die Ermittlungsmaßnahme der verdeckten „Online-Durchsuchung, wonach ohne Wissen des Computernutzers speziell zur elektronischen Ausforschung von Daten entwickelter Softwareprogramme („Trojanische Pferde") von der Polizei oder den Nachrichtendiensten über das Internet in einen bestimmten Computer hineingelangen und die Durchsicht der dort auf der Festplatte des Computers gespeicherten Daten sowie der jeweiligen Anwendungen, wie Internet-Nutzung, Versendung von E-Mails etc. ermöglichen, ist nicht von den Eingriffsgrundlagen der CMK gedeckt und deshalb nach geltendem Recht unzulässig und kann nur nach einer unter Wahrung des Gebots der Verhältnismäßigkeit geschaffenen entsprechenden gesetzlichen Ermächtigungsnorm angeordnet werden.

2- Bei der Schaffung einer solchen neuen Rechtsgrundlage ist jedoch folgendes „Kernproblem" zu sehen: Wie und in welchem Verfahrensstadium

---

Ermittlungsbeamte am Ort der Durchsuchung körperlich anwesend sind und die Ermittlungen offenlegen vgl. Sie hierzu: **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 107 f.

150 In Hinblick auf das deutsche Strafrecht stellt *Tinnefeld* fest, dass die verfassungsrechtliche Durchsuchungsregelung hier jedenfalls kein grünes Licht gibt, denn sie geht vom Grundsatz der Offenheit staatlicher Präsenz in der Wohnung aus vgl. Sie hierzu: vgl. **Tinnefeld**, Marie-Theres, "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 139.; *Heinrich/Reinbacher* hebt hervor, dass die §§ 102 ff. StPO ihrer Konzeption nach der Heimlichkeit des Vorgehens indes gerade entgegenstehen und die Durchsuchung im Sinne der §§ 102 ff. StPO ihrem Wesen nach nicht heimlich sei vgl. Sie hierzu: **Heinrich**, Bernd/**Reinbacher**, Tobias, Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018); *Kemper* hebt auch hervor, dass die §§ 102, 105 StPO nicht als Rechtsgrundlage für eine Online-Durchsuchung herangezogen werden vgl. hierzu: **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 108; Für die gegenseitige Ansicht vgl. **Hofmann**, Manfred, "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 124 f.

151 **Ünver**, Yener/**Hakeri**, Hakan, Ceza Muhakemesi Hukuku, 13. Auflage, 2017, S. 33; **Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar /**Tepe**, İlker, Ceza Muhakemesi Hukuku, 7. Auflage, 2015, S. 106 f.; **Centel**, Nur/**Zafer**, Hamide, Ceza Muhakemesi Hukuku, 14. Auflage, 2017, S. 349.

sind höchstpersönliche Daten von verfahrensrelevanten Daten zu trennen? Und wie wird der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet[152], gegenüber der Kernbereichsschutzgewährleistung des TGG (Art. 13) : „*die Grundrechte und Grundfreiheiten können, ohne dass in deren Kerngehalt eingegriffen wird, nur durch die in der Verfassung liegenden jeweiligen Gründe und nur durch ein Gesetz beschränkt werden.*

Schließlich sollen bei der Online-Durchsuchung nicht nur die in Verzeichnissen abgelegten Dateien sondern auch die schon gelöschten Dateien durchsucht werden, weil sie im Rahmen strafrechtlicher Ermittlungen von erheblicher Beweisbedeutung sein können. Insofern kommt eine vollständige 1 zu 1 Kopie (sog. „Images") des Datenträgers in Betracht, weil die schon gelöschten Daten in der Ordnerstruktur des Rechners nicht mehr vorhanden sind und sie ein normaler Kopiervorgang ignoriert. Was aber ein großes Problem darstellt, dass dabei zwangsläufig auch alle privaten Dateien kopiert werden[153].

Auf der anderen Seite ist der Verzicht auf das Kopieren von den gelöschten Daten bei diesem Kernbereichsschutzproblem keine Lösung, weil das Kopieren der dem höchstpersönlichen Lebensbereich des Betroffenen - seiner Intimsphäre- gehörenden Daten auszuschließen bei der Durchsuchungsmaßnahme folgendermaßen kaum möglich ist[154].

Bei der Online-Durchsuchung versucht die Ermittlungsbehörde bei Tausenden, sogar wenn der Nutzer zum Beispiel seine Musik- und Bilddateien dort abgelegt hat Millionen privaten Dateien, die zum Teil die intimsten Inhalte haben, einer einzelnen beweisrelevanten Datei zu erlangen. Um diese Anzahl zu verkleinern wird die Durchsuchung auf den Namen oder den Typ der Dateien auch nicht beschränkt, da dieser von den Betroffenen auf jeden Fall verändert werden kann. Obwohl jede einzelne Datei im Prinzip vor dem Kopieren des Inhalts der Datenträgern auf ihre Geeignetheit als Beweis geöffnet und gesichtet werden soll, wäre die Anforderung über die vorherige Sichtung aller Daten unverhältnismäßig und nicht möglich[155]. Infolgedessen ist es auch nicht

---

152 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 108.

153 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 109.

154 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 109; **Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 486; **Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1172.

155 **Kemper**, Martin, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 109; *Eifert* hebt auch hervor, dass bei der Online – Durchsuchungen regelmäßig Daten in großem Umfang erhoben werden und erst später, bei der Auswertung, festgestellt werden kann, ob diese Daten auch den Kernbereich privater Lebensgestaltung umfassen. Insofern weist er darauf hin, dass damit die vom *BverfG*

möglich, private und andere Daten zu trennen bzw. das Kopieren der dem höchstpersönlichen Lebensbereich des Betroffenen - seiner Intimsphäre-gehörenden Daten bei der Online Durchsuchung auszuschließen[156], obwohl auf das Kopieren von den gelöschten Daten verzichtet wurde.

Insofern ist hervorzuheben, dass die Bestimmung des BVerfG über den Kernbereichsschutz der Problemlösung auch keine Rechnung trägt. Schließlich nach dem Gericht hat eine *„gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, [...] so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden*[157]*. Ist es – wie bei dem heimlichen Zugriff auf ein informationstechnisches System – praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen*

---

regelmäßig geforderte Unantastbarkeit dieses Bereichs aber *notwendig* verletzt wird und stellt fest, dass diese Dilemma sich nur vermeiden lässt, soweit es einen Kontext gibt, aus dem auf die Art des Inhalts der Information geschlossen werden kann, ohne sie selbst zu kennen, wobei ein solcher Kontext liegt häufiger noch bei Lauschangriff oder Telefonüberwachung vor und ermöglicht dann eine rechtzeitige Beendigung der Datenerhebung. Allerdings bei der Online-Durchsuchung dürfte ein solcher Kontext die seltene Ausnahme bilden, vgl. hierzu **Eifert**, Martin, "Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen", NVwZ, 2008, S. 523 f.

156 Nach *Brügmann* würden Online-Durchsuchungen deshalb das Recht auf informationelle Selbstbestimmung aushöhlen, Vgl. hierzu „DAV lehnt heimliche Online-Durchsuchung nach wie vor ab", Redaktion FD-StrafR, Aktuelle Nachrichten, FD-StrafR 2008, 257354; **Gusy**, Christoph, "Gefahraufklärung zum Schutz der öffentlichen Sicherheit und Ordnung", JA, 2011, S. 650; Bei der Kritik dieser Maßnahme im BKAG ist auch gefragt werden, auf welche Weise allerdings sichergestellt werden soll, dass nur der Computer eines Terrorverdächtigen ausgeforscht und keine Unbeteiligten betroffen werden (**Kutscha**, Martin, "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 486) und erwähnt, dass mit dem Einsatz dieses Instruments (Online-Durchsuchungen) nicht nur die Computer einer Anzahl unbedarfter Straftäter ausgeforscht werden, sondern damit zugleich viele dort gespeicherte Daten über unbescholtene Bürger den verschiedenen Sicherheitsbehörden zur Kenntnis gelangen (**Kutscha**, Martin, "Verdeckte "Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1173).

157 Allerdings stellt sich hier die Frage, ob „Kernbereichsdaten" der richtige Maßstab sind. Das BVerfG sollte auf die Daten, die für den Prozess erforderlich sind, abstellen und für die anderen, nicht-erforderlichen Daten für hinreichenden Schutz in der Auswertungsphase sorgen. Schließlich soll der Eingriff nach den Rechtsprechungen des EGMR auf das „unbedingt erforderliche Maß" beschränkt sein, vgl. hierzu EGMR, Urteil vom 28.04.2005 – Buck gegen Deutschland, Rn. 50, abrufbar unter https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-68920%22]} (Stand vom 09.08.2018); EGMR, Urteil vom 30.09.2014 – Prezhdarovi gegen Bulgarien, Rn. 49, abrufbar unter https://hudoc.echr.coe.int/eng?i=001-146565#{%22itemid%22:[%22001-146565%22]} (Stand vom 09.08.2018).

*werden."*[158] Das BVerfG hat durch seine Vorgabe darauf hingewiesen, dass die Daten aus dem Kernbereich erhoben werden können, soweit es praktisch unvermeidbar ist, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann[159]. Dadurch nimmt aber das BVerfG hin, dass in den Kernbereich der privaten Lebensgestaltung auf irgendeine Weise eingegriffen wird und dies Hinnehmen stellt selbst einen Verstoß gegen das Kernbereichsschutzprinzip dar.

---

158 BVerfG, Urteil vom 27.02.2008, Rn. 277, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).

159 Vgl. BVerfG, Urteil vom 27.02.2008 (Online-Durchsuchung), abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018); vgl. sie hier auch **Nazari-Khanachayi**, Arian, "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 765.

## LITERATUR VERZEICHNIS

**Aydın**, Devrim: „Ceza Muhakemesi Kanunu'nda İtiraz", TBB Dergisi, Zahl Nr. 65, 2006, S.61 ff.

**Bacaksız**, Pınar/**Özbek**, Veli Özer: "Ceza Muhakemesi Hukukunda Arama", Ceza Hukuku Dergisi, Band 1, Zahl Nr. 1, September 2006, S. 145-206.

**Bär**, Wolfgang: "Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen Gesetzliche Neuregelungen zum 1.1.2008", MultiMedia und Recht, 2008, S. 215 ff.

**Baum**, Gerhart Rudolf/**Schantz**, Peter: "Die Novelle des BKA-Gesetzes Eine rechtspolitische und verfassungsrechtliche Kritik", ZRP, 2008, S. 137 ff.

**Bayraktar**, Çiler Damla: Eingriffe in die Privatsphäre durch technische Überwachung Ein deutsch-türkischer Vergleich anhand Art. 8 EMRK, Hamburg 2017.

**Baytar**, Serdal: „Koruma Tedbirlerinden Doğan Zararın Karşılanması", TBB Dergisi, Zahl Nr. 61, 2005, S. 359 ff.

**Buermeyer,** Ulf: „Die „Online-Durchsuchung" Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS, 8/2007, S. 329 abrufbar unter http://www.hrr-strafrecht.de/hrr/archiv/07-08/index.php?sz=7, (Stand vom 09.08.2018).

**Centel**, Nur/**Zafer**, Hamide: Ceza Muhakemesi Hukuku, 14. Auflage, 2017.

**Denninger**, Erhard: "Verfassungsrechtliche Grenzen des Lauschens - Der „große Lauschangriff" auf dem Prüfstand der Verfassung", ZRP, 2004, S. 101 ff.

**Eifert**, Martin: "Informationelle Selbstbestimmung im Internet Das BVerfG und die Online-Durchsuchungen", NVwZ, 2008, S. 521 ff.

**Erdem**, Mustafa Ruhan: Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri, (Dissertation) Ankara 2001.

**Gusy**, Christoph: "Gefahraufklärung zum Schutz der öffentlichen Sicherheit und Ordnung", JA, 2011, S. 641 ff.

**Gusy**, Christoph: "Lauschangriff und Grundgesetz", JuS, 2004, S. 457 ff.

**Gusy**, Christoph: "Überwachung der Telekommunikation unter Richtervorbehalt Effektiver Grundrechtsschutz oder Alibi?", ZRP, 2003, S. 275 ff.

**Gülşen**, Recep: „Yargıtay Kararları Işığında Hukuka Aykırı Aramada Elde Edilen Delillerin Ceza Muhakemesinde Değerlendirilmesi", CHKD, 2015, Band 3, Zahl Nr. 2, S. 227 ff.

**Günther**, Ralf: "Zur strafprozessualen Erhebung von Telekommunikationsdaten - Verpflichtung zur Sachverhaltsaufklärung oder verfassungsrechtlichunkalkulierbares Wagnis?", NStZ, 2005, S. 485 ff.

**Hirsch**, Burkhard: "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822," NJOZ, 2008, S. 1907 ff.

**Hoeren**, Thomas/**Gräbig**, Johannes: "Entwicklung des Internet- und Multimediarechts im Jahr 2009", MMR-Beil., 2010, S. 1 ff.

**Hofmann**, Manfred: "Die Online-Durchsuchung - staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?", NStZ, 2005, S. 121 ff.

**Holzner**, Stefan: „Rheinland-Pfalz: Online-Durchsuchung und weitere Maßnahmen der TK-Überwachung geplant", MMR-Aktuell, 2010, 302767.

**Huber**, Bertold: "Trojaner mit Schlapphut - Heimliche „Online-Durchsuchung " nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz", NVwZ, 2007, S. 880 ff.

**Kaymaz,** Seydi: Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Auflage, 2015.

**Kemper**, Martin: "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten", ZRP, 2007, S. 105 ff.

**Kudlich,** Hans: „Zur Zulässigkeit strafprozessualer Online-Durchsuchungen", HFR, 2007, S. 202 ff.,

**Kunter**, Nurullah/**Yenisey**, Feridun/**Nuhoğlu**, Ayse: Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 16. Auflage, 2008.

**Kutscha**, Martin: "Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte", LKV, 2008, S. 481 ff.

**Kutscha**, Martin: "Verdeckte „Online –Durchsuchung" und Unverletzlichkeit der Wohnung", NJW, 2007, S. 1169 ff.

**Kutscha**, Martin: "Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung - nichts Neues aus Karlsruhe?", NJW, 2005, S. 20 ff.

**Leipold**, Klaus: "Die Online-Durchsuchung", NJW-Spezial Heft, 3/2007, S.135 f.

**Conelius**, Kai: Teil 10. Besonderheiten des Straf- und Strafprozessrechts, in: Münchener Anwaltshandbuch IT-Recht, Andreas Leupold/Silke Glossner (Herausgeber), 3. Auflage, 2013.

**Martini**, Mario: "Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts", JA, 2009, S. 839 ff.

**Möllers**, Christoph: "Wandel der Grundrechtsjudikatur Eine Analyse der Rechtsprechung des Ersten Senats des BVerfG", NJW, 2005, S. 1973 ff.

**Nazari-Khanachayi**, Arian: "Sicherheit vs. Freiheit – der moderne Rechtsstaat vor neuen Herausforderungen", JA, 2010, S. 761 ff.

**Obenhaus**, Nils: "Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft", NJW, 2010, S. 651 ff.

**Özbek**, Veli Özer/**Kanbur**, Mehmet Nihat/**Doğan**, Koray/**Bacaksız**, Pınar/ **Tepe**, İlker: Ceza Muhakemesi Hukuku, 7. Auflage, 2015.

**Öztürk**, Bahri/**Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan/**Sırma**, Özge/**Kırıt**, Yasemin F. Saygılar/**Özaydın**, Özdem/**Akcan**, Esra Alan/**Erden**, Efser: Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, 9. Auflage, 2015.

**Roggan**, Fredrik: "Das neue BKA-Gesetz- Zur weiteren Zentralizierung der deutschen Sicherheitsarchitektur", NJW, 2009, S. 257 ff.

**Rux**,Johannes: "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsgrundlagen der ‚Online-Durchsuchung'", Juristen-Zeitung, 2007, S. 285 ff.

**Sachs**, Michael/**Krings**, Thomas: "Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"", JuS, 2008, S. 481 ff.

**Schantz**, Peter: "Verfassungsrechtliche Probleme von „Online-Durchsuchungen"", KritV, 2007, S. 310 ff.

**Schäuble**, Wolfgang: "Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts", ZRP, 2007, S. 210 ff.

**Soiné**, Michael: "Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder", NVwZ, 2012, S. 1585 ff.

**Şen**, Osman Nihat: „Ceza Hukukunda Bilgisayar Araştırmaları", Ceza Hukuku Dergisi, Band 1, Zahl. Nr. 1, Oktober 2006, S. 375 ff.

**Tepe**, İlker: „Federal Alman Anayasa Mahkemesinin Online Araştırmalara İlişkin 28 Şubat 2008 Tarihinde Verdiği Karar", CHD, Band: 8, 2008, S. 177 ff.

**Thiel**, Markus: Die „Entgrenzung" der Gefahrenabwehr, Tübingen, 2011.

**Tinnefeld**, Marie-Theres: "Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner", MMR, 2007, S. 137 ff.

**Tinnefeld**, Marie-Theres/**Petri**, Thomas/**Brink**, Stefan: "Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz Eine erste Analyse und Bewertung", MMR, 2010, S. 727 ff.

**Trüg**, Gerson: "Medienarbeit der Strafjustiz – Möglichkeiten und Grenzen", NJW, 2011, S. 1040 ff.

**Ünver**, Yener/**Hakeri**, Hakan: Ceza Muhakemesi Hukuku, 13. Auflage, 2017.

**Warntjen**, Maximilian: "Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online- Durchsuchung", Jura, 2006, S. 581 ff.

**Werkmeister**, Christoph/**Pötters**, Stephan: "Anfängerklausur – Öffentliches Recht: Grundrechte – Verfassungsrechtliche Anforderungen an „Online-Durchsuchungen"", JuS, 2012, S. 223 ff.

## GERICHTLICHE ENTSCHEIDUNGEN


- Großer Strafsenat beim Kassationshof, Urteil vom 26.6.2007, Nr. E.2007/7-147, K.2007/159, abrufbar unter http://bilgibankasi.istanbulbarosu.org.tr/karar/hukuka-aykiri-arama-omutlak-delil-yasaklari-onispi-delil-yasaklari-o-degerlerin-tartimi-ilkesi/e1dM (Stand vom 09.08.2018)
- BGH-Ermittlungsrichter, Beschluss vom 25.11.2006 – 1 BGs 184/2006, MMR 2007, 174 ff.
- BVerfG, Urteil vom 03.03.2004, abrufbar unter https://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898 (Stand vom 09.08.2018)
- BGH, Beschluss vom 31.01.2007 - StB 18/06, MMR 2007, S. 237 ff.
- BGH, Beschluss vom 25.11.2006 - 1 BGs 184/06, MMR 2007, S. 174 ff.
- BVerfG, Urteil vom 27.02.2008, abrufbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (Stand vom 09.08.2018).
- BGH, Beschluss vom 31.1.2007 - StB 18/06, MMR 2007, S. 237 ff. = *BGH*, NJW 2007, S. 930.
- EGMR, Urteil vom 28.04.2005 – Buck gegen Deutschland, abrufbar unter https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-68920%22]} (Stand vom 09.08.2018)
- EGMR, Urteil vom 30.09.2014 – Prezhdarovi gegen Bulgarien, Rn. 49, abrufbar unter https://hudoc.echr.coe.int/eng?i=001-146565#{%22itemid%22:[%22001-146565%22]} (Stand vom 09.08.2018).


## INTERNET QUELLEN


- **Fauß**, Patrick: „Viren-Schwemme auf einen Klick“, in: Stern, Veröffentlichung: 05.08.2007 abrufbar unter https://www.stern.de/digital/computer/-drive-by--download-viren-schwemme-auf-einen-klick-3267556.html (Stand vom 09.08.2018).
- BGH: Online-Durchsuchung eines Computers, MMR 2007, S. 237, 239.
- **Ihlenfeld**, Jens: BGH: Verdeckte Online-Durchsuchung unzulässig, in: golem.de, Veröffentlichung: 05.02.2007, abrufbar unter http://www.golem.de/0702/50334.html (Stand vom 08.08.2018)
- DAV lehnt heimliche Onlinedurchsuchung nach wie vor ab, Redaktion FD-StrafR, Aktuelle Nachrichten, FD-StrafR 2008, 257354 abrufbar unter https://beck-online.beck.de/default.aspx?words=FD-StrafR+2008%2C+257354&btsearch.x=42&btsearch.x=0&btsearch.y=0 (Stand vom 11.10.2017)
- **Heinrich**, Bernd/**Reinbacher**, Tobias: Arbeitsblatt Nr. 19 Online-Durchsuchung Stand: 1. April 2016, abrufbar unter https://www.jura.uni-wuerzburg.de/fileadmin/02150030/19-onlinedurchsuchung.pdf (Stand vom 21.03.2018).