Björn Kruse/Mathias Grzesiek

Die Online-Durchsuchung als „digitale Allzweckwaffe“ – Zur Kritik an überbordenden Ermittlungsmethoden*

Summary

Information technologies increasingly influence our everyday lives. Tablets and smartphones have become an integral part of our daily lives. They do not only serve as means of communication but are also used to organize private and professional lives.

The remote search as an investigative measure under section 100 b of the German Code of Criminal Procedure now tries to address the shift of communication as well as data collection and retention towards information technology. On the one hand, it thereby raises questions concerning the technical possibilities and the concrete application. On the other hand the jurisprudence of the German Constitutional Court focuses on section 100 b of the German Code of Criminal Procedure and has already taken a view regarding the admissibility of remote searches. The focus is not only on the general collection of communication data. The remote search aims at enabling full access to information technology systems. Besides the infringement of the fundamental right to confidentiality and probity in information technology systems caused by the collecting and retrieving of personal data, the threat of an uncontrollable infringement to the core area of a person's private life exists due to information technology systems among other things enabling audiovisual perception of the environment. Furthermore, the obstacles to remote search are to be critically evaluated in the light of the jurisprudence of the German Constitutional Court.

Résumé

De plus en plus notre quotidien est influencé par les systèmes de traitement électroniques des données. Tablettes et smartphones sont devenus des éléments indispensables de notre vie quotidienne. Ils ne servent pas seulement à communiquer mais encore à l’organisation de notre vie privée et professionnelle.

La mesure d’instruction de la surveillance de la communication électronique, de l’utilisation de l’internet et du réseau informatique de la société selon l’article 100 du code de procédure pénale allemand tente désormais de remédier au déplacement des moyens de communication ainsi qu’au traçage 07et à la conservation des données dans les systèmes de traitement électronique et soulève ce faisant des questions con-

* Dr. Björn Kruse ist als Strafverteidiger tätig bei der Feigen Graf Rechtsanwälte Partnerschaftsgesellschaft mbB in Frankfurt am Main. Dr. Mathias Grzesiek ist als Strafverteidiger bei der Tsamikakis & Partner Rechtsanwälte mbB in Frankfurt am Main tätig. Beide Autoren sind Lehrbeauftragte am Institut für Kriminalwissenschaften und Rechtsphilosophie der Goethe-Universität Frankfurt am Main.

KritV 4/2017, DOI: 10.5771/2193-7869-2017-4-331

cernant les possibilités techniques ainsi que leur application concrète. Par ailleurs la jurisprudence du Conseil constitutionnel fédéral se focalise sur l'article 100 du code de procédure pénale allemand et a déjà pris position quant aux limites de la recevabilité de la surveillance de la communication électronique, de l'utilisation de l'internet et du réseau informatique de la société. Il n'y est pas seulement question du recouvrement général des données. La surveillance de la communication électronique, de l'utilisation de l'internet et du réseau informatique de la société doit rendre possible un accès complet aux systèmes de traitement électroniques. Outre l'empiètement sur le droit fondamental à la garantie de la confidentialité et de l'intégrité des données dans les systèmes de traitement électroniques, dû aux dégraissements et tris des données personnelles, une intervention incontrôlée menace le secteur-clé de la vie privée en ce que les systèmes de traitement électroniques permettent entre autre, la reconnaissance audiovisuelle de l'environnement. Ainsi les obstacles à la surveillance de la communication électronique, de l'utilisation de l'internet et du réseau informatique de la société sont à apprécier à la lumière de la jurisprudence du Conseil constitutionnel fédéral.

I. Einführung

Der Alltag wird zunehmend von informationstechnischen Systemen aller Art beeinflusst. Tablets und Smartphones sind zum festen Bestandteil des täglichen Lebens geworden. Sie dienen nicht nur der Kommunikation, sondern auch der Organisation der privaten und beruflichen Lebensführung.

Die Ermittlungsmaßnahme der Online-Durchsuchung nach § 100 b StPO versucht nunmehr der Verlagerung von Kommunikationswegen und der Erfassung und Aufbewahrung von Daten auf informationstechnische Systeme zu begegnen und wirft damit einerseits Fragen zu technischen Möglichkeiten sowie zur konkreten Umsetzung auf. Andererseits steht § 100 b StPO im Fokus der Rechtsprechung des Bundesverfassungsgerichts, welches sich bereits zu den Grenzen der Zulässigkeit einer Online-Durchsuchung positionierte. Dabei steht nicht nur die generelle Erhebung von Kommunikationsdaten im Mittelpunkt der Betrachtung.

Mit der Online-Durchsuchung soll der vollständige Zugriff auf informationstechnische Systeme ermöglicht werden. Neben dem mit dem Abschöpfen und Auslesen von persönlichen Daten verbundenen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme droht ein unkontrollierbarer Eingriff in den Kernbereich privater Lebensgestaltung, da informationstechnische Systeme unter anderem auch die audiovisuelle Wahrnehmung der Umgebung ermöglichen. Darüber hinaus sind die Hürden für eine Online-Durchsuchung im Lichte der Rechtsprechung des Bundesverfassungsgerichts kritisch zu würdigen.

II. § 100 b StPO – ein „Mehr" zu § 102 StPO

Die „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und jugendgerichtlichen Verfahrens" äußerte sich im

Rahmen der Quellen-Telekommunikationsüberwachung[1] hinsichtlich der Ermächtigung für den Zugriff auf informationstechnische Systeme noch zurückhaltend.[2] Der 69. Deutsche Juristentag forderte hingegen eine grundlegende Anpassung strafprozessualer Ermittlungsmaßnahmen, insbesondere hinsichtlich der Online-Durchsuchung.[3] Schließlich erkannte auch der Gesetzgeber die mit dem technischen Fortschritt verbundenen Herausforderungen für Strafverfolger und nahm sich der Thematik an,[4] wobei das Gesetzgebungsverfahren zu erheblicher Kritik führte.[5] Dies hat zu einem technischen und rechtswissenschaftlichen Diskurs geführt, der nicht zuletzt auf dem 34. Herbstkolloquium der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltsvereins im Rahmen des „IT-Forums“ ausgetragen wurde.

Mobile Endgeräte wie Smartphones, Tablets und Laptops werden zunehmend zur Speicherung persönlicher Daten genutzt. Während Briefe, Dokumente oder andere Unterlagen üblicherweise im Regal oder in Schubladen gelagert werden und elektronische Daten vor nicht allzu langer Zeit ausschließlich auf lokalen Speichermedien wie Festplatten oder USB-Sticks gesichert wurden, werden heute zunehmend externe Speichermöglichkeiten wie sog. Clouds zur Datenaufbewahrung genutzt. Beim sog. Cloud-Computing werden vom Dienstanbieter Speicherplatz, Rechenleistung oder Software über das Internet zur Verfügung gestellt. Die hierfür bereitgestellten Server sind nicht selten im Ausland untergebracht. Hinter den Cloud-Systemen verbirgt sich oftmals eine komplexe Struktur, die es den Ermittlungsbehörden selbst bei unmittelbarem Zugriff erschwert, diese Daten – anders als physische Dokumente – sicherzustellen.

Die Rechtsgrundlage für die Online-Durchsuchung wirft eine Reihe technischer, praktischer und insbesondere verfassungsrechtlicher Fragen auf. Dabei könnte man zunächst eine ketzerische Gegenfrage stellen: Besteht ein Unterschied, ob eine Durchsuchung nach § 102 StPO durchgeführt wird, um den Computer des Beschuldigten zu beschlagnahmen, oder sich die Ermittlungsbehörden im Wege der Online-Durchsu-

1 Siehe dazu *Sieber*, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C 103 ff.

2 „*Technisch muss sichergestellt werden, dass mit der für die Quellen-TKÜ eingesetzten Software nur Zugriff auf Inhalt und Umstände der laufenden Telekommunikation genommen werden kann, nicht aber auf die auf dem überwachten Endgerät gespeicherten Daten*“, Bericht der Expertenkommission zur Reform der StPO, 74.

3 Der 69. DJT bescheinigte der Zivilgesellschaft eine Abhängigkeit von informationstechnischen Systemen und beschloss mit 70:4:1 Stimmen eine „grundlegende Anpassung“ des materiellen und strafprozessualen Systems, vgl. Beschlüsse Deutscher Juristentag 2012, abrufbar unter: http://www.djt-net.de/beschluesse/beschluesse.pdf, 10; Die Zulässigkeit der Online-Durchsuchung wurde mit Verweis auf die Einhaltung der durch BVerfGE 120, 274 vorgegebenen Eingriffsschwellen mit 47:27:5 Stimmen angenommen, 11; Das Gutachten von *Siebert* war dagegen kritisch und mahnte zur Vorsicht im Umgang mit der Online-Durchsuchung, *ders.*, (Fn. 1), C 108 f.

4 Formulierungshilfe der Bundesregierung für einen Änderungsantrag, Ausschussdrucksache 18(6)334 zu BT-Drucksache 18/11272 (Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze).

5 Kritisch *Roggan*, Die strafprozessuale Quellen-TKÜ und Online Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, 821 ff.; *Beukelmann*, Online-Durchsuchung und Quellen-TKÜ, in: NJW-Spezial 2017, 440.

chung nach § 100 b StPO über das Internet in den Computer hereinschleichen und die Daten abschöpfen? Für eine Ungleichheit der Maßnahmen spricht bereits die Heimlichkeit der Online-Durchsuchung, da der Beschuldigte weder Kenntnis von der Ausführung noch von der Dauer der Online-Durchsuchung erlangt. Denn der Eingriff kann „*nicht nur einmalig und punktuell stattfinden, sondern sich auch über einen längeren Zeitraum erstrecken*“.[6] Zudem bietet die Online-Durchsuchung den Ermittlungsbehörden umfassende technische Möglichkeiten,[7] die von der Eingriffsintensität selbst über die akustische Wohnraumüberwachung – den *großen Lauschangriff* – nach § 100 c StPO hinausgehen.

Vor diesem Hintergrund liegt der Gedanke nicht fern, dass der Gesetzgeber hier eine digitale „Allzweckwaffe“ geschaffen hat. Die dafür erforderliche Hardware in Form des informatorischen Systems, trägt der Beschuldigte – beispielsweise durch sein Smartphone – bereits freiwillig bei sich.

III. Technischer Hintergrund

Die Darstellung der Zugriffsmöglichkeiten auf informationstechnische Systeme, ist erforderlich, um die verfassungsrechtliche Tragweite der Online-Durchsuchung zu erfassen.

1. Zugriff auf informationstechnische Systeme im Rahmen der Online-Durchsuchung

Die Gesetzesbegründung definiert die Online-Durchsuchung als verdeckten staatlichen Zugriff auf ein fremdes informationstechnisches System mit dem Ziel, dessen Nutzung zu überwachen und gespeicherte Inhalte aufzuzeichnen.[8] Ein informationstechnisches System besteht aus Hard- und Software sowie aus Daten, die der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen dienen.[9] Mit der Online-Durchsuchung ist neben der Durchsicht der auf dem System gespeicherten Daten auch die Online-Überwachung möglich.[10] Die technischen Möglichkeiten, welche eine Online-Überwachung bietet, sind vielfältig. Exemplarisch sollen einige für die Ermittlungsarbeit relevanten Möglichkeiten dargestellt werden:

- Mittels des Einsatzes eines sog. Keyloggers (dt. „Tasten-Protokollierer“) können Passworteingaben protokolliert und an die Ermittlungsbehörden weitergeleitet werden. So kann beispielsweise der Zugriff auf ein Cloud-System oder einen im Ausland befindlichen Server erlangt werden.
- Ebenfalls ist ein Zugriff auf Hardware-Schnittstellen möglich. So können beispielsweise Screenshots (dt. Bildschirmfotos) oder Screencasts (dt. Video-Auf-

6 Ausschussdrucksache 18(6)334, 23.
7 Auf diese wird im Folgenden weiter eingegangen.
8 Vgl. hierzu BT-Drucksache 18/12785, 54.
9 Bundesministerium des Inneren, Fragenkatalog BMJ, abrufbar unter: http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, 2.
10 Fragenkatalog BMJ, (Fn. 9), 6 f.

zeichnungen des Bildschirms) angefertigt werden, um eine E-Mail oder eine Textnachricht bereits bei der Erstellung und damit noch vor dem Abspeichern abzugreifen.
- Der Fernzugriff auf die Kamera und das Mikrofon kann zu einer temporären oder dauerhaften audiovisuellen Überwachung genutzt werden.[11] In diesem Zusammenhang kann dann von einem „*großen Spähangriff*“ gesprochen werden.[12]
- Mittels des Zugriffs auf den GPS-Empfänger, der bei modernen Smartphones, Tabletts und Fitnesstrackern zum Standard gehört, können exakte Positionsdaten bestimmt und Bewegungsprofile erstellt werden.

Der Begriff des informationstechnischen Systems ist nicht auf die zur Online-Kommunikation üblicherweise genutzten Endgeräte wie Smartphones, Tablets und Laptops begrenzt. Es sind vielmehr jegliche Arten von elektronischen datenverarbeitenden Systemen erfasst.[13] Hierunter fallen beispielsweise auch Smart-TVs oder „intelligente“ Sprachassistenten (Google Home oder Amazon Echo). Durch die Übernahme eines solchen Geräts könnte eine dauerhafte akustische Überwachung des Wohnraumes erfolgen. Auch eine komplette Fernsteuerung des informationstechnischen Systems ist technisch möglich. Zu denken ist an Smart Home-Systeme, die dem Privatanwender die Überwachung und Steuerung des eigenen Heims aus der Ferne ermöglichen. Durch die Übernahme der Kontrolle über ein solches System kann neben der Überwachung auch die Durchsuchung der Wohnung vorbereitet werden, indem das Licht deaktiviert und die Eingangstür entriegelt wird. Ebenfalls könnte die Kontrolle über ein mit zahlreichen elektronischen Fahrerassistenzsystemen ausgestatteten PKW übernommen werden, um beispielsweise das Notbremssystem auszulösen und das Fahrzeug zum sofortigen Halt zu zwingen. Kraftfahrzeuge, die das autonome Fahren beherrschen, könnten – so zumindest in der Theorie – verriegelt sowie an einen anderen Zielort navigiert werden. Was auf den ersten Blick nach Science-Fiction klingt, ist technisch bereits heute durchführbar.

2. Die Quellen-TKÜ als „kleine“ Online Durchsuchung

Die Verständigung unter Abwesenden wird immer seltener mittels klassischer Telefonie abgewickelt, sondern verlagert sich unter anderem durch den Einsatz von sog. Instant-Messaging-Diensten zunehmend auf das Internet. Das herkömmliche Telefonnetz wird für die Konversation von Morgen kaum noch von nennenswerter Bedeutung sein. Hierauf hat der Gesetzgeber reagiert.

Von der Online-Durchsuchung nach § 100 b StPO lässt sich die ebenfalls eingeführte und in § 100 a Abs. 1 S. 2 StPO kodifizierte Quellen-TKÜ unterscheiden. Dies gilt jedenfalls für den rechtlichen Aspekt. Was den technischen Aspekt angeht, sind die Unterschiede, trotz der in der Gesetzesbegründung differenzierend formulierten Zielrichtung, nur marginal. Nach dem Willen des Gesetzgebers soll die für die Quellen-

11 *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, 2 u.15.
12 So *Beukelmann*, (Fn. 5), 440.
13 Fragenkatalog BMJ, (Fn. 9), 3.

TKÜ verwendete Software auf das Auslesen und Weiterleiten von Kommunikation begrenzt sein.[14] Die auf dem Zielgerät gespeicherten Nachrichten dürfen nicht erhoben werden, wenn sie nicht mehr als „aktuelle Kommunikation" gelten. Dagegen ist die für die Online-Durchsuchung vorgesehene Software nicht auf den Zweck der Kommunikationsüberwachung beschränkt. Vielmehr sollen alle auf dem System gespeicherten Inhalte erhoben sowie das gesamte Nutzungsverhalten einer Person überwacht werden.[15]

Bei einer „herkömmlichen" Telekommunikationsüberwachung leiten Telefonanbieter Telefon- oder Mobilfunkgespräche, Kurzmitteilungen (SMS), Telefaxe, E-Mails oder sonstigen Kommunikationsdaten der Zielperson an die Ermittlungsbehörden weiter. Da der sonstige Datenverkehr hierbei in aller Regel unverschlüsselt erfolgt, ist den Ermittlern ein unmittelbares Abhören bzw. Mitlesen unter Überwindung niedriger Hürden möglich. Nutzt die Zielperson für die Kommunikation jedoch sog. Instant-Messaging-Dienste (wie beispielsweise WhatsApp, Threema, Viber oder Facebook-Messenger), so kommt eine sog. Ende-zu-Ende-Verschlüsselung zum Einsatz.[16] Diese verschlüsselt die vom Absender erstellte Nachricht auf seinem Endgerät vor dem Versenden und überträgt sie dann in verschlüsselter Form über alle Übertragungsstationen hinweg bis zum Empfänger. Erst wenn die Nachricht dort eingegangen ist, wird sie von der auf dem Empfängergerät befindlichen Software entschlüsselt und somit lesbar. Die kryptografischen Schlüssel, die für die Verschlüsselung und Entschlüsselung verwendet werden, sind exklusiv auf den Endgeräten gespeichert und können auch nicht vom Dienstanbieter herausverlangt werden. Selbst wenn der Datenverkehr ausgeleitet wird, liegt den Ermittlungsbehörden die Nachricht lediglich in verschlüsselter Form vor. Ein Dechiffrieren der verschlüsselten Nachricht ist nicht möglich, da die Art von Verschlüsselung vor dem Hintergrund derzeitiger Rechenleistungskapazitäten und verfügbarer Algorithmen als „unknackbar" gilt.[17] Selbiges gilt für den Austausch von verschlüsselten Bildern, Videos oder aufgezeichneten Sprachnachrichten sowie für die verschlüsselte Internettelefonie.[18] Die Quellen-TKÜ kommt daher bereits vor dem eigentlichen Kommunikationsvorgang zum Einsatz. Das Kommunikationsgerät des Betroffenen wird zunächst infiltriert, um anschließend eine Software einzuspeisen, welche die Nachricht des Absenders noch vor der Verschlüsselung an die Ermittlungsbehörden überträgt.[19]

Mithin haben Quellen-TKÜ und Online-Durchsuchung gemein, dass das informationstechnische System der Zielperson für die Überwachungs- bzw. die Durchsuchungsmaßnahme zunächst infiltriert werden muss, um anschließend die einzusetzende Spionagesoftware auf dem Endgerät zu installieren. Es ist daher auch in techni-

14 BT-Drucksache 18/12785, 50.
15 BT-Drucksache 18/12785, 54.
16 Zur Ende-zu-Ende-Verschlüsselung beim Messenger-Dienst WhatsApp siehe: *Beuth*, Die WhatsApp-Revolution, Die Zeit v. 6.4.2016, abrufbar unter: http://www.zeit.de/digital/datenschutz/2016-04/whatsapp-ende-zu-ende-verschluesselung-analyse.
17 BT-Drucksache 18/12785, 48.
18 Auch als „IP-Telefonie" oder „Voice-over-IP" bezeichnet.
19 BT-Drucksache 18/12785, 49.

scher Hinsicht zutreffend, dass die Quellen-TKÜ eine „kleine Onlinedurchsuchung“ darstellt.[20]

3. Infiltration und Übernahme des Endgeräts durch den Staatstrojaner

Wie die Infiltration und Übernahme des Zielgeräts technisch realisiert werden soll, geht weder aus dem Gesetzestext noch aus der dazugehörigen Gesetzesbegründung hervor.[21] Nach derzeitigem Stand kann davon ausgegangen werden, dass eine sog. Remote Forensic Software (kurz: RFS) zum Einsatz kommt.[22] Hierbei handelt es sich technisch um ein sog. Trojanisches Pferd. Dies bezeichnet eine Software, die als legitime Anwendung getarnt auf das Endgerät des Nutzers geladen und dort unbemerkt aktiviert wird.[23] Die RFS wird auch häufig als „Staatstrojaner“ oder „Bundestrojaner“ bezeichnet.

Der Staatstrojaner kann auf ein informationstechnisches System gelangen, indem ein für den Austausch von Daten vorgesehener Weg missbraucht wird. Handelt es sich bei dem Zielgerät um einen PC oder Laptop, kann der Trojaner mittels eines sog. Computerwurms, der sich beispielsweise im Anhang einer E-Mail oder auf einem USB-Stick befindet, auf das Gerät transportiert werden. Anschließend wird die Spionagesoftware durch das Öffnen des E-Mail-Anhangs bzw. den Zugriff auf den USB-Stick gestartet. Bei Smartphones gelangt der Staatstrojaner beispielsweise durch den sog. Instant-Messaging-Wurm auf das Endgerät. Hierbei wird eine Nachricht mit einem Link zu einer augenscheinlich harmlosen Datei geschickt, welche den Staatstrojaner enthält. Die Übertragung auf das informationstechnische System mittels eines Wurms setzt jedoch stets die Mithilfe des Anwenders voraus, da dieser die infizierte Datei herunterladen und starten muss.

Eine gänzlich andere Methode der Einschleusung des Staatstrojaners ist die Ausnutzung sicherheitsrelevanter Schwachstellen des Systems, die bei der Entwicklung der Software entstanden sind. Dies wird auch als „Zero-Day-Exploit“ bezeichnet.[24] Bei diesem Verfahren wird eine dem Softwarehersteller nicht bekannte Sicherheitslücke ausgenutzt, um die Schadsoftware übertragen und installieren zu können, bevor die Schwachstelle bekannt und mittels eines Patches geschlossen wurde.

Ein sog. lokaler Exploit – der ähnlich wie ein Computerwurm die Unerfahrenheit des Nutzers voraussetzt – wird durch das Öffnen eines harmlosen PDF-Dokuments oder einer Bilddatei gestartet. Anschließend wird die Software auf das System heruntergeladen und ausgeführt. Bei den gefährlicheren sog. Remote-Exploits gelangt der für die Installation der Schadsoftware notwendige Code über das Netzwerk auf das Zielsystem, ohne dass die Zielperson unbeabsichtigt Hilfestellung geben muss.[25]

Es ist anzunehmen, dass der von den Ermittlungsbehörden eingesetzte Staatstrojaner aufgrund der notwendigen Mitwirkung der Zielperson und dem mit Verschicken

20 BT-Drucksache 18/12785, 50.
21 *Buermeyer*, (Fn.11), 20.
22 Fragenkatalog BMJ, (Fn. 9), 1.
23 Siehe detaillierter: https://www.kaspersky.de/resource-center/threats/trojans.
24 Siehe dazu https://www.kaspersky.de/resource-center/definitions/zero-day-exploit.
25 Siehe dazu https://www.hessen-it.de/sicherheit/Inhalte/Gefahren/Netzwerk/Exploits.html.

von E-Mails oder Links verbundenen Entdeckungsrisiko eher auf die zweite Methode, dem Ausnutzen von Exploits, zurückgreifen werden, um auf das zu überwachende oder zu durchsuchende informationstechnische Gerät zu infiltrieren.

Ist der Staatstrojaner auf dem Zielsystem geladen, wird er automatisiert gestartet und installiert. Anschließend wird das informationstechnische System durchsucht bzw. die Telekommunikation unverschlüsselt weitergeleitet. Die Steuerung des Staatstrojaners und die Übertragung der abgeschöpften Daten an die Ermittlungsbehörde erfolgen über die aktive Internetverbindung des Geräts. Sind die Daten bei der Behörde angelangt, werden sie gespeichert und können im Anschluss von den Ermittlern ausgewertet werden. Durch die Deinstallation des Staatstrojaners wird die Maßnahme letztlich beendet.[26]

Aus Medienberichten geht hervor, dass der eigens für die Online-Durchsuchung vom BKA in Auftrag gegebene Staatstrojaner bereits seit 2014 einsatzbereit ist.[27] Seit dem Jahr 2016 soll nun auch die für die Quellen-TKÜ zu verwendende Ermittlungssoftware zur Verfügung stehen.[28] Aus Gründen der Effektivität und Kostenersparnis kann davon ausgegangen werden, dass ein Großteil des bei der Entwicklung der Durchsuchungssoftware entstandenen Quellcodes wiederverwertet wurde und die für die Quellen-TKÜ verwendete Software eine im Funktionsumfang limitierte Version der für die Online-Durchsuchung genutzten Programmvariante ist. Dies ist naheliegend, da sich die beiden Ermittlungsprogramme lediglich anhand des dem Benutzer zur Verfügung stehenden Funktionsumfangs unterscheiden.

4. Missbrauchsmöglichkeiten für den Anwender und Gefahren für die allgemeine IT-Sicherheit

Bei der technischen Umsetzung der Online-Durchsuchung sind den Ermittlungsbehörden vom Gesetzgeber weder Vorgaben auferlegt noch Grenzen gesetzt worden. Neben den sich hieraus ergebenen Fragen, zum Beispiel welche Qualitätsstandards die einzusetzende Spionage-Software erfüllen muss und wer für die Einhaltung zuständig ist, bringt die Definitionsscheu des Gesetzgebers erhebliche Missbrauchsgefahren mit sich.

Eine im Jahr 2011 vom Chaos Computer Club durchgeführte Analyse des für den Einsatz zur Quellen-TKÜ entworfenen Staatstrojaner-Prototypen zeigte, dass die damals getestete Software erhebliche programmiertechnische Defizite aufwies, die teilweise auch sicherheitsrelevant waren. Zudem ergab die Analyse, dass der Funktionsumfang des Programms weiter war, als vorgesehen und kein Versuch unternommen wurde, diesen auf den vorgesehenen Zweck, das Ausspähen der Telekommunikation,

26 *Kohlmann,* Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz, 1. Aufl., 2012, 45.

27 https://www.heise.de/newsticker/meldung/Bundesregierung-Software-zur-Online-Durchsuchung-ist-einsatzbereit-2293017.html.

28 http://www.zeit.de/digital/datenschutz/2016-02/ueberwachung-bundestrojaner-bka-einsatzbereit.

zu beschränken.[29] Durch den Einsatz einer solchen Spionage-Software wären Ermittlern Grundrechtseingriffe möglich, zu denen sie weder befugt noch ermächtigt sind. Der Einsatz ist damit risikoreicher als die herkömmliche Erlangung von Kommunikationsdaten. Die technische Beschränkung des Funktionsumfangs auf den jeweiligen Einsatzzweck ist jedoch zwingend, um Missbrauchsmöglichkeiten zu verhindern und den effektiven Schutz von Grundrechten gewährleisten zu können.

Davon abgesehen wirft die Ermächtigung zur Online-Durchsuchung grundlegende Fragen zur IT-Sicherheit auf.[30] Da das Vorhandensein einer Software-Schwachstelle Voraussetzung für die Infiltration mittels eines Exploits ist,[31] haben die Behörden ein erhebliches Interesse daran, dass diese Schwachstellen unentdeckt bleiben. Sobald der jeweilige Software-Hersteller von einer Sicherheitslücke erfährt, wird er diese in der Regel schließen.[32] Hierdurch verliert sie jedoch ihren Nutzen für die Umsetzung der Maßnahmen nach §§ 100 a, 100 b StPO.

Aufgrund der Vielzahl der vorhandenen IT-Systeme reicht den Ermittlern ein einziger Exploit aus. Denn jeder Exploit ist auf eine spezifische Software zugeschnitten. Um die Infiltration wirkungsvoll umzusetzen, müssen die Ermittlungsbehörden über Exploits für alle gängigen Softwarelösungen verfügen.[33] Um an Exploits heranzukommen, müssen diese zunächst auf dem IT-Schwarzmarkt – beispielsweise dem Darknet – angekauft werden. Abgesehen von der Frage, ob ein staatlicher Ankauf von Software-Schwachstellen überhaupt rechtmäßig ist, kurbelt das staatliche Kaufinteresse den Markt für Sicherheitslücken an, was wiederum zu einer Verstärkung der Bemühungen von Hackern führt, Schwachstellen aufzudecken und deren Bekanntwerden zu verhindern. Auch führt dies unter Umständen sogar dazu, dass Behörden das Bekanntwerden der von ihnen erworbenen und genutzten Sicherheitslücken aktiv verhindern werden.[34] Zur Förderung der IT-Sicherheit hat sich die Bundesregierung jedoch kürzlich erst bekannt.[35] Durch die Einführung der Online-Durchsuchung und Quellen-TKÜ mag zwar der Effektivität und Praxistauglichkeit der strafrechtlichen Ermittlung geholfen sein, diese ist jedoch mit der Gefahr eines gravierenden Verlusts an IT-Sicherheit verbunden.

29 Vgl. *Chaos Computer Club*, Analyse einer Regierungs-Malware, Bericht v. 8.10.2011, 2 u. 11.

30 *Buermeyer*, (Fn.11), 3, 22; ebenso *Gazeas*, Stellungnahme im Rahmen der öffentlichen Anhörung im Hauptausschuss u.a. zum Gesetz zur Änderung des Polizeigesetzes (Drs. 16/2741) vom 2.11.2017, 10.

31 Vgl. *Chaos Computer Club*, Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung, Stellungnahme v. 31.5.2017, 6.

32 *Chaos Computer Club*, (Fn. 31), 6; *Buermeyer*, (Fn.11), 3, 22.

33 *Buermeyer*, (Fn.11), 21.

34 Vgl. *Roggan*, (Fn. 5), 828 f.

35 Cyber-Sicherheitsstrategie für Deutschland 2016, abzurufen auf http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html.

IV. Online-Durchsuchung im Lichte der Rechtsprechung des Bundesgerichtshofs sowie des Bundesverfassungsgerichts

Der Kodifizierung der Online-Durchsuchung sind bereits wegweisende Entscheidungen des Bundesverfassungsgerichts vorausgegangen, die dem Gesetzgeber den verfassungsrechtlichen Rahmen für den Eingriff in informationstechnische Systeme vorgab und das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG entsprechend ausprägten.

Das Gefahrenabwehrrecht der Länder sah es teilweise bereits vor, Gefahren für Leib, Leben oder Freiheit durch den Zugriff auf informationstechnische Systemen abzuwenden.[36] Auch im Rahmen der Terrorismusbekämpfung durch das BKA, lässt § 20 k BKAG verdeckte Eingriffe in informationstechnische Systeme zu. Nunmehr wurde auch mit § 100 b StPO eine Rechtsgrundlage für die Online-Durchsuchung im Rahmen der „ordentlichen" Strafverfolgung geschaffen.

Der schleichende Prozess vom „Terrorismusstrafrecht" in die „ordentliche" Strafverfolgung beschreibt eine Entwicklung, die vielfach vorskizziert wurde.[37] Bereits dadurch hebt sich die Bedeutung der Kodifizierung der Online-Durchsuchung in § 100 b StPO hervor. Damit befindet sich die Online-Durchsuchung auch in bester Gesellschaft. Denn § 100 b StPO reiht sich letztlich in eine Kette ausweitender Ermittlungsbefugnisse der Strafverfolger im Rahmen der StPO ein.[38] Diese Entwicklung hat auch das Bundesverfassungsgericht teilweise mitgetragen, da es zwar einerseits rechtsstaatliche Eckpfeiler in den ausufernden Ermittlungsmaßnahmen durch die Entwicklung eines besonderen Grundrechts einschlug, gleichwohl jedoch auch die verfassungsrechtliche Zulässigkeit der Maßnahmen – bei Berücksichtigung enger rechtsstaatlicher Grundsätze – proklamierte und insofern den rechtspolitischen Kurs verfassungsrechtlich auch absegnete. Die Rechtsprechung des Bundesverfassungsgerichts ist jedoch in diesem Zusammenhang mit Augenmaß zu betrachten.

1. Die „Gesetzeslücke" vor § 100 b StPO in der Rechtsprechung des Bundesgerichtshofs

Der Bundesgerichtshof entschied am 25. November 2006 über den Antrag der Generalbundesanwältin, gemäß §§ 102, 105, 94, 98, 169 StPO die Durchsuchung des von

36 Siehe § 15 b HSOG (Hessen) in der Fassung vom 4. Mai 2017; Art. 34 a PAG (Bayern) in der Fassung vom 1. August 2017.

37 *Albrecht*, Der Weg in die Sicherheitsgesellschaft, 2010, 671; *Mosfer*, Fragilitäten des Rechtsstaates seit dem 11. September 2001 im Spiegel der Rechtsprechung des Bundesverfassungsgerichts, 2015, 197. *Naucke* begegnet dieser „zweckgerichteten Strafgesetzlichkeit" mit dem „negativen Strafrecht" als „Verbrechensbekämpfungsbegrenzungsrecht" mit „staatskritischen Absolutheitsregeln", siehe *ders.*, Negatives Strafrecht, 2015, 40 m.w.N.

38 Zuletzt: Quellen-TKÜ § 100 a StPO, Wegfall des Richtervorbehalts bei § 81 a StPO, Erscheinungspflicht für Zeugen 163 Abs. 3 StPO.

dem Beschuldigten benutzten PCs/Laptops und deren Beschlagnahme anzuordnen.[39] Der Ermittlungsrichter des Bundesgerichtshofs befand die Ausforschung des Computers als strafprozessual unzulässig, da es sich „*um einen schwerwiegenden Eingriff in das den persönlichen Freiheitsrechten zuzuordnende Recht auf informationelle Selbstbestimmung*“ handele. Insbesondere fehle es an einer gesetzlichen Grundlage, da theoretisch einschlägige Ermächtigungsgrundlagen nicht eingreifen würden. Der allgemeine Ermittlungsauftrag nach §§ 152 Abs. 2, 163 StPO biete keine Grundlage für Eingriffe in grundrechtlich geschützte Freiheitsrechte. Telekommunikationsvorgänge könnten insoweit nur „*unter Umständen durch Zufall tangiert*“ sein, weshalb § 100 a StPO nicht in Betracht käme. Letztlich sei § 102 StPO auch nicht einschlägig, da die Durchsuchung grundsätzlich auf Offenheit angelegt und körperlicher Natur sei. Auch eine entsprechende Anwendung des § 102 StPO komme nicht in Betracht, da dies auch bei weitester Auslegung keine Rechtsgrundlage zur heimlichen Computerausforschung biete und eine analoge Anwendung nach Art. 103 Abs. 2 GG sowie § 1 StGB verwehrt sei.

2. Bundesverfassungsgericht, Urteil vom 27. Februar 2008 – 1 BvR 370/07

Das Bundesverfassungsgericht befasste sich bereits im Jahr 2008 erstmals mit der Online-Durchsuchung. Anlass waren Präventionsmaßnahmen gemäß § 5 Abs. 2 Nr. 11 S. 1 Alt. 2 NWVerfSchG (Verfassungsschutzgesetz des Landes Nordrheinwestfahlen).

Das Bundesverfassungsgericht statuierte ein seinerzeit neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, als Ausprägung des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Diesem Grundrecht kommt insoweit eine „lückenschließende Funktion“ zu, um der Gefährdung zu begegnen, die aufgrund eines „*wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse*“ entstehen kann.[40] Diese entwickelte Ausprägung des allgemeinen Persönlichkeitsrechts schützt nach der Auffassung des Bundesverfassungsgerichts vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie etwa Art. 10 oder Art. 13 GG sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist.

Das Telekommunikationsgeheimnis nach Art. 10 GG gewährleistet demnach die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs und erfasst auch Kommunikationsdienste des Internets.[41] Für das Merkmal der Telekommunikation kommt es nach den Feststellungen des Bundesverfassungsgerichts weder auf die technische Umsetzung noch auf deren Inhalt und Empfängerkreis an.[42] Art. 10 GG entfaltet in den üblichen Fällen der On-

39 *BGH* BeckRS 2007, 00295; siehe auch *BGH* BeckRS 2007, 000296, dazu *Jahn/Kudlich*, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, in: JR 2007, 57 ff.; siehe auch BGH NJW 2007, 930 ff. mit zustimmender Anmerkung *Hamm*.

40 *BVerfG* NJW 2008, 822 (824), siehe Besprechung *Kudlich, in:* JA 2008, 475 ff.

41 *BVerfG* NJW 2008, 822 (824) mit Verweis auf *BVerfG* NJW 2005, 2603 ff.

42 Siehe zum Begriff „Telekommunikation“ *BVerfG* NJW 2016, 3508 (3510), mit kritischer Anmerkung *Eidam*.

line-Durchsuchung jedoch keine Wirkung, da der Eingriff in informationstechnische Systeme nicht zwingend auch dem Eingriff in einen Kommunikationsvorgang gleich kommt. So etwa, wenn das informationstechnische System offline ist und keine Kommunikation mit anderen Systemen besteht. Dann wird folglich nur auf den gespeicherten Inhalt und eben nicht auf eine räumlich distanzierte Kommunikation eingewirkt.[43] Klarstellend entfaltet Art. 10 GG seinen Schutzbereich auf Inhalte und Umstände der laufenden Telekommunikation. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt.[44] Das Bundesverfassungsgericht erkannte, dass die Online-Durchsuchung jedoch weit über die Infiltration der Telekommunikation im Sinne der Quellen-TKÜ hinausgeht, da auch auf Daten zugegriffen werden könne, die keinen Bezug zu einer telekommunikativen Nutzung aufweisen.[45]

Auch das Grundrecht der Unverletzlichkeit der Wohnung gemäß Art. 13 GG gewährleistet keinen Schutz vor staatlichem Zugriff im Rahmen der Online-Durchsuchung. Der Schutzbereich umfasst das Interesse der Entfaltung der Persönlichkeit im elementaren Lebensraum und belässt nach dem Bundesverfassungsgericht Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme. Maßgeblich ist deshalb, dass der Eingriff unabhängig vom Standort erfolgen kann, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren, da die räumliche Privatsphäre unberührt bleibt.[46]

Das Bundesverfassungsgericht begründet das Grundrecht auf Unversehrtheit informationstechnischer Systeme mit einer neuen Gefährdung der Persönlichkeit, die auf der Überlegung einer digitalen Persönlichkeitsentfaltung gründet.[47]

> *„Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.“*[48]

Demnach trägt das Recht auf informationelle Selbstbestimmung der digitalen Persönlichkeitsgefährdung nicht vollständig Rechnung, da der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Deshalb bewahrt das Grundrecht auf Unversehrtheit informationstechnischer Anlagen auch den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik, die auf dem informationstechnischen System vorhanden ist, und nicht nur einzelne Kommunikationsvorgänge oder gespeicherte Daten.[49]

---

43 *BVerfG* NJW 2008, 822 (825).
44 Zum Umfang des Schutzbereichs von Art. 10 GG *BVerfG* NStZ 2006, 641 (642) mit Anmerkung *Günther*.
45 *BVerfG* NJW 2008, 822 (825 f.).
46 *BVerfG* NJW 2008, 822 (826).
47 *BVerfG* NJW 2008, 822 (824).
48 *BVerfG* NJW 2008, 822 (825).
49 *BVerfG* NJW 2008, 822 (827).

Das Bundesverfassungsgericht zeichnete im Rahmen der Online-Durchsuchung eine entscheidende Linie, die die Anforderungen an die Durchführung konkretisierte: Ein Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

> *„darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. 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. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.“*[50]

Das Bundesverfassungsgericht erklärte § 5 Abs. 2 Nr. 11 NWVerfSchG für verfassungswidrig und nichtig, da es den Anforderungen der Verhältnismäßigkeit nicht entsprach und keine konkrete Gefahr für ein überragend wichtiges Rechtsgut voraussetzte. Gleichwohl statuierte das Bundesverfassungsgericht hierdurch, dass das Grundrecht auf Unversehrtheit informationstechnischer Anlagen nicht schrankenlos ist und Eingriffe sowohl zu präventiven, als auch zu repressiven Zwecken gerechtfertigt sein können.[51] Damit ebnete das Bundesverfassungsgericht bereits im Jahr 2008 auch den Weg für eine künftige gesetzliche Ermächtigungsnorm und die Kodifizierung der Online-Durchsuchung.

3. Bundesverfassungsgericht, Urteil vom 20. April 2016 – 1 BvR 966/09

Es folgte die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2016 zur Zulässigkeit von § 20 k BKAG im Rahmen der Bekämpfung des internationalen Terrorismus.[52] Gemäß § 20 k BKAG darf das Bundeskriminalamt als Präventivmaßnahme ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben.

Das Bundesverfassungsgericht stellte fest, dass § 20 k BKAG in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – als digitale Ausprägung der freien Persönlichkeitsentfaltung – eingreift. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf Daten und damit insbesondere vor Online-Durchsuchungen, mit denen Computer und sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden.[53]

50 *BVerfG* NJW 2008, 822 (831).
51 *BVerfG* NJW 2008, 822 (827).
52 *BVerfG* NJW 2016, 1781 ff.
53 *BVerfG* NJW 2016, 1781 (1794).

> *„Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar."*[54]

Das Bundesverfassungsgericht erkannte, dass § 20 k BKAG einer verfassungskonformen Auslegung noch zugänglich ist und insgesamt auch dem Verhältnismäßigkeitsgrundsatz genügt, da die durch den Zugriff bedingten Veränderungen an dem informationstechnischen System minimiert werden, um deren Nutzbarkeit durch Dritte zu vermeiden und sie nach Beendigung der Maßnahme soweit möglich rückgängig zu machen. Der Umstand, dass Folgeschäden nicht auszuschließen sind, begründet demnach noch keine Unverhältnismäßigkeit.[55]

Im Einklang mit der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 sind strenge Anforderungen an die tatsächlichen Anhaltspunkte für ein im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut zu stellen, die jedoch nach der Ansicht des Bundesverfassungsgerichts durch § 20 k Abs. 1 BKAG gewahrt werden.[56] Demnach muss eine Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit vorliegen, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Einer verfassungskonform einschränkenden Auslegung bedarf demnach jedoch § 20 k Abs. 1 S. 2 BKAG. Die in dieser Vorschrift eröffnete Möglichkeit, auch schon im Vorfeld einer konkreten Gefahr Maßnahmen durchzuführen, sofern bestimmte Tatsachen auf eine im Einzelfall erst drohende Gefahr einer Begehung terroristischer Straftaten hinweisen, ist dahingehend auszulegen,

> *„dass Maßnahmen nur erlaubt sind, wenn die Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen und wenn erkennbar ist, 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".*[57]

Dadurch setzte das Bundesverfassungsgericht den Strafverfolgungsbehörden bei der Durchführung von Vorfeldmaßnahmen Grenzen, sodass Ermittlungen „ins Blaue hinein" unzulässig sind und jedenfalls eine Konkretisierung erfordern.

V. Zur verfassungswidrigen Umsetzung des § 100 b StPO

Die Online-Durchsuchung nach § 100 b StPO trat am 24. August 2017 in Kraft und versucht die Anforderungen des Bundesverfassungsgerichts zu würdigen. Allerdings werfen insbesondere die technischen Möglichkeiten beim Zugriff auf informations-

54 *Ebd.*
55 *Ebd.*
56 *Ebd.*
57 *Ebd.*

technische Systeme sowie der Straftatenkatalog des § 100 b Abs. 2 StPO verfassungsrechtliche Fragen auf.

1. Eingriff in informationstechnisches System

Nach der Legaldefinition der Online-Durchsuchung in § 100 b Abs. 1 StPO darf auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und Daten daraus erhoben werden. Dafür müssen folgende Voraussetzungen kumulativ vorliegen:

Bestimmte Tatsachen müssen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete 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 – im Sinne der Subsidiaritätsklausel – auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die konkrete Ausgestaltung des Eingriffs in ein informationstechnisches System wurde durch den Gesetzgeber offengelassen. Die bereits dargestellten technischen Zugriffsmöglichkeiten zeigen jedenfalls, dass diesen regelmäßig nur durch die Hardware des Nutzers Grenzen gesetzt werden und die Strafverfolgungsbehörden grundsätzlich auf sämtliche technischen Mittel zugreifen könnten.

Dieser enorme Befugnisumfang wirft folglich die Frage auf, ob eine solche Zugriffsmöglichkeit noch den Charakter einer Online-Durchsuchung aufweist und von der Rechtsprechung des Bundesverfassungsgerichts gedeckt sein kann. Denn durch die Nutzung von Webcam und Mikrophonen schöpfen Strafverfolgungsbehörden keine Daten ab, sondern betreiben aktiv eine Datenproduktion, da die Daten – ohne die Aktivierung – überhaupt nicht existieren. Gemäß § 100 b Abs. 1 StPO dürfen Daten „erhoben“ werden, was dafürspricht, dass nur eine Feststellung und eben keine Herstellung der Daten zulässig ist.

Ein Zugriff auf Mikrophone und Webcams ermöglicht neben der Aufzeichnung der Daten auch einen „Live-Zugriff“ in die durch Art. 13 GG geschützte Wohnung.[58] Das Bundesverfassungsgericht verneinte zwar in den zitierten Entscheidungen einen Eingriff in Art. 13 GG, bezog sich dabei allerdings lediglich auf das Abschöpfen der Daten von einem informatorischen System und nicht auf das Einsehen der Wohnung. Ob diese hier jedenfalls theoretisch diskutierte Ermittlungsmethode einer gerichtlichen oder sogar verfassungsgerichtlichen Rechtsprechung in Zukunft zugänglich sein wird, erscheint zweifelhaft. Aus Beschuldigten- und Verteidigungssicht wird nur dann der Rechtsweg eröffnet sein, wenn der Zugriff auf Mikrophone und Webcams aktenkundig wird und letztlich Eingang in das Strafverfahren findet.

58 *Roggan*, (Fn. 5), 826.

2. Straftatenkatalog nach § 100 b Abs. 2 StPO

Das Bundesverfassungsgericht stellte besonders hohe Anforderungen an die Durchführung der Online-Durchsuchung, die im Straftatenkatalog der „besonders schweren Straftaten" gemäß § 100 b Abs. 2 StPO Berücksichtigung finden sollten.

a) Im Vergleich zu den nur „schweren Straftaten" im Straftatenkatalog des § 100 a StPO wird zunächst deutlich, dass der Gesetzgeber zu „besonders schweren Straftaten" sehr wohl differenziert. Als Beispiel dienen dafür etwa die Korruptionsdelikte. Die Telekommunikationsüberwachung ist gemäß § 100 a Abs. 2 Nr. 1 u) StPO bei Bestechlichkeit und Bestechung gemäß §§ 332 und 334 StGB möglich. Dagegen ist im Rahmen der Online-Durchsuchung gemäß § 100 b Abs. 2 Nr. 1 m) StPO lediglich der besonders schwere Fall der Bestechlichkeit und der Bestechung erfasst. Zudem sind Straftaten nach der Abgabenordnung, nach dem Anti-Doping-Gesetz, nach dem Außenwirtschaftsgesetz, aus dem Grundstoffüberwachungsgesetz sowie aus dem Neue-psychoaktive-Stoffe-Gesetz jeweils in § 100 a Abs. 2 StPO jedoch nicht in § 100 b Abs. 2 StPO aufgenommen. Man kann insoweit davon sprechen, dass der Gesetzgeber § 100 b StPO insoweit mit Augenmaß schuf.
b) Der Straftatenkatalog des § 100 b Abs. 2 StPO entspricht dem seinerzeit für die Wohnraumüberwachung geltenden Katalog in § 100 c Absatz 2 StPO a.F. Bereits dort wurden Inhalt und Ausmaß des Straftatenkatalogs diskutiert.[59] Der Gesetzgeber verfügt – nach Ansicht des Bundesverfassungsgerichts – über einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung, welche Straftaten Anlass für Ermittlungsmaßnahmen sein sollen. Dafür gibt der – freilich durch den Gesetzgeber selbst geschaffene – Strafrahmen einen maßgebenden Anhaltspunkt. Ein besonders schweres Tatunrecht weisen demnach Delikte mit einer höheren Höchststrafe als fünf Jahren Freiheitsstrafe auf, die damit den Bereich der mittleren Kriminalität eindeutig verlassen sollen.[60] Das Bundesverfassungsgericht stellte seinerzeit die Verfassungswidrigkeit einzelner Katalogstraftaten des § 100 c StPO a.F. fest.[61]
c) Erhebliche Kritik wirft der Straftatenkatalog des § 100 b StPO im Lichte der Anforderungen des Bundesverfassungsgerichts an die Online-Durchsuchung auf.[62] Denn der Maßstab des Straftatenkatalogs von § 100 c StPO a.F. kann bereits durch die konkretisierende Rechtsprechung des Bundesverfassungsgerichts zur Online-

59 Siehe *Löffelmann*, Das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung), in: ZIS 2006, 87 (88 f.).
60 *BVerfG* NJW 2004, 999 (1011).
61 *Ebd.*; siehe dazu *Hauck*, in: LR-StPO, 26. Auflage 2014, § 100 c Rn. 72.
62 So auch *Buermeyer*, (Fn.11), 12; dagegen *Sinn*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334), 10 f.; dagegen auch *Huber*, Stellungnahme zur Sachverständigenanhörung am 31.5.2017 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18 (6) 334), 3 f.

Durchsuchung, nicht ohne weiteres übertragen werden. Das Bundesverfassungsgericht beschränkte die Durchführung der Online-Durchsuchung auf tatsächliche Anhaltspunkte einer konkreten Gefahr für ein „überragend wichtiges Rechtsgut“ wie Leib, Leben und Freiheit der Person sowie der (diskussionswürdigen) Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. [63] Auch an diesem Maßstab wurde § 20 k BKAG gemessen.[64]

Diese Feststellungen des Bundesverfassungsgerichts bezogen sich auf die präventive Online-Durchsuchung im Rahmen des Gefahrenabwehrrechts. Das heißt, dass nur bei den aufgezählten überragend wichtigen Rechtsgütern ein Grundrechtseingriff zur Abwehr einer Gefahr zulässig ist. Daraus folgt, dass eine Verletzung der Rechtsgüter Eigentum und Vermögen – im Hinblick auf die präventive Online-Durchsuchung – hingenommen werden muss. Folglich gilt dies erst recht für repressive Maßnahmen, bei denen bereits eine Rechtsgutsverletzung an diesen Rechtsgütern eingetreten ist.[65]

d) Im Lichte dessen sind die von § 100 c StPO a.F. übernommenen Delikte auf die Online-Durchsuchung nach § 100 b StPO teilweise nicht übertragbar, da einzelne Strafnormen Rechtsgüter „schützen“, die das Bundesverfassungsgericht eben nicht im Rahmen der Online-Durchsuchung als „überragend wichtig“ ansieht. Dies betrifft insbesondere Delikte gegen das Vermögen und das Eigentum. So etwa Geld- und Wertzeichenfälschung, die Qualifikationen zur Hehlerei sowie die Geldwäsche.[66] Denn unabhängig davon, dass diese Delikte nicht den Kernbereich individualer Rechte, wie Leib, Leben und Freiheit der Person tangieren, sind auch keine Güter der Allgemeinheit betroffen, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Auch die Übernahme von Straftaten im Rahmen des Aufenthalts- und des Asylgesetzes scheinen vor dem Hintergrund der Eingriffsintensität der Online-Durchsuchung als nicht „überragend wichtig“.[67] Es muss festgestellt werden, dass Taten aus dem Asylgesetz, wie die Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3 AsylBLG oder nach dem Aufenthaltsgesetz, wie das Einschleusen von Ausländern nach § 96 Abs. 2 AufenthG, im Verhältnis zu anderen schweren Straftaten, etwa nach dem Völkerstrafgesetzbuch – unabhängig vom Strafmaß –, deutlich geringwertiger sind. Der Gesetzgeber hebt zwar den Maßstab des Bundesverfassungsgerichts hervor, indem er im Bereich der Strafverfolgung ein angemessenes Verhältnis zwischen der Maßnahme und der Schwere und Bedeutung der Straftat fordert,[68] scheint diesem allerdings nicht vollständig gerecht zu werden. Hier hätte es insoweit einer entsprechenden Anpassung bedurft.

Obwohl die im Verhältnis zu § 100 a StPO restriktive Bestimmung des Straftatenkatalogs zu begrüßen ist, bleiben die einzelnen Parameter unschlüssig. Beispielsweise wurden Straftaten nach dem Gesetz über die Kontrolle von Kriegswaffen in

63 *BVerfG* NJW 2008, 822 (831).
64 *BVerfG* NJW 2016, 1781 (1795).
65 *Buermeyer*, (Fn.11), 12.
66 Deutlich *Buermeyer*, (Fn.11), 12 f.
67 Vgl. *Buermeyer*, (Fn.11), 13.
68 Ausschussdrucksache 18(6)334, 24.

den Katalog des § 100 b Abs. 2 StPO aufgenommen, gleichwohl wurde jedoch § 17 AWG ausgenommen, der auch sog. Waffenembargos erfasst und die Sanktionierung als Verbrechen in Absatz 2 sowie einer Freiheitsstrafe nicht unter zwei Jahren nach Absatz 3 zulässt. Der Strafunwert dürfte in diesem Zusammenhang jedenfalls vergleichbar sein.

e) Kritisch hervorzuheben ist zudem, dass neben dem Straftatenkatalog des § 100 b Abs. 2 StPO auch der Versuch dieser Delikte – anliegend an die akustische Wohnraumüberwachung gemäß § 100 c StPO – übernommen wurde. Unabhängig von der Frage, dass die Versuchsstrafbarkeit auch bereits zuvor in anderen Eingriffsnormen wie § 100 a StPO aufgenommen wurde, muss die Frage gestellt werden, ob es bei dem durch das Bundesverfassungsgericht hervorgehobenen intensiven Eingriff in das Grundrecht auf Unversehrtheit informationstechnischer Anlagen auch weiterhin der Aufnahme der Versuchsstrafbarkeit bedurft hat. Die Versuchsstrafbarkeit schwächt den Strafunwert der Handlung erheblich ab, sodass der Maßstab einer „besonders schweren Straftat" nicht ohne weiteres übertragbar ist. Gleichwohl wurde die seinerzeit bei § 100 c StPO a.F. diskutierte Aufnahme der Vorbereitung einer Anlasstat durch eine sonstige Straftat nicht umgesetzt.[69]

Der Gesetzgeber hat die Vorgaben des Bundesverfassungsgerichts verfehlt, indem er Straftatbestände, die nicht im Zusammenhang mit überragend wichtigen Rechtsgütern stehen, in den Katalog des § 100 b StPO aufnahm. Die bisherige Rechtsprechung des Bundesverfassungsgerichts spricht deshalb dafür, dass im Bereich des Straftatenkatalogs nachgebessert werden muss.

3. Online-Durchsuchung bei anderen Personen

Die Online-Durchsuchung darf sich gemäß § 100 b Abs. 3 S. 1 StPO nur gegen den Beschuldigten richten. Nach § 100 b Abs. 3 S. 2 StPO ist ein Eingriff in informationstechnische Systeme anderer Personen nur dann zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der in der Anordnung nach § 100 e Abs. 3 StPO bezeichnete 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.

Der Eingriff in das informationstechnische System einer anderen Person ist in Anlehnung an § 100 c Abs. 3 StPO nur konsequent, sofern das System dieser anderen Person genutzt wird. Gleichwohl ist anzumerken, dass auch hier auf einen nicht abgrenzbaren Kreis von Daten des Dritten zugegriffen werden kann. Nach § 100 b Abs. 3 S. 3 StPO dürfen Maßnahmen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen sind, also wenn der Zugriff auf Geräte des Beschuldigten selbst allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten genügt.[70] Insofern wurde hier klarstellend die Zulässigkeit des Eingriffs in die Daten Dritter kodifiziert.

69 Siehe BT-Drucksache 15/4533, 12; dazu *Löffelmann*, (Fn. 59) 88 f.
70 Ausschussdrucksache 18(6)334, 25.

4. Spezifischer Kernbereichsschutz

Besonders tiefgreifende Überwachungsmaßnahmen in das Privatleben des Betroffenen, die mit berechtigten Vertraulichkeitserwartungen kollidieren, erfordern strenge Schutzmaßnahmen für den absoluten Kernbereich der Persönlichkeit, der nicht ausgeforscht werden darf. [71] Tagebuchartige Aufzeichnungen sowie intime Erklärungen sowie Film- und Tonaufzeichnungen werden häufig in Dateiform gespeichert und teilweise ausgetauscht.[72] Die elektronische Übermittlung höchstpersönlicher Kommunikation erfolgt von internetbasierten Kommunikationsdiensten, die teilweise auch an soziale Netzwerke gebunden sein können.[73]

Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100 a bis 100 c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme gemäß § 100 d StPO unzulässig. Dass Erkenntnisse „allein“ aus dem Kernbereich privater Lebensgestaltung erlangt werden, wird im Rahmen der Online-Durchsuchung gemäß § 100 b StPO selten zu prognostizieren sein. Bereits deshalb kann von einem insoweit leerlaufenden Kernbereichsschutz ausgegangen werden.[74] Unabhängig davon ist gemäß § 100 d Abs. 3 S. 1 StPO allerdings technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Technisch sichergestellt werden könnte dies jedenfalls dann, wenn generell kein Zugriff auf Mikrophone und Webcams erfolgen würde. Da beim Zugriff eben nicht sichergestellt werden kann, dass kein Eingriff in den Kernbereich privater Lebensgestaltung erfolgt – wie sollte man auch die Aufzeichnung von Audio- und Videodateien davon abhängig machen – gehört ein solcher Eingriff folglich zum Normprogramm.[75] Das Bundesverfassungsgericht löst diesen Konflikt durch eine Verlagerung des Kernbereichsschutzes von der Erhebungsebene auf die nachgelagerte Auswertungs- und Verwertungsebene.[76]

VI. Fazit

Der mit der Online-Durchsuchung verbundene Eingriff in die Grundrechte des Betroffenen wiegt aufgrund der diversen Einsatzmöglichkeiten des Staatstrojaners erheblich schwerer, als es bei vergleichbaren Ermittlungsmaßnahmen der Fall ist. Die Online-Durchsuchung nach § 100 b StPO lässt nicht nur ein „Mehr“ an Durchsuchung zu, als die „offene“ Durchsuchung nach den §§ 102 ff. StPO.[77] Sie bietet Ermittlungsbehörden daneben weitreichendere Einsatzmöglichkeiten als die Telekommunikationsüberwachung nach § 100 a StPO und die akustische Wohnraumüberwachung nach § 100 c StPO. Die Begrenzung der Anwendbarkeit auf besonders schwere Straftaten nach

71 Ausschussdrucksache 18(6)334, 15 f.
72 *BVerfG* NJW 2016, 1781 (1794).
73 *Ebd.*
74 *Roggan*, (Fn. 5), 828.
75 *Ebd*.
76 *BVerfG* NJW 2016, 1781 (1794); *BVerfG* NJW 2008, 822 (834).
77 Ausschussdrucksache 18(6)334, 23.

§ 100 b Abs. 2 StPO allein, bietet keinen ausreichenden Schutz. Die Auswertung des Straftatenkatalogs zeigt, dass die Erfassung einzelner Delikte, die nicht im Zusammenhang mit überragend wichtigen Rechtsgütern stehen, nicht von der Rechtsprechung des Bundesverfassungsgerichts gedeckt ist. Indes ist nicht zu erwarten, dass das Bundesverfassungsgericht § 100 b StPO im Rahmen repressiver Maßnahmen per se für verfassungswidrig erklärt. Auch hier wird sich vor dem Hintergrund der „Effektivität der Strafverfolgung" ein Zugriff auf informationstechnische Systeme im engen Korsett überragend wichtiger Rechtsgüter herleiten lassen. Verfassungsrechtlich geboten ist jedoch, dass der Zugriff auf die Telekommunikation, wie im Rahmen der bisherigen Überwachungsmaßnahmen, beschränkt bleibt, um eine Ausforschung des Kernbereichs privater Lebensführung durch die Übernahme des informationstechnischen Systems zu verhindern. Denn das Strafprozessrecht bleibt auch im Lichte ausweitender technischer Möglichkeiten bei der Nutzung informationstechnischer Systeme „*Verbrechensbekämpfungsbegrenzungsrecht*".[78]

78 Vgl. *Naucke,* (Fn. 37), 40.