Ein „Geschenk“ für den Rechtsstaat

Der Bundestrojaner als digitales Werkzeug kriminalpolizeilicher Überwachung

*Hao-Hao Wu**

Die Verwendung verdeckter Ermittlungsmaßnahmen zur Verfolgung und Aufklärung schwerer Straftaten oder im Bereich der Terrorbekämpfung ist immer wieder Gegenstand politischer und juristischer Debatten. Der Beitrag widmet sich dem besonders heiklen Thema des Bundestrojaners.

I. Einleitung: Themenumfeld und Aktualität

In Zeiten der internationalen Bedrohung durch terroristische Aktivitäten, insbesondere durch die des sog. Islamischen Staates (IS), ist die Bedeutung einer effektiven Gefahrenabwehr durch die Sicherheitsbehörden größer denn je. In aktuellen sicherheitspolitischen Überlegungen fügt sich die vom Bundeskriminalamt (BKA) für Herbst geplante Einführung des Bundestrojaners ein,[1] der unbemerkt (Kommunikations-)Daten am PC eines Verdächtigen erheben und den Sicherheitsbehörden übermitteln soll. Er ist damit ein Mittel, welches sowohl bei der Online-Durchsuchung als auch bei der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingesetzt werden kann. Diese Maßnahmen können wiederum zur Gefahrenabwehr (präventiv) oder zur Strafverfolgung (repressiv) eingesetzt werden. Für die präventiven Ermittlungsmaßnahmen stehen die Rechtsgrundlagen im Gesetz über das Bundeskriminalamt (BKAG) derzeit auf dem verfassungsrechtlichen Prüfstand beim BVerfG.[2] Ein Urteil wird für Herbst 2015 erwartet.[3] Dabei ist nicht nur die technische Bewerkstelligung interessant, sondern auch die verfassungsrechtlichen Vorgaben, an denen sich eine derartige Überwachung zu messen hat. Über beides soll der folgende Beitrag einen Überblick geben.

II. Warum eigentlich „Bundestrojaner“?

Schon der Begriff des Bundestrojaners als solcher erregt Interesse und ist in der Öffentlichkeit daher als politisches Schlagwort präsent. Sein offizieller – und dennoch kaum bekannter – Name lautet hingegen *Remote Forensic Software*. Doch was versteckt sich eigentlich dahinter?

1. Der Begriff des trojanischen Pferdes und seine moderne Bedeutung

Während des bereits zehn Jahre andauernden Krieges der Griechen gegen die Trojaner im 12. oder 13. Jahrhundert vor Christus, so erzählt es die griechische Mythologie,[4] versteckten sich griechische Soldaten im Bauch eines hölzernen

---

* *Der Verfasser ist Studierender der Rechtswissenschaften an der LMU München und Mitglied der Redaktion von rescriptum.*

1 Vgl. Interview mit dem Präsidenten des Bundeskriminalamtes *Holger Münch*, Ein zahnloser Tiger, DER SPIEGEL, Ausgabe 18/2015, S. 40 ff., hinweisend auf die Tätigkeiten des sog. Islamischen Staates.

2 Verfahren über mehrere Verfassungsbeschwerden anhängig, Az. 1 BvR 966/09, 1 BvR 1140/09.

3 Etwa Legal Tribune Online vom 07.07.2015, BVerfG sieht BKAG-kritisch, Datenschatz vs. Datenschutz, abrufbar auf http://www.lto.de/recht/nachrichten/n/bverfg-1bvr114009-bka-befugnisse-terrorabwehr-kritik/ (Stand: 06.09.2015).

4 Zur Frage des Wahrheitsgehaltes der Legende siehe etwa Focus Online, Mystische Stätten, Troja – Legende oder Wirklichkeit, abrufbar auf http://www.focus.de/wissen/mensch/archaeologie/legenden/troja_aid_13081.html (Stand: 06.09.2015).

Pferdes, welches als vermeintliches Geschenk an die Kriegsgöttin Athene vor die Tore der Stadt Troja gebracht wurde. Nachdem die trojanischen Wachen das hölzerne Pferd freudig hereingelassen hatten, schlichen sich die Griechen in der Nacht aus dem Pferd heraus und öffneten die Stadttore für die anderen Soldaten, die nunmehr ungehindert die Stadt angreifen und besiegen konnten.[5] Der Begriff des trojanischen Pferdes wurde unterdessen zum geflügelten Wort.

Mehr als 3000 Jahre später hat der Begriff des trojanischen Pferdes eine ganz neue Erscheinung erhalten, ohne jedoch seine ursprünglich angelegte Bedeutung auch nur im Geringsten einzubüßen. Als trojanisches Pferd („Trojaner") bezeichnet man eine nicht (unbedingt) schädliche Software, die vordergründig eine nützliche Funktion erfüllt, im Hintergrund aber andere, verdeckte Tätigkeiten ausübt, von denen der Anwender keine Kenntnis hat.[6] So funktioniert auch der Bundestrojaner, der unbemerkt Informationen sammelt und an Sicherheitsbehörden zur Auswertung übermittelt.[7]

2. Begriffsabgrenzungen: Bundestrojaner gleich Online-Durchsuchung gleich Quellen-TKÜ?

Es ist wichtig, sich den Unterschied zwischen den Begriffen Bundestrojaner, Online-Durchsuchung und der Quellen-TKÜ deutlich zu machen, da die klare Abgrenzung notwendig ist, um den verfassungsrechtlichen Rahmen zu bestimmen.

a) Online-Durchsuchung

Als Online-Durchsuchung bezeichnet man die umfassende, „heimliche Infiltration eines informationstechnischen Systems[8], mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können"[9].

b) Quellen-TKÜ

Nach dem gleichen Prinzip funktioniert auch die Quellen-TKÜ, bei der jedoch deutlich weniger Daten erhoben und ausgewertet werden; nämlich nur die über den Computer laufende Telekommunikation. Gemeint ist etwa die Internettelefonie (etwa via Skype). Daten, die nicht der Telekommunikation zugeordnet sind, also nicht für den Versand vorgesehene Bilder und Dokumente, dürfen im Rahmen der Quellen-TKÜ nicht erhoben werden. Die Quellen-TKÜ ist wiederum von der netzbasierten Telekommunikationsüberwachung (Abhören eines Telefonates) und der Vorratsdatenspeicherung abzugrenzen. Das Wort „Quelle[n]" bezieht sich auf den Umstand, dass die Daten bereits vor einer etwaigen Verschlüsselung durch den Betroffenen „an der Quelle" und nicht erst in der Leitung abgehört werden.[10]

c) Bundestrojaner

Bei dem Bundestrojaner hingegen handelt es sich um ein *Mittel*, um eben die vorgenannten Ermittlungsmaßnahmen durchzuführen. Er ist daher nur eine Untergruppe der in Gesetzen genannten *technischen Mitteln* (vgl. nur in §§ 20k Abs. 1 S. 1 Hs. 1, 20l Abs. 2 S. 1 BKAG) und ist demnach nicht besonders geregelt. Eine Legaldefinition des Bundestrojaners oder dessen genaue Einsatzmodalitäten sucht man daher vergeblich.

3. Technische Funktionsweise

Aufschluss über die Frage der technischen Funktionsweise gibt eine im Jahre 2011 durch den *Chaos Computer Club* veröffentliche Analyse einer ihm zugespielten Trojaner-Software.[11] Danach gibt es insgesamt drei Möglichkeiten der Infektion.[12] Zum einen kann ein physischer Angriff auf den PC selbst erfolgen, womit jedoch immer zugleich in Art. 13 GG eingegriffen wird. Daher wird diese Form der Infektion nicht angewendet.[13] Ferner kann der Bundestrojaner wie eine gewöhnliche Malware als E-Mail-Anhang auf den PC gelangen oder vom Betroffenen von einer manipulierten Seite unbeabsichtigt heruntergeladen werden (sog. *Drive-By-Download*). Anfällig an dieser Infektion ist die leichte Erkennbarkeit des Bundestrojaners durch eine Antivirensoftware.[14] Für die Behörden ist dementsprechend eine Kooperation mit Anbietern von sog. *Infection Proxies* vorzugswürdig, da hierdurch bekannte Sicherheitslücken des informationstechnischen Systems ausgenutzt werden und die Infektion „sicher" ist.[15] Ist die Datei einmal auf den Zielrechner des Betroffenen gelangt, baut sie eine Verbindung zu einer „Kommandozentrale" auf und kann mit dieser fortan kommunizieren.[16] Der *Chaos Computer Club* kritisiert eine fehlende Verschlüsselung von Daten, die an den Trojaner gesendet werden. Dadurch sei es ein Leichtes, diese Daten

5 Siehe *Schmeh*, Das trojanische Pferd: klassische Mythen erklärt, 2007, S. 30.

6 Vgl. tagesschau.de vom 03.03.2008, Schnüffeln ohne aufzufallen, Wie funktioniert der Bundestrojaner?, abrufbar auf https://www.tagesschau.de/inland/meldung490134.html (Stand: 06.09.2015).

7 Vgl. unter II.3.

8 Das kann z.B. ein PC oder informationstechnische Komponente in Telekommunikationsgeräten (etwa Mobilfunkgeräten) sein, vgl. dazu *Jarass,* in: Jarass/Pieroth, GG, 13. Aufl. 2014, Art. 2 Rn. 46.

9 So etwa *Murswiek*, in: Sachs, GG, 7. Aufl. 2014, Art. 2 Rn. 121c.

10 Siehe dazu SZ.de vom 17.05.2010, Bundestrojaner, Wie kommt er auf den Rechner?, abrufbar auf http://www.sueddeutsche.de/digital/bundestrojaner-wie-kommt-er-auf-den-rechner-1.265048 (Stand: 06.09.2015).

11 *Chaos Computer Club e.V.*, Analyse einer Regierungs-Malware, 2011, vollständiges Dokument abzurufen auf http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (Stand: 06.09.2015); die folgenden Ausführungen beziehen sich auf die damals zugespielte Software, haben aber auch allgemeingültigen Charakter vgl. *Chaos-Computer-Club e.V.*, Stellungnahme an das BKA-Gesetz und zum Einsatz von Staatstrojanern, 2015, abzurufen auf http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf (Stand: 06.09.2015).

12 *Chaos Computer Club e.V,* Analyse einer Regierungs-Malware, 2011, S. 3, vollständiges Dokument abzurufen auf http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf; so auch SZ.de vom 17.05.2010 (Fn. 10).

13 In der Beantwortung (BT-Drs. 17/7760, S. 15) einer kleinen Anfrage der Fraktion der Linken (BT-Drs. 17/7104, S. 7) hat die Bundesregierung explizit darauf hingewiesen, dass bei der Infektion des Zielcomputers kein Eingriff in Art. 13 GG erfolge.

14 Darauf wird auch auf SZ.de (Fn. 10) hingewiesen.

15 *Chaos Computer Club e.V* (Fn. 12), S. 3.

16 *Chaos Computer Club e.V* (Fn. 12), S. 3.

von einem Dritten einzusehen und den Trojaner damit zu manipulieren,[17] womit das ganze System übernommen werden könne und mithin eine „klaffende Sicherheitslücke“[18] entstehe. Auf diese Gefahren hat der *Chaos Computer Club* in seiner Stellungnahme an das BVerfG[19] nochmals hingewiesen. Wie die Ausgestaltung des neuen Bundestrojaners aussehen wird, ist nicht bekannt.

In diesem Zusammenhang ist auch die Frage von Interesse, ob es technisch möglich ist, dass die Software nur bestimmte Daten erhebt und übermittelt, etwa ausschließlich die Telekommunikationsdaten. Bei der Quellen-TKÜ schreibt das BVerfG nämlich vor, dass eine Verwendung des Bundestrojaners nur dann stattfinden darf, wenn sichergestellt ist, dass keine anderen (mit der Telekommunikation nicht in Verbindung stehenden) Daten erhoben werden können.[20] Ansonsten ändere sich nämlich der Prüfungsmaßstab.[21] Nach derzeitigem Stand der Technik scheint es eine derartige Begrenzung der Software jedoch nach Ansicht mehrerer vor dem BVerfG im Rahmen der Verhandlung zur Online-Durchsuchung angehörter Sachverständiger nicht geben zu können.[22] Wie das BVerfG damit in der aktuell zu erwartenden Entscheidung zum BKAG umgeht, bleibt abzuwarten.

III. Gegenwärtige Rechtslage

1. Eine Kompetenzbetrachtung: der Bundestrojaner doch Landessache?

Bevor man sich mit den materiellen Schranken für den Einsatz eines Bundestrojaners auseinandersetzt, ist zunächst festzustellen, ob der Bund für den Erlass entsprechender Normen überhaupt gesetzgebungskompetent ist.

Unstreitig ist jedenfalls, dass der Bund für das Strafprozessrecht und dementsprechend auch für die Anwendung eines Bundestrojaners auf dem Gebiet der Strafrechtspflege die konkurrierende Gesetzgebungskompetenz aus Art. 74 Abs. 1 Nr. 1 GG hat.

Beim Gefahrenabwehrrecht bedarf es allerdings einer genaueren Betrachtung. Denn das *allgemeine* Gefahrenabwehrrecht gehört zu den Kernkompetenzen der Länder[23], weshalb es nicht unproblematisch ist, dem BKA als Bundesoberbehörde weitgehende Kompetenzen im Bereich des Trojanereinsatzes einzuräumen. In der Förderalismusreform I im Jahre 2006 hat der Verfassungsgesetzgeber jedoch auf den internationalen entstehenden Terrorismus, der sich spätestens seit den Anschlägen vom 11.09.2001 bemerkbar gemacht hat, reagiert und dem Bund erstmals bedeutende Kompetenzen auf dem Gebiet der „originären“ Gefahrenabwehr eingeräumt.[24] Durch den neu geschaffenen Art. 73 Abs. 1 Nr. 9 lit. a GG kann der Bund nunmehr Gesetze erlassen, die der Abwehr von konkreten Gefahren des internationalen Terrorismus[25] dienen, soweit eine der im Kompetenztitel genannten Voraussetzungen, etwa eine länderübergreifende Gefahr, vorliegt.[26] Im Übrigen bleiben die Länder zuständig.

Der Bundestrojaner ist also je nach Einsatzbereich („einfache“ Gefahrenabwehr, Abwehr der Gefahren des internationalen Terrorismus oder Strafrechtspflege) sowohl Bundes- als auch Ländersache.

2. Verfassungsrechtlich gesetzte Grenzen der Anwendung durch die Grundrechte

Materiell-verfassungsrechtlich setzen vor allem die Grundrechte der Anwendung des Bundestrojaners teils erhebliche Grenzen. Welches Grundrecht dabei einschlägig ist, hängt maßgeblich davon ab, *wie* der Bundestrojaner zum Einsatz kommt.

a) Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 GG

Wie bereits dargestellt, wird durch den Trojaner-Einsatz mangels Eindringen in Räumlichkeiten nicht in Art. 13 GG eingegriffen, es sei denn die gesetzliche Grundlage sieht explizit das physische Eindringen in die Wohnung vor. Die Infiltration des Systems selbst als Eingriff zu sehen, scheitert indes an der Standortunabhängigkeit des verwendeten Systems. [27]

b) Grundrecht auf Fernmeldegeheimnis aus Art. 10 GG

Art. 10 GG schützt das Brief-, Post- und Fernmeldegeheimnis und ist somit als ein bedeutendes Grundrecht im Rahmen der Kommunikationsverfassung zu verstehen.[28] Es gewährleistet eine „Privatheit auf Distanz“[29], die der freien Entfaltung der Persönlichkeit und dem Schutz der Menschenwürde dient.[30] Sinn und Zweck ist es damit, den spezifischen Gefahren der räumlich distanzierten Kommunikation Rechnung zu tragen.[31] Demnach schützt Art. 10 GG nur den Transportweg als solchen und nicht den Kommunikationsbestand auf dem Computer selber. Dann kann der Empfänger nämlich selbst geeignete Schutzmaßnahmen treffen und ist auf den grundrechtlichen Schutz des Art. 10

17 *Chaos Computer Club e.V* (Fn. 12), S. 4 f.

18 *Chaos Computer Club e.V* (Fn. 12), S. 6.

19 *Chaos Computer Club e.V.*, Stellungnahme zum BKA-Gesetz und Staatstrojaner, 2015, abrufbar auf http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf (Stand 06.09.2015).

20 Vgl. dazu unter C.II.2.

21 Vgl. dazu unter C.II.3.

22 Vgl. dazu *Hoffmann-Riem*, JZ 2008, 1010 (1022); vgl. auch *Chaos Computer Club e.V* (Fn. 19), S. 8 ff.

23 Vgl nur *Thiel*, Polizei- und Ordnungsrecht, 2013, § 1 Rn. 6; ausführlich auch BVerfGE 8, 143 (149 f.)

24 Vgl. *Heintzen*, in: v. Mangoldt/Klein/Starck, GG, Bd. 2, 2010, Art. 73 Rn. 92.

25 Siehe zum Terrorismusbegriff *Degenhart*, in: Sachs, GG, 7. Aufl. 2014, Art. 73 Rn. 46.

26 *Kunig*, in: von Münch/Kunig, GG, Bd. 2, 6. Aufl. 2012, Art. 73 Rn. 40.

27 Dazu ausführlich BVerfGE 120, 274 (310 f.)

28 Besonders betont auch bei *Löwer*, in: von Münch/Kunig, GG, Bd. 1, 6. Aufl. 2012, Art. 10 Rn. 1.

29 BVerfGE 115, 166 (182).

30 BVerfGE 113, 348 (391); auch *Epping*, Grundrechte, 6. Aufl. 2014, Rn. 689.

31 Vgl. BVerfGE 85, 386 (396); auch *Pieroth/Schlink/Kingreen/Poscher*, Grundrechte, Staatsrecht II, 30. Aufl. 2014, § 19 Rn. 826.

GG nicht mehr angewiesen.[32] Die Online-Durchsuchung, in dessen Rahmen alle Daten erhoben werden können, kann sich daher nicht an Art. 10 GG messen lassen. Nur in den Fällen, in denen ausschließlich die laufende Kommunikation im Rahmen der Quellen-TKÜ überwacht wird, greift der Schutz des Art. 10 GG ein.[33] Problematisch ist insoweit, dass der Übergang zur Online-Durchsuchung fließend ist, da mit der Infiltration die entscheidende Hürde genommen sei, um das System insgesamt auszuspähen.[34] Art. 10 GG ist also mit den Worten des BVerfG nur dann alleiniger Prüfungsmaßstab des Bundestrojaners, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist.[35]

c) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wurde im Urteil des BVerfG vom 27.02.2008[36] entwickelt und soll „auf neuartige Gefährdungen der Persönlichkeit"[37] durch die „zunehmende Verbreitung vernetzter informationstechnischer Systeme" reagieren. Dieses aus dem allgemeinen Persönlichkeitsrecht abgeleitete Grundrecht hat mithin eine lückenschließende Funktion und soll einen umfassenden Schutz des Einzelnen im Bereich der modernen Technik gewährleisten, weshalb es auch den Beinamen „Computer-Grundrecht" trägt.[38] Es entwickelt das Grundrecht auf informationelle Selbstbestimmung[39] fort und bringt den Grundrechtsschutz gewissermaßen auf die nächste Stufe. Im Bereich der Infiltration informationstechnischer Systeme ist es nach Ansicht des BVerfG das Grundrecht, welches staatliche Eingriffe abzuwehren vermag. Es ist daher bei einer umfassenden Infiltration informationstechnischer Systeme im Rahmen der Online-Durchsuchung alleiniger verfassungsrechtlicher Prüfungsmaßstab.

d) Vom BVerfG entwickelte Maßstäbe für den Einsatz der Online-Durchsuchung

Mit der genannten Entscheidung zur Online-Durchsuchung hat das BVerfG damals in der Ausgestaltung des nordrheinwestfälischen Verfassungsschutzgesetzes mehrere Maßstäbe aufgestellt, an denen sich derartige Maßnahmen zu messen haben. Danach ist eine Online-Durchsuchung (und der damit verbundene Einsatz des Bundestrojaners) verfassungsrechtlich nur dann zulässig, wenn

- tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut (z.B. Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt) bestehen[40],
- sie dem Vorbehalt richterlicher Anordnung unterliegt[41] und
- ausreichende Vorkehrungen zum Schutz des Kernbereiches privater Lebensgestaltung getroffen wurden.[42] Dabei hat das BVerfG ein zweistufiges Schutzkonzept[43] aufgestellt: Schutz sowohl bei Erhebung als auch bei Auswertung der Daten.
- Neben den vorgenannten, speziellen Vorgaben, müssen gleichwohl alle anderen allgemeinverfassungsrechtlichen Gebote beachtet werden, namentlich die Grundsätze der Normenklarheit und -bestimmtheit sowie der Verhältnismäßigkeit.[44]

Zwar war Gegenstand des Urteils ausschließlich die am Maßstab des Grundrechtes auf Vertraulichkeit und Integrität informationstechnischer Systeme zu messende Online-Durchsuchung; die Feststellungen und Dogmen sind aber auf die Quellen-TKÜ zu übertragen.[45]

Im Bereich der Strafrechtspflege gelte nach *Wolters* allerdings ein restriktiverer Rahmen für die Anwendung von verdeckten Ermittlungsmaßnahmen, namentlich der Quellen-TKÜ.[46] Er begründet dies mit den in der Strafverfolgung besonders zu berücksichtigenden Schutzpflichten des Staates. Dem ist zuzustimmen. Anders als bei der Gefahrenabwehr, in dessen Rahmen bedeutende Rechtsgüter vor einem drohenden und noch abzuwendendem Eingriff geschützt werden sollen, dient das Strafverfahren „lediglich" der Aufklärung bereits eingetretener Rechtsgutverletzungen. Demnach erscheint es geboten, den Rechtfertigungsmaßstab entsprechend anzupassen und den staatlichen Aufklärungs- und Vergeltungsanspruch bei besonders intensiven Grundrechtseingriffen zurücktreten zu lassen, um den besonderen staatlichen Schutzpflichten ausreichend Rechnung zu tragen.

32 Dazu grundlegend BVerfGE 115, 166 = StV 2006, 453 = NJW 2006, 976; anders noch Kammerentscheidung des BVerfG vom 04.02.2005, 2 BvR 308/04 = NJW 2005, 1637, 1639; kritisch auch *Schoch*, Jura 2011, 194 (195).

33 BVerfGE 120, 274 (309).

34 Deutlich BVerfGE 120, 274 (308).

35 BVerfGE 120, 274 (309).

36 BVerfGE 120, 274 – *Online-Durchsuchung.*

37 BVerfGE 120, 274 (303).

38 Ähnlich etwa auch bei *Epping* (Fn. 30), Rn. 652.

39 Entwickelt im Volkszählungsurteil des BVerfG, BVerfGE 65, 1.

40 BVerfGE 120, 274 (274), 2. Leitsatz; teilweise wortlautgleich in gesetzliche Vorschriften übernommen, vgl. etwa § 20k Abs. 1 Nr. 1 und 2 BKAG.

41 BVerfGE 120, 274 (274), 3. Leitsatz.

42 BVerfGE 120, 274 (274), 3. Leitsatz, weitergehende Ausführungen in BVerfGE 120, 274 (335 ff.).

43 BVerfGE 120, 275 (338).

44 So auch *Albrecht/Dienst*, JurPC Web-Dok. 5/2012, Abs. 8.

45 Vgl. auch *Bruns*, Karlsruher Kommentar zur StPO, 7. Aufl. 2013, § 100a Rn. 28.

46 *Wolter*, in: Wolter (Hrsg.), Systematischer Kommentar zur StPO, Bd. II, 4. Aufl. 2010, § 100a Rn. 30.

3. Umsetzung in einfaches Bundesrecht

Eine Regelung, die explizit den Einsatz eines Bundestrojaners vorsieht und regelt, existiert im deutschen Recht nicht, da der Bundestrojaner wie bereits dargestellt „nur" ein technisches Mittel ist, um bestimmte gesetzlich normierte Maßnahmen durchführen zu können. Solche Maßnahmen sind in den Gefahrenabwehrnormen der §§ 20k und 20l des BKAG[47] und für die Strafverfolgung in den §§ 100a f. der StPO geregelt, weshalb eine genauere Betrachtung eben dieser Normen vorgenommen werden soll. Auf die landesrechtlichen Vorschriften und der hierzu teilweise ergangenen Kritik (etwa § 34d BayPAG[48] und Art. 6e BayVSG[49] für die Online-Durchsuchung) wird nicht eingegangen.

a) Bedeutung und Reichweite der §§ 20k und 20l BKAG

Sowohl § 20k als auch § 20l BKAG wurden im Rahmen einer umfassenden Änderung des BKAG im Jahre 2008 eingefügt.[50] In dessen Zuge wurden die Kompetenzen des BKAs erheblich gestärkt,[51] was freilich nicht unumstritten war und ist.[52] Im Jahre 2009 wurden dementsprechend mehrere Verfassungsbeschwerden gegen diese und weitere Vorschriften des BKAG eingereicht,[53] die nunmehr beim BVerfG anhängig sind und am 07.07.2015 mündlich verhandelt wurden.[54]

47 Eine Gefahrenabwehrregelung findet sich auch in § 29 Zollfahndungsdienstgesetz (ZFdG); er wird allerding hier nur der Vollständigkeit halber genannt.

48 Sehr kritisch zu der Norm äußert sich etwa *Heckmann*, in: Becker/Heckmann/Kempen/Manssen, Öffentliches Recht in Bayern, 5. Aufl. 2011, 3. Teil Rn. 44a.

49 *Gudemann* merkt etwa an, dass die Verfassungsschutzbehörden weit im Vorfeld der Gefahr tätig werden würden, so dass für die Online-Durchsuchung zur Gefahrenabwehr schlicht kein Raum sei, *Gudemann*, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010, S. 240.

50 Eingefügt mit Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25.12.2008 (BGBl. 2008, Teil I, S. 3083 ff.) m.W.v. 01.01.2009.

51 Ausführliche Besprechung bei *Roggan*, NJW 2009, 257.

52 Kritisiert wurde etwa ein fehlendes sicherheitspolitisches Gesamtkonzept, in dessen Rahmen sich zu viele Kompetenzen bei dem Bundeskriminalamt bündelten. *Christoph Möllers* drückte sich im Rahmen des Gesetzgebungsverfahrens wie folgt aus: „(…) Das unausgesprochene Organisationskonzept dieses Gesetzes ist: Wir geben eigentlich einmal allen Behörden, die wir haben, alle Kompetenzen, die wir kennen und dann sehen wir weiter." (Wortprotokoll der Anhörung des Innenausschusses des Deutschen Bundestages vom 15.09.2008 zum Gesetzesentwurf in BT-Drs. 16/9588, Protokoll Nr. 16/73 S. 21).

53 *Möller/Feidt*, MMR 03/2009, S. XIX, Verfassungsbeschwerde einer Beschwerdeführerin unter http://www.heise.de/tp/r4/artikel/29/29614/1.html (Stand 06.09.2015) abrufbar; weitere Ausführungen bei *Tanneberger*, Die Sicherheitsverfassung, 2014, zugl. eingereicht als Dissertation, S. 278 f.

54 Vgl. die Verhandlungsgliederung für die mündliche Verhandlung des Ersten Senats des Bundesverfassungsgerichts am 07. Juli 2015, abrufbar auf http://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/Verhandlungsgliederungen/bkagesetz_mv.pdf?__blob=publicationFile&v=2 (Stand: 06.09.2015).

aa) § 20k BKAG als Befugnisnorm für die Online-Durchsuchung

§ 20k Abs. 1 BKAG erlaubt dem Bundeskriminalamt unter bestimmten Voraussetzungen, zu Zwecken der Terrorbekämpfung nach § 4a BKAG ohne Wissen des Betroffenen in informationstechnische Systeme einzugreifen und Daten zu erheben. Es ist damit die maßgebliche Befugnisnorm für die Online-Durchsuchung im Bereich der präventiven Gefahrenabwehr auf Bundesebene.

Sinn und Zweck der Regelung ist es, auf die zunehmende Verwendung moderner Technologien im Bereich des internationalen Terrorismus zu reagieren. Nach der Gesetzesbegründung sei es daher für eine effektive Gefahrenabwehr notwendig, auch auf Daten zugreifen zu können, die nicht oder nicht mehr Gegenstand einer laufenden Telekommunikation sind. Dies gelte gleichwohl auch für Daten, die überhaupt nicht für die Telekommunikation bestimmt sind.[55]

Ein Richtervorbehalt ist in § 20k Abs. 5 vorgesehen. § 20k Abs. 7 der Vorschrift sieht überdies Schutzvorkehrungen vor, um den Kernbereich privater Lebensgestaltung zu schützen, um den Anforderungen des BVerfG gerecht zu werden.

Von einer Ansicht in der Literatur wird bestritten, dass der Bund für den Erlass der entsprechenden Norm die Gesetzgebungsbefugnis habe.[56] Aus Art. 73 Abs. 1 Nr. 9 lit. a GG ergebe sich nämlich nur die Kompetenz zur Abwehr *konkreter* Gefahren des internationalen Terrorismus[57], während der Regelungsbereich des § 20k BKAG vorgelagert sei und an keine Gefahr anknüpfe. Hierfür sei die Norm des Art. 73 Abs. 1 Nr. 9 lit. a GG aber nicht konzipiert.

Die Norm sei im Hinblick auf das Verhältnismäßigkeitsprinzip einschränkend auszulegen, als die Online-Durchsuchung nur dann angewendet werden kann, wenn eine „existenzielle Bedrohungslage" aufgeklärt und abgewendet werden kann.[58] Die „einfache" Gefährdung der in Abs. 1 bezeichneten Rechtsgüter reiche nicht aus.[59]

Ferner wird kritisiert, dass eine Online-Durchsuchung ausweislich des Wortlautes in § 20k Abs. 7 S. 1 BKAG nur dann unzulässig ist, wenn *allein* Daten erhoben werden würden, die den Kernbereich privater Lebensgestaltung betreffen.[60] Es dürfte jedoch eine lebensfremde Annahme sein, dass bei einer geplanten umfassenden Erhebung eine Situation anzutreffen ist, bei der *ausschließlich* Kernbereichsdaten erhoben werden würden.[61] Die Norm schützt also nicht

55 Dazu *Schenke*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 20k BKAG Rn. 1 mit Hinweis auf BT-Drs. 16/10121, S. 28.

56 So etwa *Roggan*, NJW 2009, 257 (257).

57 Begründet wird dies mit einer restriktiv gebotenen Auslegung der Gesetzgebungskompetenz, vgl. *Stettner*, in: Dreier (Hrsg.), GG, 2. Aufl. 2007, Bd. 2, Supplementum 2007, Art. 73 Rn. 54.

58 *Roggan*, NJW 2009, 257 (260) m.w.N.

59 *Roggan* (NJW 2009, 257 (260)) führt als Beispiel eine einfache Körperverletzung an.

60 Zur Kritik *Albrecht/Dienst* (Fn. 44), Abs. 11.

61 Ähnlich *Braun/Fuchs* DIE POLIZEI, 2010, 185 (189 f.); mit deutlichen Worten *Roggan*, NJW 2009, 257 (261).

vor einer Erhebung von Kernbereichsdaten als „Beifang“[62]. Im Endeffekt führe dies zu einem leerlaufenden Kernbereichsschutz und sei daher mit dem GG nicht vereinbar.[63]

bb) § 20l BKAG als Befugnisnorm für die Telekommunikations-überwachung

§ 20l BKAG erlaubt dem BKA die Überwachung und Aufzeichnung von Telekommunikation und trägt nach der Gesetzesbegründung dem Umstand Rechnung, dass der internationale Terrorismus länderübergreifend agiere und vernetzt sei, was schließlich eine Kommunikation über Mobilfunkgeräte oder auch über das Internet voraussetze.[64] Aus diesem Grund sei eine Überwachung und Verwertung der Telekommunikation unerlässlich.

§ 20l Abs. 1 BKAG bestimmt als Grundtatbestand, bei welchen Personen zu welchem Zwecke und unter welchen Voraussetzungen eine Überwachung und Aufzeichnung der Telekommunikation zulässig ist. Im Rahmen des § 20l BKAG können dabei nur sog. Inhaltsdaten, aber keine Verkehrsdaten[65] erhoben werden. Im Zusammenhang mit der Verwendung eines Bundestrojaners ist jedoch der Abs. 2 der Norm der wesentlich Interessantere. Er konstatiert die besonderen Voraussetzungen für die bereits oben dargestellte Quellen-TKÜ, bei der die Telekommunikation mittels eines Eingriffes in die vom Betroffenen genutzten informationstechnischen Systeme erfolgt. Dabei entstehen Parallelen zu § 20k BKAG, dem die Norm mit einer Verweisung auf bestimmte Teile der Norm Rechnung trägt (§ 20l Abs. 2 S. 2 BKAG). Es wird überdies klargestellt, dass § 20k BKAG im Übrigen unberührt bleibt[66], was zur Folge hat, dass § 20l BKAG gegenüber § 20k BKAG immer dann subsidiär zurücktritt, wenn sich ein Eingriff nicht ausschließlich auf die Telekommunikation beschränkt.[67] Im Übrigen beinhaltet auch § 20l BKAG einen Richtervorbehalt[68] und Regelungen zum Schutze des Kernbereiches privater Lebensgestaltung.

Von einer kritischen Literaturansicht wird vor allem angemerkt, dass der in § 20l Abs. 2 S. 1 Nr. 1 BKAG genannte Vorbehalt der technischen Begrenzung auf die Telekommunikationsüberwachung nicht möglich ist, so dass die Quellen-TKÜ verfassungsrechtlich wie die Online-Durchsuchung zu behandeln sei.[69]

Auf verfassungsrechtliche Bedenken stößt indes § 20l Abs. 1 Nr. 2 BKAG, wonach die Maßnahme auch zulässig ist, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten gemäß § 4a Abs. 1 S. 2 BKAG vorbereitet werden. Hierbei handelt es sich mangels Vorliegen einer Gefahr um keine Befugnis zur Gefahrenabwehr, sondern um eine Vorfeldbefugnis, die einer konkreten Gefahrenlage vorgeschaltet ist.[70] In solchen Fällen muss jedoch das Bestimmtheitsgebot in einem besonderen Maße beachtet werden.[71] Danach muss die Norm „handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist“[72]. Solche Tatbestandselemente hat § 20l Abs. 1 Nr. 2 BKAG, anders als der (von der Gesetzestechnik her) vergleichbare § 23a Abs. 2 Zollfahndungsdienstgesetz (ZfDG) nicht. Es werden keine Verhaltensweisen umschrieben, die auf eine sichere Prognose schließen, dass eine (terroristische) Straftat vorbereitet wird. Der ausschließliche Verweis auf „bestimmte Tatsachen“ ist mithin verfassungsrechtlich zu unbestimmt.[73] Die nicht überzeugende Gegenansicht[74] sieht in dem Wort „vorbereitet“ eine deutliche Konturierung der Norm und daher keine Bedenken in Bezug auf das Bestimmtheitsgebot. Sie sieht in der Formulierung die Notwendigkeit, „dass sich der auf bestimmte Tatsachen gestützte Verdacht auf eine bereits im Gange befindliche Vorbereitung von Straftaten bezieht“[75].

Bezüglich der Kritik zur Kernbereichsregelung wird auf die Ausführungen zu § 20k Abs. 6 BKAG verwiesen.

b) Online-Durchsuchung und Quellen-TKÜ in der StPO

Während die zwar verfassungsrechtlich nicht unumstrittenen §§ 20k und 20l BKAG vom Wortlaut eindeutig zur Quellen-TKÜ und Online-Durchsuchung berechtigen, vermisst man derartig klare Regelungen in der StPO.

aa) §§ 100a, 100b der Strafprozessordnung als taugliche Ermächtigungsgrundlage für die Quellen-TKÜ in der Strafverfolgung?

§ 100a StPO[76] regelt abschließend[77] die Überwachung und Aufzeichnung der Telekommunikation, sofern die in Abs. 1 genannten Voraussetzungen – unter anderem das Vorliegen einer „schweren Straftat“ – gegeben sind. Abs. 2 listet schließlich umfassend die schweren Straftaten im

62 So die Bezeichnung bei *Albrecht/Dienst* (Fn. 44), Abs. 11.

63 *Roggan*, NJW 2009, 257 (261); *Thiel*, Die Entgrenzung der Gefahr, 2011, S. 341 m.w.N.; die gleichlautende Vorschrift des § 100a Abs. 4 StPO hat das BVerfG jedoch gebilligt (BVerfGE 129, 208, (246)); kritisch dazu wiederum *Roggan*, HRRS 05/2013, S. 153 ff.

64 I.E. etwa *Böckenförde*, JZ 2008, 925 (934).

65 Zur Unterscheidung beider Arten siehe etwa BVerfGE 115, 166 (183); die Befugnis des BKA zur Erhebung und Speicherung von Verkehrsdaten im Sinne des Telekommunikationsgesetzes ist in § 20m BKAG geregelt. Da diese Erhebung jedoch nicht mittels Trojaners erfolgt, wird hier nicht darauf eingegangen.

66 Vgl. dazu auch BT-Drs. 16/10121, S. 31.

67 So etwa auch *Schenke* (Fn. 55), § 20l BKAG Rn. 26.

68 § 20l Abs. 3 sieht jedoch eine spezielle Regelung für Gefahr im Verzuge an. In solchen Situationen kann die richterliche Entscheidung nachgeholt werden.

69 Vgl. bereits oben unter II.3.

70 Die Einordnung trifft auch *Schenke* (Fn. 55), § 20l BKAG Rn. 13.

71 Zuletzt BVerfGE 113, 348 (377 ff.).

72 BVerfGE 113, 348, (378) mit Verweis auf BVerfGE 110, 33 (56).

73 Im Ergebnis auch *Roggan*, NJW 2009, 257 (262).

74 *Schenke* (Fn. 55), § 20l BKAG Rn. 26.

75 *Möstl*, Schriftliche Stellungnahme zur öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages am 15.09.2008, Ausschussdrucksache A-Drs. 16(4)460 I, S. 13.

76 Fassung aufgrund des Gesetzes zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (GVVG-Änderungsgesetz) vom 12.06.2015 (BGBl. I S. 926) m.W.v. 20.06.2015.

77 *Bruns* (Fn. 45), § 100a Rn. 1.

Sinne des Abs. 1 S. 1 in Gestalt eines Straftatkatalogs auf. Abs. 4 sieht Regelungen zum Schutz von Erkenntnissen aus dem Bereich der Kernbereiches privater Lebensgestaltung vor. Das genaue Verfahren zur Durchführung der Telekommunikationsüberwachung ist indes in § 100b StPO gesondert geregelt. Ein eingeschränkter Richtervorbehalt wird in § 100b Abs. 1 StPO vorgeschrieben.

Ob die §§ 100a f. StPO für den Einsatz des Bundestrojaners im Bereich der Quellen-TKÜ eine taugliche Rechtsgrundlage darstellen, ist jedoch umstritten. Während die Rechtsprechung überwiegend eine Rechtsgrundlage erblickt,[78] wird diese Ansicht von der herrschenden Literatur abgelehnt.[79] Für die letztere Ansicht spricht der Wortlaut des § 100a StPO, der die Infiltration eines informationstechnischen Systems mit keinem Wort erwähnt, sondern nur eine Überwachung und Aufzeichnung vorsieht. Damit hat der Gesetzgeber die Quellen-TKÜ nicht im Blick gehabt, sondern ausschließlich die netzbasierte Telekommunikationsüberwachung. So fehlt der vom BVerfG geforderte[80] und in § 20l Abs. 1 Nr. 1 BKAG bereits umgesetzte Vorbehalt, dass durch technische Maßnahmen sichergestellt werden muss, dass *ausschließlich* laufende Telekommunikation überwacht und aufgezeichnet wird. Eine von Teilen der Literatur konstruierte Annexkompetenz[81] zur Infiltration informationstechnischer Systeme, die einer Ausleitung von Telekommunikationsdaten zwingend vorgeschaltet sei, kann indes nicht erblickt werden. Eine derartige, über den Wortlaut der Norm hinausgehende Kompetenzherleitung widerspricht dem Wesentlichkeitsgrundsatz, wonach dem Gesetzgeber die Bestimmungen der wesentlichen Eingriffsvoraussetzungen vorbehalten sind.[82] Dies gilt bei heimlichen Maßnahmen aufgrund ihrer Eingriffsintensität umso mehr.

Eine Ermächtigungsgrundlage für die Quellen-TKÜ kann nach alledem nicht in § 100a f. StPO erblickt werden. Der Einsatz ist nach der derzeitigen Rechtslage mangels förmlicher Rechtsgrundlage mithin verfassungswidrig.

bb) Möglichkeit der Online-Durchsuchung nach der StPO?

Für die Online-Durchsuchung gibt es in der StPO indes keine Ermächtigungsgrundlage. Sie kann insbesondere nicht auf § 102 StPO gestützt werden.[83] Damit fehlt es an einer für den Grundrechtseingriff notwendigen formell-gesetzlichen Befugnisnorm, womit die Online-Durchsuchung zur Strafrechtspflege unzulässig ist.

78 Vgl. etwa LG Landshut, NStZ 2011, 479; LG Hamburg, MMR 2011, 693; AG Bayreuth, MMR 2010, 266; *Bruns* (Fn. 45), § 100a Rn. 28 meint unter Verweis auf die ergangene Rechtsprechung, dass „für eine Übergangszeit – bis zu einer gesetzlichen Reglung – die Quellen-TKÜ auf § 100a gestützt werden kann".

79 Siehe etwa nur *Vogel/Brodowski*, StV 2009, 630, 632 ff.

80 BVerfGE 120, 274 (309).

81 *Bruns* (Fn. 45), § 100a Rn. 28; auch *Graf*, in: Graf (Hrsg.), Beck´scher Online-Kommentar zur StPO (Stand: 01.05.2015), § 100a Rn. 107 f. Beide halten jedoch eine gesetzliche Regelung für notwendig.

82 Im Ergebnis auch *Albrecht/Dienst* (Fn. 44), Abs. 9 m.w.N.

83 Dazu ausführlich BGHSt 51, 211.

IV. Fazit

Der Einsatz eines Bundestrojaners im Rahmen der Online-Durchsuchung und der Quellen-TKÜ erweist sich sowohl im Gefahrenabwehrbereich als auch bei der Verfolgung von Straftaten als eine grundsätzlich effektive und vielversprechende Ermittlungsmaßnahme, wobei für letztere allerdings nach hiesiger Rechtsauffassung keine verfassungsrechtlich tragbare Befugnisnorm vorliegt. Der Gesetzgeber muss dementsprechend tätig werden, sofern sich Strafverfolgungsbehörden des Mittels bedienen möchten.

Ob indes die einschlägigen (und zweifelsohne vorhandenen) Rechtsgrundlagen im BKAG der verfassungsrechtlichen Kritik und Überprüfung insgesamt standhalten, wird das für Herbst erwartete Urteil zeigen. In jedem Fall kann es dazu beitragen, den verfassungsrechtlichen Rahmen für derartige verdeckte Ermittlungsmaßnahmen weiter zu konkretisieren und mehr Rechtssicherheit für diesen grundrechtlich sehr relevanten Bereich zu schaffen. Das BVerfG kann damit die Möglichkeit ergreifen, das Urteil zur Online-Durchsuchung aus dem Jahre 2008 weiterzuentwickeln und etwaige Ungereimtheiten der bisherigen Rechtsprechung zu beseitigen, was vor allem im Interesse eines effektiven Grundrechtsschutzes sehr begrüßenswert ist. Denn auch wenn der internationale Terrorismus eine immer größere Gefahr zu werden scheint, darf der Grundrechtsschutz nicht ausgehebelt werden. Nur so kann auch in (außen-) politisch „schwierigen" Situationen eine vernünftige Balance zwischen Freiheit und Sicherheit hergestellt werden, die eines demokratischen Rechtsstaates würdig ist.