Gutachterliche Stellungnahme

zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess

Ausschuss-Drucksache 18(6)334

im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
am 31. Mai 2017

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin
Vorsitzender der Gesellschaft für Freiheitsrechte e.V. (GFF)

ulf@buermeyer.de

Berlin, den 29. Mai 2017

We live in dangerous times, but we are not the first generation
of Americans to face threats to our security. Like those before us,
we will be judged by future generations on how we react to this crisis.
And by that I mean not just whether we win … but also
whether, as we fight that war, we safeguard for our citizens the
very liberties for which we are fighting.[1]

Robert Swan Mueller III am 13. Juni 2003
Director, Federal Bureau of Investigation

Wesentliche Ergebnisse

1. „Staatstrojaner" sind ein außerordentlich eingriffsintensives Instrument. Ihr Einsatz in Form der **Online-Durchsuchung geht** hinsichtlich der Eingriffstiefe **noch über die akustische Wohnraumüberwachung hinaus**: Wer Rechner und Smartphones überwacht, der kann deren Mikrofone aktivieren und alle Datenspeicher auslesen, weiß also nahezu alles über die Zielperson. Daher stellt die Online-Durchsuchung gegenüber dem „Großen Lauschangriff" ein Mehr dar, kein Aliud oder gar ein Minus.

2. Die vorgesehene Rechtsgrundlage zur **Online-Durchsuchung** ist insbesondere wegen ihres allzu weiten Straftatenkatalogs **verfassungsrechtlich nicht zu rechtfertigen**, denn sie steht mit den Vorgaben des BVerfG (BVerfGE 120, 274) nicht im Einklang.

3. Die vorgesehene Rechtsgrundlage zur **Quellen-TKÜ** geht ebenfalls über den Rahmen dessen hinaus, was das BVerfG als Eingriff allein in Art. 10 Abs. 1 GG für zulässig gehalten hat. Die geplanten Maßnahmen nach § 100a Abs. 1 Satz 2 und 3 StPO-E beziehen sich nicht nur auf die laufende Kommunikation und stellen daher gerade keine Quellen-TKÜ, sondern eine **verfassungswidrige** Online-Durchsuchung dar.

---

1 Wir leben in gefährlichen Zeiten, aber wir sind nicht die erste Generation von Amerikanern, die sich mit Gefahren für ihre Sicherheit konfrontiert sieht. Wie die Menschen früher, werden auch wir von späteren Generationen danach beurteilt werden, wie wir auf diese Krise reagieren. Und damit meine ich nicht die Frage, ob wir gewinnen, sondern ob wir – während wir diesen Krieg führen – unseren Bürgern ebenjene Freiheiten bewahren, für die wir Krieg führen. – Zitiert nach https://archives.fbi.gov/archives/news/speeches/protecting-americans-against-terrorism (letzter Abruf: 28. Mai 2017), Übersetzung des Verfassers.

4. Gravierende Bedenken bestehen auch gegen die verfahrensrechtliche Ausgestaltung des Einsatzes von Staatstrojanern: Die §§ 100a ff. StPO stellen in keiner Weise sicher, dass die von den Ermittlungsbehörden einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit und Resistenz gegen Manipulationsversuche erfüllen. Hier **fehlen Regelungen** sowohl **über die** an Staatstrojaner zu stellenden **technischen Anforderungen**, die wenigstens im Verordnungswege erlassen werden müssen, als auch über eine **obligatorische unabhängige Prüfung**, dass ein Staatstrojaner diese Anforderungen tatsächlich erfüllt.

5. Zudem schaffen die §§ 100a, 100b StPO-E ein massives Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen (!), um Systeme von Zielpersonen gegebenenfalls gem. §§ 100a ff. StPO-E „hacken" zu können. Die gesellschaftlichen Folgen einer solchen **Kultur der kalkulierten IT-Unsicherheit** können erheblich sein, wie jüngst der Ausbruch des „wannacry"-Trojaners deutlich gemacht hat. Diese Fehlanreize sollten durch ein bisher **fehlendes Verbot der Ausnutzung von Sicherheitslücken** verhindert werden, die auch den Herstellern noch unbekannt sind. Hierzu wird unten ein Formulierungsvorschlag gemacht.

6. Schließlich enthält die Formulierungshilfe **unzureichende Regelungen zum Schutz von Berufsgeheimnisträgern**, insbesondere Journalistinnen und Journalisten. Denn sie schließt Eingriffe ihnen gegenüber nicht zuverlässig aus, sondern überlässt solche Maßnahmen einer nicht zu prognostizierenden Abwägungsentscheidung.

7. Die vorgesehenen Maßnahmen sind schließlich auch **in keiner Weise eilbedürftig**, da für den Bereich der Terrorismusabwehr bereits Rechtsgrundlagen im BKAG für den Einsatz von Staatstrojanern in Kraft sind, diese aber bisher kaum genutzt werden, weil ohnehin keine hinreichend praxistauglichen Trojaner zur Verfügung stehen. Zudem verfügen die Ermittlungsbehörden über vielfältige Möglichkeiten, anderweitig an die gewünschten Daten zu gelangen. Der Entwurf sollte daher insgesamt überarbeitet, in zahlreichen Punkten geändert und in der 19. Wahlperiode erneut beraten werden. In der vorliegenden Form ist die „Formulierungshilfe" mit allem Nachdruck abzulehnen.

Einzelaspekte

Eine erschöpfende Stellungnahme zu einem 30 Seiten umfassenden, inhaltlich sehr komplexen de-facto-Gesetzentwurf würde deutlich mehr Zeit erfordern als die rund zehn Tage, die den Sachverständigen zur Verfügung standen. Hingewiesen werden kann daher nur auf ausgewählte rechtlich besonders bedenkliche Vorschläge oder sonst änderungsbedürftige Aspekte des Entwurfs. Ist eine Regelung in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies keineswegs dahingehend zu verstehen, dass sie als unbedenklich anzusehen wäre.

1.) Einführung

Der Entwurf des BMJV sieht mit Ermächtigungen für den Einsatz von staatlich kontrollierter Überwachungs-Software („Staatstrojaner“) die mit Abstand weitgehendsten Eingriffe in Grundrechte vor, die die Strafprozessordnung zur Informationsgewinnung kennt. Insbesondere die vorgesehene Online-Durchsuchung umfasst all jene Eingriffe, die bisher bereits nach § 100c StPO als akustische Wohnraumüberwachung („Großer Lauschangriff“) zulässig waren, und fügt ihnen noch weitere erhebliche Eingriffe hinzu: Durch Infektion der informationstechnischen Systeme von Beschuldigten soll nämlich ermöglicht werden

- die heimliche Auswertung der gesamten laufenden und früheren Kommunikation,

- die Auswertung aller digital gespeicherten Inhalte auf den infizierten Systemen sowie

- ein „Großer Spähangriff“ auf die Umgebung des überwachten Systems, sofern es über eine Kamera-Funktion verfügt wie heute jedes Smartphone, jedes Tablet und nahezu jeder Laptop[2].

[2] Eine solche Maßnahme wäre in einer Wohnung an Art. 13 GG zu messen und nur für präventive Zwecke zulässig (Art. 13 Abs. 4 GG). § 100b StPO-E enthält aber keine entsprechende Begrenzung, vielmehr wäre eine

Die Bedeutung der geplanten Regelung wird deutlich, wenn man sich vor Augen führt, dass Computer und Smartphones heute oft eine unermessliche Fülle an Informationen[3] enthalten: alltägliche bis intimste Emails und Nachrichten wie SMS oder WhatsApp, Terminkalender, Kontakte, Kontoumsätze, Tagebücher und Social-Media-Daten. Mit Speicherkapazitäten im Giga- bis Terabyte-Bereich enthalten sie ein weitgehendes digitales Abbild unseres Lebens. Moderne informationstechnische Systeme gleichen so einem ausgelagerten Teil des Gehirns. Erhalten Ermittlungsbehörden Zugriff auf diese Datenmengen, können sie die Besitzer der Systeme so vollständig ausspähen, dass sie sie nicht selten besser kennen als die Besitzer sich selbst. Hinzu kommt bei der Online-Durchsuchung die Möglichkeit des Live-Zugriffs – Ermittler können den Betroffenen also virtuell heimlich über die Schulter blicken und ihnen so beim Denken zuschauen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen[4].

Dieser unvergleichlich tiefe Einblick in das Wissen und Fühlen eines Menschen macht den Einsatz von Trojanern in einem Rechtsstaat unvergleichlich heikel. Wie keine andere Ermittlungsmethode erlaubt es die Online-Durchsuchung, Menschen zum Objekt der Ausspähung zu machen. Gegen keine andere Methode sind Beschuldigte – für die immerhin die Unschuldsvermutung gilt – so wehrlos, denn der direkte Zugriff auf das System dient gerade dem Zweck, Verschlüsselungsverfahren zu umgehen, also den informationellen Selbstschutz ins Leere laufen zu lassen. Keine andere Ermittlungsmethode bietet insgesamt ein vergleichbares totalitäres Potential: Selbst der „Große Lauschangriff“ beschränkt sich auf die akustische Wahrnehmung dessen, was aktuell in einer Wohnung geschieht. Wird ein Rechner oder Smartphone mit einem Trojaner infiziert, so erlaubt dies ebenfalls einen Lauschangriff auf dessen Umgebung.

---

solche Maßnahme vom Wortlaut der Norm gedeckt. Der Formulierungsvorschlag des BMJV überlässt es mithin dem einzelnen Kriminalbeamten, der eine Online-Durchsuchung durchführt, ob er die Grenzen des GG einhält und eine Funktion zur Video-Überwachung nicht aktiviert. Verfahrensrechtlich sichergestellt ist dies nirgends.

[3] Vgl. bereits BVerfGE 120, 274, 303 ff. (2008).

[4] BVerfGE 120, 274, 323.

Hinzu kommt bei der Online-Durchsuchung aber ein heimlicher Zugriff auf mitunter über Jahrzehnte angesammelte digitale Daten sowie ein großer Spähangriff, indem auf die Kameras der infizierten Systeme zugegriffen wird. Die Eingriffstiefe einer Online-Durchsuchung geht daher über die einer akustischen Wohnraumüberwachung nochmals deutlich hinaus.

Neben einer ganz gravierenden Eingriffstiefe, auf die noch einzugehen sein wird, weisen die vorgesehene Regelungen zum Einsatz von Staatstrojanern auch verfahrensrechtliche Defizite auf, die miteinander verzahnt sind: Die vorgesehenen Regelungen in der Fassung des Entwurfs überlassen es den Ermittlungsbehörden und dem Gericht, die technischen Anforderungen an Software zu definieren, die in informationstechnische Systeme eingreift, obwohl von ihnen – ebenso wie von den verfahrensrechtlichen Vorkehrungen, um ihre Einhaltung sicherzustellen – das Gewicht des Grundrechtseingriffs maßgeblich bestimmt wird. Dies ist mit dem Gebot des Grundrechtsschutzes durch Verfahrensgestaltung ebenso wie mit dem Wesentlichkeitsgrundsatz unvereinbar.

Außerdem lassen die Normen den Ermittlungsbehörden und dem Gericht Raum für den Missbrauch von Sicherheitslücken in informationstechnischen Systemen (sog. *Zero Day Exploits* oder kurz *0days*[5]) zum Zwecke der Infiltration. Dies schafft fatale Fehlanreize, weil deutsche Behörden damit ein erhebliches Interesse hätten, Sicherheitslücken in informationstechnischen Systemen nicht an die Hersteller zu melden, sodass sie geschlossen werden können, sondern sie vielmehr zu horten. Dies ist der Mechanismus, der dem jüngst unter dem Stichwort „wannacry“ bekannt gewordenen Trojaner-Ausbruch zugrunde lag: Der US-amerikanische Geheimdienst NSA hatte seit Jahren Kenntnis von der Lücke, meldete sie aber dem Hersteller Microsoft nicht, sodass dieser seine Systeme nicht nachbessern konnte. Erst nachdem Unbekannte die Informationen über die Lücke der NSA gestohlen und sie im Internet veröffentlicht hatten, gab Microsoft für einige (nicht alle) betroffenen Systeme Korrekturen heraus. Diese konnten in der kurzen Zeit bis zum Ausbruch von „wannacry“ aber nicht mehr flächendeckend

[5] Gesprochen: Oh-Days.

eingespielt werden. Dies ist nur ein Beispiel für die real bestehende Missbrauchsgefahr aus jüngster Vergangenheit.

Die vorgeschlagenen Regelungen sind vor diesem Hintergrund insgesamt verfassungsrechtlich wie rechtspolitisch deutlich misslungen.

2.) Vorgaben des Bundesverfassungsgerichts

Der unvergleichlichen Gefahren staatlicher Überwachungssoftware war sich auch das Bundesverfassungsgericht bewusst, als es im Jahre 2008 über eine Rechtsgrundlage für Staatstrojaner im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen zu entscheiden hatte. Der Erste Senat leitete aus der Menschenwürdegarantie des Art. 1 Abs. 1 GG sowie dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ ab (BVerfGE 120, 274). Wie alle Grundrechte mit Ausnahme der Menschenwürdegarantie gilt es zwar nicht schrankenlos. Doch geht das BVerfG von einem außerordentlichen Gewicht aller Eingriffe in dieses „Computer-Grundrecht“ aus. Denn eine heimliche technische Infiltration ermöglicht die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten[6]. Weiter vertieft wird der Eingriff durch seine unvermeidliche Streubreite[7]. Angesichts dieser Intensität entspricht ein Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, selbst im Rahmen einer präventiven Zielsetzung

> *„nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen*

[6] BVerfGE 120, 274, 323.
[7] BVerfG a.a.O.

Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern."[8]

Zudem muss die Gefahr ganz bestimmten besonders wichtigen Rechtsgütern drohen:

„Ein derartiger Eingriff 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."*[9]

Das bedeutet im Umkehrschluss:

„Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine ***existentielle Bedrohungslage*** *nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die ... die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt."*[10]

Selbst präventiv ist der Einsatz von Staatstrojanern mithin nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr vorliegen, die für 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

---

[8] BVerfGE 120, 274, 326.
[9] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.
[10] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.

Menschen berührt, besteht. Andere Rechtsgüter wie etwa Eigentum oder Vermögen können einen Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hingegen per se nicht rechtfertigen.

Eingriffe mittels Staatstrojanern sind hingegen nicht am „Computer-Grundrecht", sondern lediglich am Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG zu messen, wenn ausschließlich „laufende Kommunikation" mitgeschnitten wird. Im Falle einer solchen Online-Durchsuchung „light" – genannt Quellen-Telekommunikationsüberwachung oder auch Quellen-TKÜ – muss jedoch durch „technische Vorkehrungen und rechtliche Vorgaben"[11] sichergestellt werden, dass sich die Datenerhebung wirklich auf die laufende Kommunikation beschränkt.

Dies ist insbesondere deswegen bedeutsam, weil eine Quellen-TKÜ technisch von einer vollumfänglichen Online-Durchsuchung nicht zu unterscheiden ist: In beiden Fällen muss das Zielsystem mittels eines Staatstrojaners infiziert werden, was die Integrität und Vertraulichkeit des Systems aufhebt. Dieser Eingriff muss sodann jedoch durch „technische Vorkehrungen und rechtliche Vorgaben" gleichsam kastriert werden, damit ausschließlich laufende Kommunikation erhoben werden kann.

Daraus ergibt sich sogleich die besondere Gefährlichkeit von Quellen-TKÜ-Maßnahmen: Sie laufen stets Gefahr, bei einer Fehlfunktion des eingesetzten Trojaners oder bewusst pflichtwidrigem oder gar nur fahrlässigem Handeln des bedienenden Personals in eine vollumfängliche Online-Durchsuchung abzugleiten, die wesentlich höheren verfassungsrechtlichen Anforderungen unterliegt[12]. Neutrale IT-Sicherheits-Experten außerhalb der Ermittlungsbehörden vertreten daher praktisch einhellig die Ansicht, dass die Anforderungen an eine Quellen-TKÜ technisch nicht zu erfüllen sind[13]. Das BVerfG hat eindeutig verlangt, dass eine solche Maßnahme zu unterbleiben hat, solange dies technisch nicht möglich ist[14].

---

[11] BVerfGE 120, 274, 309.
[12] BVerfGE 120, 274, 309.
[13] Vgl. die Wiedergabe in BVerfGE 120, 274, 309, die sich der Senat zu eigen macht.
[14] BVerfG a.a.O.

3.) Schranken-Transfer von präventiven zu repressiven Eingriffen

Bei einer Regelung für den Strafprozess ist neben der Umsetzung der oben genannten Vorgaben des BVerfG auch eine Transferleistung zu erbringen. Die Anforderungen des BVerfG an Eingriffe in das Computer-Grundrecht, also an die Online-Durchsuchung, beziehen sich unmittelbar nur auf den *präventiven* Einsatz von Staatstrojanern, weil nur dieser Gegenstand des Verfassungsbeschwerdeverfahrens war. Zu fragen ist also, welche Eingriffsschwellen für *repressive* Eingriffe in das Computer-Grundrecht gelten, denn nur solche können in der Strafprozessordnung geregelt werden (Art. 74 Abs. 1 Nr. 1 GG).

Aus verfassungsrechtlicher Perspektive ist dies vergleichsweise leicht zu beantworten: Während bei präventiven Maßnahmen unmittelbar die bedrohten Rechtsgüter und der Grad der Gefahr in die Abwägung eingestellt werden können, dient eine repressive Regelung zunächst „nur“ der Durchsetzung des staatlichen Strafanspruchs und nur mittelbar dem Rechtsgüterschutz. Da die Funktionsfähigkeit der Strafrechtspflege jedoch nicht etwa Selbstzweck ist, sondern ihrerseits allein dem Schutz von Rechtsgütern dient, ist bei Eingriffsermächtigungen zu repressiven Zwecken stets zunächst der Nebel des „Meta-Rechtsguts“ Funktionsfähigkeit der Strafrechtspflege zu lichten und zu fragen, welche Rechtsgüter durch die Strafrechtspflege letztlich konkret geschützt werden sollen.

Darüber hinaus ist insbesondere auf der Ebene der Verhältnismäßigkeit zu berücksichtigen, dass – bildhaft gesprochen – bei einem Eingriff in das Computer-Grundrecht zu präventiven Zwecken (hoffentlich) noch verhindert werden, dass „das Kind in den Brunnen fällt“, also eine Rechtsgutsverletzung tatsächlich eintritt. Ist das Kind indes bereits gestürzt, so dienen die dann nur noch möglichen repressiven Eingriffe primär der Sanktionierung der Verantwortlichen, können das Kind aber nicht wieder zum Leben erwecken, da die Rechtsgutsverletzung bereits eingetreten ist. Da wie gezeigt die Strafrechtspflege als solche keinen verfassungsrechtlichen Rang hat, sondern dieser sich alleine aus den durch sie zu schützenden Rechtsgütern ableitet, sind an Eingriffe in das Computer-Grundrecht zu repressiven Zwecken jedenfalls keine geringeren Anforderungen zu stellen als an präventive Eingriffe. Mit Blick auf die

Gewichtung von Prävention und Repression im Hinblick auf den verfolgten Rechtsgüterschutz sind bei der Verfolgung allein repressiver Ziele eher höhere Anforderungen zu stellen. Denn es wird am Ende „nur“ die Sanktionierung eines bereits irreversibel eingetretenen Rechtsgutsverstoßes verfolgt. Dass von Verfassungs wegen deutlich größere Spielräume für präventive als für repressive Eingriffe bestehen zeigt sich schließlich auch an der Wertung des Art. 13 GG (Unverletzlichkeit der Wohnung), der zu präventiven Zwecken (Art. 13 Abs. 3 GG) weitaus mehr Eingriffe zulässt als zu repressiven Zwecken (Art. 13 Abs. 4 GG).

Im Lichte dessen ist daher zunächst maßgeblich, ob die Strafnorm ihrerseits *unmittelbar* dem Rechtsgüterschutz dient, letztlich also im repressiven Gewande der Abwehr einer konkreten Gefahr dient. So mag es sich etwa in Einzelfällen des § 129a StGB (Bildung einer terroristischen Vereinigung) oder des § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) verhalten, sofern die Planungen sich zu einer konkreten Rechtsgutsgefährdung verdichtet haben, oder auch bei Erfolgsdelikten, die das Versuchsstadium erreichen.

In der Regel aber wird bei strafrechtlichen Ermittlungen *keine konkrete Gefahr* für ein überragend wichtiges Rechtsgut mehr gegeben sein; insbesondere ist dies bei den meisten Ermittlungsverfahren wegen Organisationsdelikten gerade nicht der Fall, und liegt doch ausnahmsweise eine konkrete Gefahr vor, so ist neben der Strafverfolgung parallel auch der Bereich der Gefahrenabwehr eröffnet, dessen Zulässigkeit und Umfang sich wiederum nach den existierenden Vorgaben hierzu richtet. In den meisten hier in Rede stehenden Fällen indes, bei denen es lediglich noch um Grundrechtseingriffe zu repressiven Zwecken ohne jede konkrete Gefahr geht, müsste also die Durchsetzung des staatlichen Strafanspruchs verfassungsrechtlich zumindest von gleicher Wertigkeit sein wie die Abwehr einer konkreten Gefahr für die vom BVerfG aufgezählten Rechtsgüter. Dies wird man allenfalls bei Straftatbeständen annehmen können, die die vom BVerfG genannten „überragend wichtigen“ Rechtsgüter schützen sollen, und dies auch nur dann, wenn die Verletzungen einen erheblichen Schweregrad erreichen. Dies gebietet auch die Verfassungsrang genießende und in Art. 6 Abs. 2 EMRK verankerte

Unschuldsvermutung, die im Rahmen der Verhältnismäßigkeitsprüfung bei Ermittlungseingriffen zu beachten ist.

4.) Die Regelung zur Online-Durchsuchung (§§ 100b, 100c StPO-E)

Gemessen insbesondere an diesen Vorgaben ist die vorgesehene Ermächtigungsgrundlage für Online-Durchsuchungen verfassungsrechtlich nicht zu rechtfertigen.

a) Straftaten-Katalog

So überschreitet insbesondere der im Entwurf vorgesehene Katalog von Straftaten (§ 100b Abs. 2 StPO-E), zu deren Aufklärung eine Online-Durchsuchung nach § 100b Abs. 1 StPO-E zulässig sein soll, den Rahmen des verfassungsrechtlich Möglichen. Denn der Straftatenkatalog, der weitgehend dem der klassischen Telekommunikationsüberwachung (§ 100a Abs. 2 StPO) entspricht, enthält viele Straftatbestände, die Rechtsgüter schützen, für die das BVerfG selbst eine präventive Online-Durchsuchung **nicht** für zulässig hält. Mit anderen Worten dürfte eine Online-Durchsuchung in diesen Fällen nicht einmal zur Abwehr einer konkret drohenden Gefahr für dieses Rechtsgut eingesetzt werden. Um es noch deutlicher zu formulieren: Wenn allein eine Online-Durchsuchung die Gefahr abwenden könnte, so müsste der Staat von Verfassungs wegen die drohende Rechtsgutsverletzung – etwa eine Verletzung des Vermögens – gleichwohl geschehen lassen. Wenn jedoch selbst eine potentiell noch abzuwendende Verletzung eines bestimmten Rechtsguts eine Online-Durchsuchung nicht rechtfertigen könnte, dann vermag die bloße Verfolgung einer (vermuteten) Verletzung desselben Rechtsguts dies umso weniger – schließlich ist „das Kind bereits in den Brunnen gefallen“, das Rechtsgut nicht mehr zu retten. Folglich ist eine repressive Online-Durchsuchung zur Verfolgung von Straftaten schlechthin unzulässig, wenn durch die mutmaßliche Straftat lediglich Rechtsgüter verletzt wurden, zu deren Schutz vor konkreter Gefahr eine Online-Durchsuchung nicht angeordnet werden dürfte. Dies betrifft alle Rechtsgüter mit Ausnahme der vom BVerfG als überragend wichtige Rechtsgüter bezeichneten:

> *„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.“*[15]

Bei den Katalogtaten aus dem StGB, die gemäß § 100b Abs. 2 Nr. 1 StPO-E eine Online-Durchsuchung sollen rechtfertigen können, betrifft dies insbesondere solche, die primär Vermögen oder Eigentum schützen, also

- § 100b Abs. 2 Nr. 1 lit. c StPO-E (Geld- und Wertzeichenfälschung),
- § 100b Abs. 2 Nr. 1 lit. h StPO-E (Bandendiebstahl),
- § 100b Abs. 2 Nr. 1 lit. i und j StPO-E (bestimmte Formen von Raub oder räuberischer Erpressung, sofern es nicht tateinheitlich zu Körperverletzungen gekommen ist),
- § 100b Abs. 2 Nr. 1 lit. k StPO-E (Qualifikationen der Hehlerei)
- § 100b Abs. 2 Nr. 1 lit. l StPO-E (Geldwäsche u. ä.)

Ebenso zweifelhaft ist der Bezug zum Katalog der vom BVerfG genannten „überragend wichtigen“ Rechtsgüter bei den Straftaten gegen das Asyl- und Aufenthaltsgesetz. Jedenfalls die oben genannten Katalogtaten sowie die Taten der § 100b Abs. 2 Nr. 2 und 3 StPO-E sollten daher ersatzlos entfallen.

b) Verhältnismäßigkeit im engeren Sinne

Zudem ist die Regelung auch insoweit unzulänglich, als sie nicht hinreichend sicherstellt, dass es sich bei den mutmaßlichen Straftaten, zu deren Verfolgung eine Online-Durchsuchung möglich sein soll, auch tatsächlich um äußerst schwere Straftaten gegen die betreffenden Rechtsgüter handelt. Zwar soll nach § 100b Abs. 1 Nr. 2 StPO-E zu prüfen sein, ob „die Tat auch im Einzelfall besonders schwer wiegt“. Diese Prüfung durch

[15] BVerfGE 120, 274, 328.

die Kammer bzw. den Senat (vgl. § 100e Abs. 2 StPO) ist indes in keiner Weise angeleitet, weil jeder Hinweis darauf fehlt, wann dieses Kriterium erfüllt sein soll. So bleibt die Subsumtion unter dieses Tatbestandsmerkmal letztlich eine Frage des richterlichen Bauchgefühls, ob eine Tat nach bestehender Akten- und damit Verdachtslage „wirklich schlimm“ war oder nicht.

Im Bereich der Strafverfolgung gibt es indes ein vergleichsweise einfach zu handhabendes Kriterium für die Schwere einer Tat: die im Einzelfall zu erwartende Strafe. Die Einschätzung der Straferwartung ist im Bereich ermittlungsrichterlicher Entscheidungen auch gängige Praxis, nämlich bei der Entscheidung über Anträge auf Erlass eines Haftbefehls, wo die Straferwartung zentralen Einfluss auf die Frage hat, ob Fluchtgefahr (§ 112 Abs. 2 Nr. 2 StPO) anzunehmen ist oder nicht. Auch Spruchrichter haben aus ihrer täglichen Praxis in aller Regel in gutes Judiz, welche Strafe in etwa angemessen sein könnte. Freilich sind im Ermittlungsverfahren noch nicht alle Umstände bekannt, die in einer Hauptverhandlung für die Strafhöhe Bedeutung erlangen können. Dem kann jedoch durch plausible Annahmen über nach dem Stand der Ermittlungen wahrscheinliche Umstände mühelos begegnet werden – auch dies ist ständige Praxis im Ermittlungsverfahren. Daher sollte der bisher konturenlose Begriff der „besonderen Schwere der Tat“ durch ein Tatbestandsmerkmal der im Einzelfall zu erwartenden Strafe präzisiert werden. Angesichts der beispiellosen Eingriffstiefe der Online-Durchsuchung erscheint diese Maßnahme jedenfalls nicht unterhalb einer konkret zu erwartenden Freiheitsstrafe von 5 Jahren angemessen. Milderungen wegen erheblich verminderter Schuldfähigkeit sollten zur Vereinfachung außer Betracht bleiben, weil sie im Ermittlungsverfahren typischerweise noch nicht ohne Weiteres bestimmbar sind.

Formulierungsvorschlag:

An § 100b Abs. 1 werden folgende Sätze 2 und 3 angefügt:

„Eine Tat wiegt besonders schwer (Satz 1 Nr. 2), wenn im konkreten Fall nach dem jeweiligen Stand der Ermittlungen eine Freiheitsstrafe nicht unter fünf Jahren zu erwarten ist. Milderungen gemäß §§ 21, 49 Absatz 1 StGB bleiben außer Betracht.“

c) Wertungswidersprüche beim Kernbereichsschutz

Wie oben bereits gezeigt geht die Eingriffstiefe der Online-Durchsuchung über die der akustischen Wohnraumüberwachung deutlich hinaus – nicht zuletzt, weil praktisch alle im Wege einer akustischen Wohnraumüberwachung zu erwartenden Kenntnisse auch mittels einer Online-Durchsuchung zu erlangen sind, indem heimlich das Mikrofon eines Laptops oder Smartphones aktiviert wird. Die Online-Durchsuchung stellt gegenüber dem „Großen Lauschangriff" also ein – erhebliches – Plus dar, kein Aliud oder gar Minus.

Diesem Stufenverhältnis trägt indes die Regelung des Schutzes des Kernbereichs privaten Lebensgestaltung in § 100d Abs. 3 und 4 StPO-E nicht ausreichend Rechnung. Für die akustische Wohnraumüberwachung ist – zu Recht – ein vergleichsweise strenger Schutz des Kernbereichs vorgesehen. Maßnahmen dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Insbesondere ist die Maßnahme „unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden" (§ 100d Abs. 4 Satz 2 StPO-E) – mit anderen Worten muss „live" überwacht werden. Nach § 100d Abs. 3 StPO-E soll ein vergleichbarer Schutz für die Online-Durchsuchung hingegen nicht gelten. Hier ist lediglich „soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden". Mit anderen Worten soll für die schwerer wiegende Maßnahme der Online-Durchsuchung ein weniger zuverlässiger und weniger weitgehender Schutz des Kernbereichs privater Lebensgestaltung gelten – das leuchtet nicht ein. Die Differenzierung in § 100d Abs. 3 und 4 StPO-E sollte daher entfallen.

5.) Die Regelung zur Quellen-TKÜ (§ 100a StPO-E)

Noch weiter als die Regelung zur Online-Durchsuchung verfehlt die vorgeschlagene Norm zur Quellen-TKÜ die Vorgaben insbesondere aus der Entscheidung des BVerfG zur Online-Durchsuchung (BVerfGE 120, 274). Wie dargestellt ist *conditio sine qua non* einer

nur an Art. 10 Abs. 1 GG zu messenden Quellen-TKÜ – sonst liegt eine am „Computer-Grundrecht“ zu messende Online-Durchsuchung vor –, dass ausschließlich „laufende Kommunikation“ erhoben wird[16]. Hierüber setzt sich der Entwurf jedoch hinweg: Gemäß § 100a Abs. 1 Satz 3 StPO-E soll über die laufende Kommunikation hinaus auch die Erhebung „gespeicherter Inhalte und Umstände der Kommunikation“ – also das Auslesen quasi „kondensierter“ Kommunikation – unter den erleichterten Voraussetzungen der Quellen-TKÜ ausgelesen werden dürfen. Dies steht in einem offenen Widerspruch zu den Vorgaben des BVerfG, welches wie gezeigt nur die Erhebung *laufender* und nicht früherer Kommunikation aus dem Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme herausdefiniert hat.

Dessen war sich die Bundesregierung durchaus bewusst. Zur Begründung verweist die „Formulierungshilfe“ indes auf eine klassische Analogie: Ebenso wie bei laufender Kommunikation erscheint es ihnen auch bei früherer Kommunikation „verfassungsrechtlich nicht geboten, die wegen der besonderen Sensibilität informationstechnischer Systeme ... aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das Computer-Grundrecht] anzuwenden“[17]. Indes ist bereits die Figur der Quellen-TKÜ für laufende Kommunikation wie dargestellt eine Ausnahme von der Regel, dass Trojaner-Einsätze einen Eingriff in dieses Grundrecht darstellen; hinzu kommt, dass diese Ausnahme aus technischer Sicht ihrerseits eine fragwürdige, da kontrafaktische ist. Und Ausnahmen können gerade nicht analog angewendet werden, sondern sind restriktiv auszulegen. Dies lässt es unvertretbar erscheinen, aufgrund letztlich willkürlicher Überlegungen zur „Gebotenheit“ eines Grundrechtsschutzes die klaren Vorgaben des BVerfG zur Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ zu übergehen.

Neben das rechtstechnische tritt indes ein weiteres, informationstechnisches Argument. Selbst die Entwurfsverfasser räumen ein, dass nicht sämtliche gespeicherte Kommunikation als Quellen-TKÜ auslesbar sein soll, sondern nur solche

---

[16] Vgl. zu Begriff und Inhalt eingehend *Buermeyer* StV 2013, 470.
[17] „Formulierungshilfe“, Seite 20.

Kommunikationsinhalte, die nach Erlass eines Beschlusses gem. § 100a StPO gespeichert wurden. Um diese Prüfung ausführen zu können, müsste der Trojaner – wie die Entwurfsbegründung wiederum zugesteht – zunächst *alle* gespeicherten Kommunikations-Inhalte auslesen und auswerten, um entscheiden zu können, welche davon nach dem Beginn der Maßnahme gespeichert wurden, sodass sie als Quellen-TKÜ erhoben werden können. In dieser *vollumfänglichen*, zeitlich naturgemäß nicht begrenzten Auswertung der gespeicherten Kommunikationsinhalte läge jedoch bereits eine dem Staat zuzurechnende Kenntnisnahme und damit eine Online-Durchsuchung, auch wenn die Daten nicht ausgeleitet, sondern noch „vor Ort" auf dem infizierten System der Zielperson analysiert werden. Mit anderen Worten schlägt der Entwurf eine stillschweigende Online-Durchsuchung vor, um festzustellen, welche ehemaligen Kommunikationsinhalte der Staatstrojaner unter den leichteren Voraussetzungen einer Quellen-TKÜ ausleiten darf. Ein solcher Taschenspielertrick des Gesetzgebers dürfte vor dem BVerfG kaum Bestand haben, zumal es sich der Sache nach um eine Ausweitung der vom Ersten Senat erkennbar als eng umrissene Ausnahme von der Online-Durchsuchung konzipierten Quellen-TKÜ handelt.

Schließlich ist zu berücksichtigen, dass eine solche Ausweitung der Quellen-TKÜ auf frühere Kommunikation auch im Tatsächlichen auf allzu schwankendem Grund stünde. Denn schon ein aus welchen Gründen auch immer falscher Zeitstempel einer gespeicherten Nachricht würde dazu führen, dass Inhalte ausgelesen würden, die vor Beginn einer Maßnahme gespeichert wurden. Dies jedoch würde bewirken, dass statt der angeordneten Quellen-TKÜ eine „irrtümliche" Online-Durchsuchung durchgeführt würde. Der Irrtum ändert jedoch nichts an der damit verbundenen Eingriffstiefe und die anzusetzenden verfassungsrechtlichen Anforderungen an eine Rechtfertigung dieses Eingriffs.

Angesichts all dessen muss § 100a Abs. 1 Satz 3 StPO entfallen; gleiches gilt für dessen verfahrensrechtliche Umsetzung in § 100a Abs. 5 Nr. 1 lit. b StPO-E. Dies ließe sich gesetzestechnisch wie folgt erreichen:

Formulierungsvorschlag

1. § 100a Abs. 1 Satz 3 wird gestrichen.

2. § 100a Abs. 5 Nr. 1 wird wie folgt gefasst:

„1. ausschließlich die laufende Telekommunikation (Absatz 1 Satz 2) überwacht und aufgezeichnet werden kann,“

6.) Mangelhafte verfahrensrechtliche Sicherungen des Trojaner-Einsatzes

Die Eingriffsbefugnisse der § 100a Abs. 5, § 100b Abs. 1 StPO-E enthalten zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des „Eingreifens“, etwa eine Beschränkung von Veränderungen auf das Notwendige oder einen Schutz vor unberechtigten Zugriffen durch Dritte. Diese als solche begrüßenswerten Regelungen finden indes im Gesetz keinerlei verfahrensrechtliche Absicherung. Gemessen an den Anforderungen an die Anordnung und ihre Begründung (§ 100e Abs. 3 und 4 StPO-E) muss das „technische Mittel“, dessen Einsatz beabsichtigt ist – also immerhin der einzusetzende Staatstrojaner (!) – nicht einmal benannt, geschweige denn in seinen technischen Spezifikationen näher bezeichnet werden. Dies ermöglicht nach dem Wortlaut des Entwurfs den Einsatz beliebiger Staatstrojaner nach Gutdünken der Ermittlungsbehörden, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann. Das ist angesichts der erheblichen Eingriffstiefe der Online-Durchsuchung, aber auch der massiven Gefahren einer schleichenden Ausweitung eines Quellen-TKÜ hin zu einer Online-Durchsuchung, denen nur durch die Gestaltung des Trojaners entgegengewirkt werden kann, in jeder Hinsicht unangemessen. Jedenfalls nach den Vorstellungen des Entwurfs soll offenbar jede Steckdose[18] strengeren Anforderungen an die technisch sichere Gestaltung unterliegen als eine Software, die zur Ausspähung von Bürgerinnen und Bürgern eingesetzt werden soll. Das erscheint in einem Rechtsstaat unvorstellbar.

[18] Vgl. nur https://de.wikipedia.org/wiki/IEC_60309.

Die Verantwortung für die Prüfung der technischen Beschaffenheit des einzusetzenden Staatstrojaners kann auch nicht auf die Richter abgewälzt werden, die die Maßnahme anordnen sollen. Zum einen müssten sie gezielt Rückfragen stellen, um überhaupt zu erfahren, welches technische Mittel eingesetzt werden soll und wie dieses im Einzelnen beschaffen ist. Zum anderen kann von dem zuständigen Ermittlungsrichter (bei der Quellen, TKÜ, vgl. § 100e Abs. 1 StPO-E) und der zuständigen Kammer bzw. dem Senat (bei der Online-Durchsuchung, vgl. § 100e Abs. 2 StPO-E) nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwenigen Zeit – wenigstens Tage, wohl eher Wochen – in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird kaum eine ein Gericht auf sich nehmen wollen, sodass man sich im Zweifel auf Beteuerungen der antragstellenden Staatsanwaltschaft verlassen wird, mit dem Staatstrojaner habe schon alles seine rechte Ordnung. Im Ergebnis ist daher zu besorgen, dass die Einhaltung der in §§ 100a, 100b StPO-E genannten, aber auch weiterer aus der Perspektive der Informationssicherheit gebotener technischer Anforderungen an Staatstrojaner allenfalls von den Ermittlungsbehörden (wohlwollend) geprüft werden wird.

Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ist ein derart blindes Vertrauen in die von den Ermittlungsbehörden einzusetzenden Staatstrojaner ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Dies gilt insbesondere angesichts des Umstands, dass die Software nach dem Wortlaut des Gesetzes durchaus von einem externen Anbieter stammen kann, sodass die Ermittlungsbehörden mitunter selbst nicht mit Sicherheit einzuschätzen vermöchten, welche Funktionen die einzusetzende Software ausführt. Ausdrücklich zu begrüßen ist in diesem Kontext, dass sich das Bundeskriminalamt nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-TKÜ soll diese einsatzbereit sein[19]. Der vorliegende Gesetzentwurf schließt aber gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum

[19] https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html

Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind.

Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Die durch einen Staatstrojaner zu erfüllenden Spezifikationen könnten etwa im Verordnungswege durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben werden. Der Gesetzentwurf sollte hierzu um eine entsprechende Verordnungsermächtigung ergänzt werden. Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Eine entsprechende Darlegung dessen sollte in den Katalog der obligatorischen Inhalte einer Anordnung (§ 100e Abs. 3 und 4 StPO-E) aufgenommen werden.

7.) Fehlanreize, die die Datensicherheit insgesamt schwächen

Zumindest ebenso schwer wie die geschilderten rechtlichen Bedenken gegen die fehlende Prüfung der Staatstrojaner wiegen indes die fatalen Fehlanreize, die die Norm für die Arbeit der Bundesbehörden – namentlich die im Aufbau befindliche „ZITIS“ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) – mit sich bringt. Nach §§ 100a, 100b StPO-E sollen Ermittlungsbehörden in informationstechnische Systeme „eingreifen“ dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen einer hoheitlichen Software, die Daten ausliest und an das BKA übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Der Entwurf definiert indes nicht weiter, wie der Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege[20]:

[20] Vertiefend zu den technischen Grundlagen *Buermeyer* HRRS 2007, S. 154 ff.

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle

- Aufspielen durch Hoheitsträger durch heimliches Betreten der Räumlichkeiten, in denen sich das System befindet

- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen EMail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde

- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*)

Es erschließt sich unmittelbar, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Art. 13 Abs. 1 GG ohne eine (bisher fehlende) spezifische Ermächtigungsgrundlage hierzu schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden eine E-Mail mit einem getarnten Staatstrojaner (kriminalistische List), soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken – wiewohl vom Wortlaut der §§ 100a, 100b StPO-E gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Bundesbehörden solche Lücken ausnutzen dürfen, so haben sie ein durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, gefundene oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Bundesbehörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu horten.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur Bundesbehörden diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für *0days* kauft, die Lücken zur Infiltration informationstechnischer Systeme missbrauchen – insbesondere auch Cyber-Kriminelle, die es beispielsweise darauf anlegen könnten, die betroffenen Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen. Im Ergebnis würden Bundesbehörden mitunter viele Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von der jeweiligen Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aussetzen, um Sicherheitslücken im Einzelfall selbst für Maßnahmen nach §§ 100a, 100b StPO ausnutzen zu können. – Und all dies nur, um mit Blick auf die verfolgte Sanktionierung einer Einzelperson wegen einer vermuteten Straftat den Sachverhalt aufzuklären oder den Aufenthaltsort des Beschuldigten zu ermitteln. Das weltweite Missbrauchsrisiko, das hier durch ein Horten von Sicherheitslücken eingegangen wird, steht in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck (bessere Strafverfolgung im Einzelfall).

Eine solche aus der Sicht einer Ermittlungsbehörde noch nachvollziehbare Güterabwägung verbietet sich aus der Perspektive des Gesetzgebers, der das Wohl der Allgemeinheit in den Blick zu nehmen hat. Nicht zuletzt hat sich die Bundesregierung politisch zur Förderung der IT-Sicherheit bekannt[21]. Damit sind Anreize für Bundesbehörden, die Cyber-Sicherheit in Deutschland und weltweit im Interesse einer möglicherweise einmal erforderlichen Gefahrenabwehr zu schwächen, schlechthin unvereinbar.

Die §§ 100a, 100b StPO-E sollten daher um ein explizites Verbot des Einsatzes von dem Hersteller eines informationstechnischen Systems bisher unbekannten Sicherheitslücken (sog. *0days*) ergänzt werden, um sicherzustellen, dass sich alle

[21] Vgl. die sog. Cyber-Sicherheitsstrategie für Deutschland 2016, abzurufen auf http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html

Bundesbehörden darum bemühen, ihnen bekannte Sicherheitslücken durch die Hersteller der Systeme so schnell wie möglich schließen zu lassen. Eine Sicherheitslücke, die dem Hersteller bereits bekannt ist, aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann hingegen auch aus der Perspektive der IT-Sicherheit ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems.

Formulierungsvorschlag

An § 100a Abs. 5 wird der folgende Satz 2 angefügt:

Für den Einsatz des technischen Mittels dürfen Sicherheitslücken des informationstechnischen Systems, die auf die fehlerhafte Gestaltung von Systemkomponenten durch ihre Hersteller zurückgehen, nur ausgenutzt werden, wenn die Sicherheitslücken den jeweiligen Herstellern bereits bekannt sind.

8.) Unzureichender Schutz von Berufsgeheimnisträgern, namentlich der Presse

Nach § 100d Abs. 5 StPO des Entwurfs sollen Online-Durchsuchung und akustische Wohnraumüberwachung in „den Fällen des § 53“ StPO nicht zulässig sein. Was auf den ersten Blick wie eine begrüßenswerte Regelung zum Schutz von Berufsgeheimnisträgern erscheint, erweist sich bei genauerer Betrachtung als jedenfalls rechtstechnisch wenig gelungen. Denn die Formulierung in „den Fällen“ des § 53 StPO könnte jedenfalls so verstanden werden, dass die in § 53 Abs. 1 Satz 1 genannten Personen nicht etwa umfassend geschützt sind, sondern nur, soweit tatsächlich ein Fall der berechtigten Zeugnisverweigerung nach § 53 StPO vorläge. Dies wiederum würde auch auf die Verhältnismäßigkeitsprüfung des § 53 Abs. 2 Satz 2 StPO verweisen und dazu führen, dass jedenfalls in vielen Fällen der Ausschluss von Online-Durchsuchung und „Großem Lauschangriff“ ausgerechnet gegenüber Journalistinnen und Journalisten nur wenig Wirkung entfalten würde.

Aus der Perspektive der Pressefreiheit – insbesondere des vom Schutzbereich des Art. 5 Abs. 1 GG umfassten Schutzes des Vertrauensverhältnisses zwischen Journalist und

Quelle – wäre ein solches Ergebnis fatal. Der Gesetzentwurf berücksichtigt hier nicht hinreichend, dass für die nach der ständigen Rechtsprechung des BVerfG von Art. 5 Abs. 1 GG geschützte [22] journalistische Recherche ein *absolutes* Vertrauen in den Informantenschutz erforderlich ist. Ein Schutz von Informantinnen und Informanten allein nach Maßgabe einer im Einzelfall nicht zu prognostizierenden Abwägung kommt aus der Sicht eines potentiellen Informanten einem insgesamt fehlenden Schutz gleich, weil er sich nicht darauf verlassen kann, dass seine Kommunikation mit einer Journalistin oder einem Journalisten nicht ausgespäht werden darf. Dies wiegt im Bereich der journalistischen Recherche umso schwerer, als potentielle Informanten – anders als etwa Menschen, die medizinische Behandlung benötigen – auf den Kontakt zur Presse im Zweifel verzichten werden.

Dabei ist auch in Rechnung zu stellen, dass Informanten brisante Informationen auch vergleichsweise risikolos ins Netz stellen können, wobei die Kollateralschäden für die von Leaks betroffenen Personen typischerweise erheblich höher sind als bei verantwortlichem „Durchstechen" von Informationen an die Presse, die Persönlichkeitsrechte berücksichtigen kann. Daraus folgt ein erhebliches öffentliches Interesse daran, dass Leaks an verantwortungsbewusste Journalistinnen und Journalisten und nicht etwa an Plattformen wie Wikileaks erfolgen. Gerade angesichts dessen erscheint der nur relative – und damit im Ergebnis nicht hinreichend belastbare – Ausschluss von Journalistinnen und Journalisten anachronistisch.

Formulierungsvorschlag

§ 100d Abs. 5 Satz 1 wird wie folgt gefasst:

Gegenüber den in § 53 Abs. 1 Satz 1 genannten Personen sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass eine solche Person von der Maßnahme betroffen ist, gilt Absatz 2 entsprechend.

---

[22] Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten (vgl. BVerfGE 100, 313 <365> m.w.N.). „Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann." (BVerfGE 117, 244 <259>, vgl. bereits BVerfGE 20, 162 <176, 187>; 36, 193 <204>).

9.) Zeitplan

Eine so gewichtige Einschränkung von Grundrechten, wie sie die StPO in der Fassung der „Formulierungshilfe“ erlauben würde, bedarf der eingehenden Diskussion in der Öffentlichkeit wie auch im Parlament. Eine solche Diskussion schein dem Verfasser angesichts der wenigen Tage, die für die Vorbereitung der Anhörung zur Verfügung stehen, und den wenigen Wochen bis zum Ende der Legislaturperiode nicht mehr realistisch. Daher ist zu fragen, ob tatsächlich ein so besonderer Zeitdruck besteht, der es rechtfertigt, die vorgeschlagenen Normen mit all ihren verfassungsrechtlichen Sollbruchstellen ohne eingehende Beratung und Diskussion zu verabschieden.

Ein Sachgrund, der zur Eile drängen könnte, ist indes nicht zu erkennen. Für den Bereich der Terrorismusabwehr verfügt das BKA bereits über analoge Rechtsgrundlagen, sodass insoweit kein zwingendes Bedürfnis für strafprozessuale Rechtsgrundlagen besteht. Im Übrigen führt der Einsatz von Verschlüsselungstechnologien zwar dazu, dass bestimmte Beweismittel nicht mehr zur Kenntnis genommen werden können. Indes verfügen die Ermittlungsbehörden insbesondere in Form von Verkehrsdatenabfragen vor allem zu Verbindungen und Standorte von Mobilfunkgeräten über weitreichende Erkenntnisquellen, die sich auch durch Einsatz von Verschlüsselung nicht verbergen lassen. Außerdem lässt sich die Mehrzahl der Erkenntnisse, die sich mittels Online-Durchsuchung und Quellen-TKÜ gewinnen ließen, auch durch einen Zugriff und die Auswertung beschlagnahmter Systeme erlangen. Bei Licht betrachtet geht es also weniger darum, Erkenntnisse *überhaupt* zu gewinnen, sondern darum, sie früher und heimlich zu bekommen. So nützlich derlei taktische Möglichkeiten sein mögen, so wenig können sie indes eine mit allzu heißer Nadel gestrickte Rechtsgrundlage für Staatstrojaner im Strafverfahren rechtfertigen.

Schließlich ist auch zu berücksichtigen, dass massive technische Probleme bei der Entwicklung bisher den Einsatz von Trojanern auf der Grundlage des BKAG auf eine einstellige Anzahl beschränkt haben. Mit anderen Worten dürfte sich eine Verzögerung der Schaffung einer Rechtsgrundlage bis in die 19. Wahlperiode in der Praxis kaum auswirken.

Schlussbemerkung

Schon angesichts des erheblichen Änderungsbedarfs in den in dieser Stellungnahme erörterten Teilen des Entwurfs sollte der Entwurf insgesamt überarbeitet werden. In der vorgesehenen Form sind die geplanten Neuregelungen mit Nachdruck abzulehnen. Dies gilt umso mehr, führt man sich vor Augen, dass die Stellungnahmen der Sachverständigen schon aus Zeitgründen nur einen Abriss der verfassungsrechtlichen, aber auch rechtspolitischen Probleme des vorliegenden Entwurfs wiedergeben können.

Berlin, den 29. Mai 2017

Dr. Ulf Buermeyer, LL.M. (Columbia)