Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt Prof. Dr. Hermann Weber, Schriftleiter von 1982–2001

24 2020

Seite 1–15

39. Jahrgang

15. Dezember 2020

Professor Dr. Mario Martini und Sarah Fröhlingsdorf*

Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik

Die Quellen-TKÜ ist grundrechtsdogmatisch gleichsam ein Sandwichkind zwischen Telekommunikationsüberwachung und Online-Durchsuchung. Mit ihrer kleinen Schwester, der Telekommunikationsüberwachung, teilt sie die Eigenschaft, auf die gleichen Kommunikationsdaten, nämlich zu übermittelnde Inhalte, zuzugreifen. Mit ihrer großen Schwester, der Online-Durchsuchung hat sie gemeinsam, das gesamte Endgerät zu infiltrieren. Anders als diese darf sie aber nicht das Gesamtsystem ausspähen, sondern ausschließlich „laufende Kommunikation" überwachen. Wie sich dies technisch gewährleisten lässt, damit die Quellen-TKÜ nicht in eine Online-Durchsuchung umschlägt, präzisieren die Ermächtigungsnormen bislang nur ungenügend. Der Beitrag sucht nach grundrechtsdogmatisch tragfähigen Antworten auf die verfassungsrechtlichen Problemlagen und legt den Finger in offene Wunden der gesetzlichen Regelungen.

I. Telekommunikationsüberwachung an der Quelle?

Manch einem Ermittler, der den *WhatsApp-* oder *Telegram*-Chat eines Verdächtigen einmal mehr nicht überwachen kann, weil die Kommunikation verschlüsselt erfolgt, geht unausgesprochen die Losung durch den Kopf: „Ist der Wassertopf leer, vermag die Quelle den Durst zu stillen." Genau dieser Logik folgt die sogenannte Quellen-TKÜ. Sie greift auf ein Endgerät wie Smartphone oder Laptop („die Quelle") zu, um laufende Kommunikation (aber nicht den kompletten Speicherinhalt) auszulesen. In welchen rechtlichen Grenzen Ermittlungsbehörden davon Gebrauch machen dürfen, ist Gegenstand einer intensiven verfassungsrechtlichen und rechtspolitischen Diskussion.[1]

Dass sich Kommunikation vielfach nur mithilfe der Quellen-TKÜ abfangen lässt, ist das Ergebnis einer an sich begrüßenswerten Entwicklung: der wachsenden Sicherheit der individuellen Kommunikation.[2] Früher konnte sich der Staat in laufende Kommunikationsvorgänge über Schnittstellen bei dem Zugangsanbieter (Access Provider) vergleichsweise einfach „einklinken" und so etwa Telefongespräche mithören oder SMS-Nachrichten aufzeichnen.[3] Heute begleitet die Verschlüsselung vielfach den gesamten Weg der Kommunikation vom Absender zum Empfänger (sog. Ende-zu-Ende-Verschlüsselung).

Integrieren Kommunikationsanwendungen wie *WhatsApp* oder *Signal* solche kryptografischen Sicherungen standardmäßig in ihr technisches Repertoire,[4] machen sie dadurch polizeilichen Ermittlern das Leben schwer. Lässt sich die Verschlüsselung nicht aufbrechen[5] oder umgehen, ist der

* *Mario Martini* ist Lehrstuhlinhaber an der DUV Speyer und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung. *Sarah Fröhlingsdorf* ist dort Forschungsreferentin.

Die Autoren danken Herrn *Michael Kolain* für seine sehr gute inhaltliche Mitwirkung.

1 Vgl. insbes. *BVerfGE* 120, 274 (309) = NJW 2008, 822 (826) Rn. 190. Während das BKA bereits im Jahr 2009 eine Ermächtigungsgrundlage für die Quellen-TKÜ erhielt (§§ 20l, 20k II, III BKAG aF), fehlte in der StPO bis zur Neuregelung des § 100a I 2, 3 StPO im Jahr 2017 eine klare Befugnisnorm; vgl. *LG Hamburg* 1.10.2007 – 629 Qs 29/07, BeckRS 2008, 12389; *Becker/Meinicke*, StV 2011, 50 (52); *Buermeyer/Bäcker*, HRRS 2009, 433 (440); Sankol, CR 2008, 13 (18); aA *AG Bayreuth* 17.9.2009 – Gs 911/09, BeckRS 2010, 8265; *LG Landshut* 20.1.2011 – 4 Qs 346/10, BeckRS 2011, 2429. Seitdem steht nunmehr insbes. die Frage im Raum, ob § 100a I 2, 3 StPO verfassungsgemäß ist, dazu näher III. 2. b) bb).

2 In Übereinstimmung damit hat sich die Bundesregierung zum Ziel gesetzt, Deutschland zum Verschlüsselungsstandort Nr. 1 zu machen; s. Die Bundesregierung, Legislaturbericht Digitale Agenda 2014–2017, Mai 2017, 106.

3 Näher *Pohlmann/Riedel*, DuD 2018, 37 (39).

4 Näher *Brendel/Gerber*, DuD 2019, 276 (278).

5 Wie aufwändig die Entschlüsselung ist, hängt vom Verschlüsselungsverfahren ab. Vgl. *Brodowski*, JR 2011, 532 (533); *Brunst*, DuD 2012, 333. Quantencomputer könnten künftig zwar womöglich Abhilfe verschaffen – noch ist das aber Zukunftsmusik. Das ZITiS plant, Quantencomputer zur Entschlüsselung zu nutzen. Vgl. Bundesministerium für Bildung und Forschung, Quantentechnologien – von den Grundlagen zum Markt, 2018, 25.

Zugriff auf den verwertbaren Inhalt der Information nicht mehr in der Leitung, sondern grundsätzlich nur noch an der Quelle, d. h. auf dem Endgerät des Absenders oder Empfängers, möglich, solange die Kommunikationsinhalte dort noch unverschlüsselt bzw. wieder entschlüsselt vorliegen. Um auf die Kommunikationsinhalte zuzugreifen, installiert die Behörde dann heimlich eine Überwachungssoftware auf dem Endgerät der verdächtigen Person. Sie infiziert also beispielsweise das Smartphone oder den Laptop des Betroffenen mit Malware. Anschließend leitet der sogenannte Staatstrojaner diejenigen Telekommunikationsdaten an die Behörde weiter, die in verschlüsselnden Kommunikationsanwendungen entstehen.[6]

1. Technische Voraussetzung: Infiltration des Systems

a) *Physischer Zugriff*. Eine naheliegende Methode, um ein Endgerät mit Überwachungssoftware zu infizieren, ist der physische Zugriff.[7] Dafür muss die Behörde das Gerät beschlagnahmen. Ein solches Vorgehen ist indes nur dann zielführend, wenn die Infiltration unentdeckt geschieht. Denn eine Zielperson, die weiß, dass der Staat ihre Nachrichten mitliest, wird sich ein neues Gerät zulegen.

Um zu verheimlichen, dass sie die Überwachungssoftware aufbringen, können die Ermittler (im Rahmen der Verhältnismäßigkeit) kriminalistische List anwenden, d. h. über die wahre Ermittlungsabsicht täuschen.[8] Die Behörde kann den Computer eines Beschuldigten etwa bei einer Sicherheitsüberprüfung am Flughafen beschlagnahmen und dabei das Überwachungsprogramm unbemerkt installieren.[9] Soweit eine Ermächtigungsgrundlage, wie etwa § 5 I 2 LuftSiG, dazu berechtigt, ein IT-Gerät temporär an sich zu nehmen, reicht die Befugnisnorm für eine Quellen-TKÜ („mit technischen Mitteln in das informationstechnische System einzugreifen“[10]) zumindest so weit, der Behörde in der Kontrollsituation am Flughafen zu erlauben, eine Überwachungssoftware ohne Wissen des Betroffenen aufzuspielen.[11]

Eine Ermächtigung, auch die Wohnung zu betreten, um die Überwachungssoftware etwa auf einem Desktop-Computer zu installieren, ist davon nicht umfasst. Eine solche sieht bisher nur Art. 44 I 5 BayPAG vor.[12] Das könnte sich aber bald ändern: Die Justizminister des Bundes und der Länder haben in ihrer Frühjahrskonferenz 2018 auch für die Strafverfolgung eine entsprechende gesetzliche Grundlage gefordert.[13]

b) *Zugriff auf das Endgerät und Installation der Überwachungssoftware aus der Ferne*. Statt auf das Endgerät einer Zielperson unbemerkt, mit erheblichem Ermittlungsaufwand und zahlreichen Risiken physisch zuzugreifen, können die Behörden auch einen anderen Weg wählen, der häufig mehr Erfolg verspricht: Da die meisten digitalen Endgeräte an das Internet angebunden sind, lassen sie sich technisch aus der Ferne infiltrieren.

Ein Ermittler geht dabei ähnlich wie ein Einbrecher vor, der überprüft, ob jemand ein Fenster offengelassen hat, durch das er in das Haus einsteigen kann: Er sucht Sicherheitslücken auf dem System des Betroffenen, die er ausnutzen kann, um dort „einzudringen“.[14] Um eine große Trefferquote zu erzielen, richtet der Eindringling sein ermittlungstaktisches Dietrich-Set insbesondere auf Sicherheitslücken aus, die sich in verbreiteten Softwareanwendungen, etwa Webbrowsern (z. B. *Chrome* oder *Firefox*) oder Programmen zur Dokumentbearbeitung (z. B. *Word*), finden.[15]

Sind Sicherheitslücken bekannt, entwickeln Angreifer eine Software, welche die Schwachstellen automatisiert ausnutzt (sog. „Exploit“).[16] Hat diese sich im System des Betroffenen eingenistet, kann sie die Überwachungssoftware nachladen.[17] „Exploits“, die aus der Ferne agieren, verstecken sich dafür in der Regel in gesendeten Dateien (zB in einem E-Mail-Anhang), in via Internet geladener Software oder sie infizieren das System, während der Nutzer eine präparierte Internetseite öffnet („Drive-by-Exploits“).[18]

2. Konfliktlage zwischen IT-Sicherheit und effektiver Ermittlung bei sog. Zero-Day-Exploits

Greift der Staat für die Quellen-TKÜ auf Schwachstellen zu, zu denen die Hersteller noch keine Fehlerbehebung anbieten

6 Zur Vorgehensweise s. auch BT-Drs. 18/12785, 48 f.
7 Vgl. *Brodowski*, JR 2011, 532 (535).
8 So auch die Gesetzesbegründung zu § 100 a I 2 und 3 StPO, BT-Drs. 18/12785, 52; *Bruns* in *Hannich*, KK StPO, 8. Aufl., 2019 § 100 a Rn. 46; *Soiné*, NStZ 2018, 497 (501); zu den Grenzen kriminalistischer List, *Soiné*, NStZ 2019, 596 (597 f.).
9 So ging bspw. das Bayerische LKA im Fall des *LG Landshut*, Beschl. v. 20.1.2011 – 4 Qs 346/10, BeckRS 2011, 02429 vor; dazu auch *Stadler*, MMR 2012, 18.
10 Vgl. § 51 II 1 BKAG; 100 a I 2 StPO. Näher III. 1.
11 *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, 29.5.2017, 21. Vgl. auch *Bär*, MMR 2011, 691 (693); *Roggan*, StV 2017, 821 (822); *Soiné*, NStZ 2018, 497 (501).
12 § 100 a StPO ist nur auf einen Eingriff in Art. 10 GG und nicht auf einen Eingriff in Art. 13 GG zugeschnitten, *Bruns* in *Hannich*, KK StPO § 100 a Rn. 46; *Roggan*, StV 2017, 821 (822); i. E. auch BT-Drs. 18/12785, 52. So auch *Soiné*, NStZ 2018, 497 (501), der allerdings für ein Betretungsrecht, um eine Online-Durchsuchung durchzuführen, die kombinierte Anordnung von Maßnahmen nach § 100 b und § 100 c StPO ausreichen lassen will; dazu in anderer Konstellation krit. *Rüscher*, NStZ 2018, 687 (692).
13 Beschluss der 89. Konferenz der Justizministerinnen und Justizminister, TOP II. 8. Ergänzung der Regelungen zur Quellen-TKÜ und zur Online-Durchsuchung um ein Betretungsrecht, 6./7.6.2018. Soll dieser Beschluss verfassungskonform in Gesetzesform gegossen werden, ist jedoch zu klären, ob der Schrankenkatalog des Art. 13 II–VII GG einer Ergänzung bedarf. Denn das Recht, eine Wohnung zu betreten, um eine Überwachungssoftware aufzuspielen, fügt sich in dessen Konzeption nicht recht ein: *Durchsuchungen iSd Art. 13 II GG* sind regelmäßig offene Maßnahmen (*Gornig* in *v. Mangoldt/Klein/Starck*, GG, 7. Aufl., 2018 Art. 13 Rn. 65; *Roggan*, DÖV 2019, 425 [431]). Art. 13 III-V GG beziehen sich dagegen auf den Einsatz technischer Mittel, um die Wohnung – und nicht die laufende Kommunikation – zu überwachen. *Art. 13 VII GG* eröffnet zwar einen Auffangtatbestand; er lässt aber den gesetzlichen Eingriff nur zu, um „dringende Gefahren für die öffentliche Sicherheit und Ordnung“ zu verhüten. Um ein strafprozessuales Betretungsrecht gesetzlich zu verankern, das dem Zweck dient, eine Überwachungssoftware (für eine Quellen-TKÜ oder eine Online-Durchsuchung) auf ein Endgerät zu spielen, ist daher im Ergebnis eine Verfassungsänderung notwendig. AA wohl *Böckenförde*, JZ 2008, 925 (933).
14 Vgl. *Huang/Siegel et al.*, ACM Comput. Surv. 51 (2018), 1 (4).
15 Besonders zielgerichtete Angriffe sind zugleich jedoch nur effektiv, wenn sie mehrere Schwachstellen attackieren, *Pohlmann/Riedel*, DuD 2018, 37, 40 (42).
16 Näher *Pohlmann/Riedel*, DuD 2018, 37 (39).
17 Vgl. *Huang/Siegel et al.*, ACM Comput. Surv. 51 (2018), 1 (7).
18 *Huang/Siegel et al.*, ACM Comput. Surv. 51 (2018), 1 (6). Dem täuschenden Charakter dieser (Begleit-)Maßnahme sind rechtliche Grenzen gesetzt, *Derin/Golla*, NJW 2019, 1111 (1113 f.). Obwohl § 136 a StPO in direkter Anwendung nur für die Vernehmung gilt, ist der ihm zugrunde liegende Gedanke übertragbar, dass — in Abgrenzung zu kriminalistischer List — aktive und bewusste Fehlinformationen des Betroffenen im rechtsstaatlichen Ermittlungsverfahren verboten sind; s. *Schuhr* in *Knauer/Kudlich/Schneider*, MK StPO, 2014 § 136 a Rn. 75 ff. Außerdem darf die staatliche Stelle den Betroffenen aufgrund des Nemo-tenetur-Grundsatzes nicht in eine Situation versetzen, in der er aufgrund der „vorgespielten“ Vertraulichkeit sich selbst belastet. Zulässig ist es aber, bestehende Irrtümer oder Situationen – auch heimlich – auszunutzen; vgl. *Soiné*, NStZ 2019, 596 (598).

(sog. „Zero-Day-Exploits“[19]), gerät er in eine Zwickmühle:[20] Die Sicherheitsbehörden entwickeln dann ein ermittlungstaktisches Interesse daran, dass der Zeitraum zwischen Entdeckung der Schwachstelle und Fehlerbehebung lange währt.[21] Das GG verpflichtet den Staat jedoch dazu, die Bürger im Rahmen des Möglichen vor den Risiken zu schützen, die mit der Nutzung sensibler technischer Systeme einhergehen; er ist insbesondere im Grundsatz dazu angehalten, die Vulnerabilität der IT-Geräte nicht gegen die Bürger selbst zu richten.[22] Nutzt der Staat bislang unentdeckte Sicherheitslücken gezielt aus, um eine Quellen-TKÜ einzuleiten, gefährdet er zwangsläufig zugleich die IT-Sicherheit aller Bürger,[23] um gegen einige wenige verdächtige Personen effektiv ermitteln zu können.[24]

Bislang fehlen konkrete Leitplanken des nationalen Gesetzgebers, die klar abstecken, wie Behörden mit ihnen bekannten Sicherheitslücken umzugehen haben. Je nach Bedeutung der Sicherheitslücke (Verbreitungsgrad, Wahrscheinlichkeit, ob und welche anderen Akteure sich die Schwachstelle ggf. zunutze machen können, etc.) und dem Zweck, den die Behörde verfolgt, sollte der Gesetzgeber den Ermittlern jedoch hinreichend klare Vorgaben dafür mit auf den Weg geben, ob und inwieweit sie die Schwachstelle ausnutzen dürfen, bis die Unternehmen sie aus eigener Initiative schließen.[25] Zudem fehlen normative Rahmenbedingungen dafür, unter welchen Voraussetzungen sich die staatlichen Ermittler das Wissen über Schwachstellen zu Marktpreisen[26] auf dem sogenannte Grauen Markt hinzukaufen dürfen, um Zero-Day-Exploits überhaupt nutzen zu können.[27]

Vordergründig scheint das *Unionsrecht* den Handlungsspielraum der Mitgliedstaaten, Sicherheitslücken unbegrenzt auszunutzen, nachhaltig zu verengen. Denn wenn eine Sicherheitsbehörde einen personenbezogenen Datenverarbeitungsprozess durchführt, unterliegt sie als Verantwortlicher der unionsrechtlichen Verpflichtung, Sicherheitsmaßnahmen für ein angemessenes Schutzniveau zu treffen. So verfügt es Art. 29 I JI-RL (RL [EU] 2016/680), der als Lex specialis die Vorgaben des Art. 32 I DS-GVO verdrängt.[28] Die Richtlinie untersagt es den Mitgliedstaaten jedoch nicht, im Interesse der Strafverfolgung Verarbeitungsvorgänge durchzuführen, die Sicherheitslücken instrumentalisieren. Vielmehr soll Art. 29 I JI-RL Betroffene gegen Verletzungen der Datensicherheit durch *Dritte* schützen, die den Zweck der Verarbeitung durch unberechtigten Zugriff torpedieren. Um Verarbeitungsvorgänge zu legitimieren, die dazu dienen, *Aufgaben der Strafverfolgung oder Gefahrenabwehr* zu erfüllen, belässt die Union den Mitgliedstaaten einen eigenen Regelungsspielraum (Art. 6 I JI-RL): Sie können Vorschriften erlassen, die Ermittlungsbehörden dazu ermächtigen, Sicherheitslücken auszunutzen. Von dieser Regelungsfreiheit hat der deutsche Gesetzgeber in strafprozessualen und gefahrenabwehrrechtlichen Ermächtigungsnormen (§ 51 II 1 BKAG; § 100 a I 2 StPO) mit Regelungen über Maßnahmen zum Schutz vor dem unberechtigten Zugriff Dritter (§ 49 II 2, 3 BKAG; § 100 a V 2 StPO) in unionsrechtlich zulässiger Weise Gebrauch gemacht.

II. Verfassungsrechtliche Einordnung: Eingriff in Art. 10 GG oder in das IT-Grundrecht?

1. Abgrenzung zur Telekommunikationsüberwachung

Die Quellen-TKÜ teilt mit der herkömmlichen Telekommunikationsüberwachung eine wichtige Gemeinsamkeit. Beide verschreiben sich insbesondere dem gleichen *Zweck*: Sie sollen Kommunikationsinhalte, die zwei oder mehrere Personen per Telefon, Sprach-, Video- oder Textnachricht austauschen, für Ermittlungszwecke zweckentfremden. Die Zugriffsinstrumente zielen damit auf die gleichen Kommunikationsdaten. Die *Methodik* des Zugriffs auf die Telekommunikation unterscheidet sich jedoch: Die Quellen-TKÜ zapft nicht das *Telefongespräch* bei dem Zugangsanbieter (bspw. der Deutschen Telekom) an. Sie infiltriert vielmehr das *Endgerät*, das die Kommunikation herstellt. Die Quellen-TKÜ greift auf die Kommunikationsinhalte also nicht auf dem Übertragungsweg, sondern im Herrschaftsbereich des Betroffenen zu und setzt damit das gesamte System der Ausspähung aus.[29] Als (ungewollten) Nebeneffekt gewährt die Quellen-TKÜ staatlichen Behörden dadurch einen Einblick fühlbar höheren Ausmaßes als die klassische Telekommunikationsüberwachung:[30] Selbst wenn die Maßnahme nicht darauf zielt, können die Ermittler technisch nicht nur auf laufende Kommunikationsvorgänge, sondern auch auf viel größere, hochsensible Datenbestände auf dem Datenspeicher zugreifen. Wer Zugriff auf ein Smartphone als Ganzes hat, kann dort beispielsweise nicht nur die eingehenden Nachrichten eines Messengers mitlesen, sondern gegebenenfalls auch im Nachrichtenarchiv suchen, private Bilder aus dem Datenspeicher aussondern, unbemerkt auf die Kamera zugreifen oder die GPS-Daten mitschneiden, um Bewegungsprofile zu erstellen. An der Quelle ist die Sicht auf die Persönlichkeit der Beobachteten also nicht nur klar (da [i. d. R.] unverschlüsselt), sondern auch tiefer als im Falle der klassischen Form der TKÜ. Dann verlässt die Quellen-TKÜ die grundrechtlichen Schutzsphären des Art. 10 I GG; sie fügt sich nicht mehr ohne weiteres in das dogmatische Raster ein, das die Mütter und Väter des GG dem Telekommunikationsgeheimnis mit auf den Weg gegeben haben. Mit Blick auf die spezifischen Gefährdungen für die Persönlichkeit, die sich mit dem Zugriff *auf alle Daten eines Endgeräts* verknüpfen, steht die Quellen-TKÜ deshalb der Online-Durchsuchung näher als der Telekommunikationsüberwachung.

19 „Zero-Day“ bezieht sich darauf, dass der Hersteller noch nicht von der Schwachstelle weiß, und daher noch keine Maßnahmen in die Wege geleitet hat, um sie zu schließen. Näher *Ablon/Bogart*, Zero Days, Thousands of Nights, 2017, ix.

20 Vgl. bereits *BVerfGE* 120, 274 (325 f.) = NJW 2008, 822 (830) Rn. 241.

21 *Pohlmann/Riedel*, DuD 2018, 37 (39).

22 Das folgt aus dem sog. IT-Grundrecht (Art. 2 I iVm Art. 1 I GG), dazu unten II. 2., *Buermeyer*, Gute Lücken, schlechte Lücken? Zur objektivrechtlichen Dimension des IT-Grundrechts, verfassungsblog.de vom 8.9.2018; *Derin/Golla*, NJW 2019, 1111 (1114); *Hoffmann-Riem*, JZ 2008, 1009 (1013 f.).

23 Öffentlich unbekannte Schwachstellen stehen nämlich auch anderen Akteuren offen – seien es Cyberkriminelle oder ausländische Sicherheitsbehörden.

24 *Derin/Golla*, NJW 2019, 1111 (1115); *Pohlmann/Riedel*, DuD 2018, 37 (44).

25 *Derin/Golla*, NJW 2019, 1111 (1115); *Herpig*, Schwachstellen-Management für mehr Sicherheit, 2018, 23 f. Die verfassungsrechtlichen Fragestellungen, die sich aus dem Interessenkonflikt zwischen IT-Sicherheit und Strafverfolgung ergeben, tragen aktuell etwa der Verein *Digitalcourage*, die *FDP-Bundestagsfraktion* und die *Gesellschaft für Freiheitsrechte* mittels Verfassungsbeschwerde gegen § 100 a StPO an das *BVerfG* heran (2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18).

26 Exploits kosten schätzungsweise zwischen $ 50.000 und $ 100.000, *Ablon/Bogart*, Zero Days, Thousands of Nights, 86.

27 *Buermeyer*, Gute Lücken, schlechte Lücken? Zur objektiv-rechtlichen Dimension des IT-Grundrechts verfassungsblog.de vom 8.9.2018. Der Staat tritt dann in Konkurrenz zu Initiativen wie „Bug-Bounty“-Programmen, welche die IT-Sicherheit stärken wollen, indem sie durch finanzielle Anreize dazu anregen, Wissen über Schwachstellen preiszugeben, *Pohlmann/Riedel*, DuD 2018, 37 (43).

28 Auf Maßnahmen der Gefahrenabwehr, Strafverfolgung und Strafvollstreckung ist die DS-GVO nicht anwendbar (Art. 2 II lit. d DSGVO; Art. 1 I der RL 2016/680/EU).

29 *BVerfGE* 120, 274 (308) = NJW 2008, 822 (825) Rn. 188.

30 S. auch *Stadler*, MMR 2012, 18 (19).

2. Abgrenzung zur Online-Durchsuchung

Von außen betrachtet ist der Eingriff der Quellen-TKÜ in das informationstechnische System nicht von der Online-Durchsuchung zu unterscheiden. In beiden Fällen infiltriert der Staat ein Computersystem über Netzwerkverbindungen und späht es aus; beide Maßnahmen berühren die Integrität des Systems dadurch, dass die Überwachungssoftware das System manipuliert.[31]

Um die Eigenart dieser Gefährdung durch die Online-Durchsuchung grundrechtlich zu erfassen, hat sich in der verfassungsrechtlichen Dogmatik das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme herausgebildet (sog. IT-Grundrecht – Art. 2 I iVm Art. 1 I GG).[32] Eingriffe in dieses Grundrecht gestattet die Verfassung nur unter sehr hohen Voraussetzungen, die deutlich über die Anforderungen an die herkömmliche Telekommunikationsüberwachung[33] hinausgehen. In der Deutung des *BVerfG* müssen „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen“,[34] um einen gefahrenabwehrrechtlichen Eingriff[35] zu legitimieren. Auf verfahrensrechtlicher Ebene erfordert eine verfassungsgemäße Eingriffsbefugnis einen präventiven Richtervorbehalt[36] sowie Vorkehrungen, um Eingriffe in den Kernbereich privater Lebensgestaltung zu verhindern.[37]

Mit Blick auf die strukturell ähnliche grundrechtsdogmatische Gefährdungslage liegt es nahe, die verfassungsrechtlichen Maßstäbe des sogenannten IT-Grundrechts für die Online-Durchsuchung auch an die Quellen-TKÜ anzulegen. Das hieße aber nicht nur, den zulässigen Einsatzradius des Instruments im Verhältnis zur bisherigen Rechtslage deutlich zu reduzieren (da die Eingriffsbefugnisse[38] den hohen grundrechtlichen Rechtfertigungsanforderungen des IT-Grundrechts nicht gerecht werden), sondern auch ihre unterschiedliche grundrechtliche Eingriffsintensität zu verkennen: Die Online-Durchsuchung greift ihrem Wesen nach *bewusst auf den Gesamtbestand persönlicher Daten* eines informationstechnischen Systems zu (und gewährt dadurch einen deutlich tieferen Einblick in die Persönlichkeit der betroffenen Person).[39] Demgegenüber ist die Quellen-TKÜ grundsätzlich enger angelegt: Sie soll nur Daten aus einem laufenden verschlüsselten Kommunikationsvorgang erfassen, deren Inhalt sie „an der Quelle“ im Klartext mitliest. Solange die Überwachung diese Voraussetzungen *faktisch* sicherstellt, unterscheiden sich die erlangten Daten und Ermittlungserkenntnisse nicht von denen, die eine herkömmliche Telekommunikationsüberwachung unverschlüsselt auf dem Übertragungsweg abfängt und die Art. 10 I GG schützt. Muss der Einzelne also nicht fürchten, dass die Behörde auf den Gesamtdatenbestand zugreift, ist die Eingriffsintensität der Quellen-TKÜ nicht mit jener einer Online-Durchsuchung vergleichbar.

Das bedeutet auch: Schließt die Quellen-TKÜ den Zugriff auf Daten, die nicht zur laufenden Kommunikation gehören, aus dem Zugriffsradius der Überwachungssoftware wirksam aus, ist es sachlich gerechtfertigt, die grundrechtlichen Zulässigkeitshürden abzusenken. Das *BVerfG* misst eine Quellen-TKÜ aus diesem Grund solange lediglich an Art. 10 GG, wie *technische Vorkehrungen und rechtliche Vorgaben* garantieren, dass nur *laufende Gespräche oder Chats* in den Ermittlungsradar geraten.[40] Das Gericht verknüpft also – geleitet von der Wertung, dass der Eingriffszweck der Quellen-TKÜ demjenigen eines Eingriffs in Art. 10 GG entspricht[41] – die speziellen Anforderungen an die Zugriffsmodalitäten mit der dogmatischen Grundstruktur eines Eingriffs in Art. 10 GG.[42] Es konstruiert gleichsam eine *Schutzbereichsausnahme vom IT-Grundrecht* für die Quellen-TKÜ[43] – vorausgesetzt der Gesetzgeber hält diese „im Käfig

31 Vgl. *Buermeyer/Bäcker*, HRRS 2009, 433 (437).
32 *BVerfGE* 120, 274 (313 f.) = NJW 2008, 822 (827) Rn. 201 ff.
33 Wohl ausreichend für den – obgleich schwerwiegenden – Eingriff in das Fernmeldegeheimnis ist der Schutz besonders gewichtiger Rechtsgüter, vgl. *BVerfGE* 141, 220 (270) = NJW 2016, 1781 (1784) Rn. 108. Den Schutz *überragend* wichtiger Rechtsgüter verlangte das BVerfG dagegen etwa für die Vorratsdatenspeicherung, *BVerfGE* 125, 260 (328) = NJW 2010, 833 (841) Rn. 227. Von unterschiedlich hohen Messlatten ging der Gesetzgeber zu Recht auch für die Strafverfolgung aus: Für die herkömmliche *Telekommunikationsüberwachung* (und die Quellen-Telekommunikationsüberwachung) verlangt er eine schwere Straftat (§ 100 a I StPO), während er für die *Online-Durchsuchung* eine besonders schwere Straftat voraussetzt (§ 100 b I StPO).
34 *BVerfGE* 120, 274 (328) = NJW 2008, 822 (831) Rn. 247.
35 An Eingriffe zu *repressiven* Zwecken sind strengere Anforderungen anzulegen, da sich die eingetretene Rechtsgutsverletzung nicht mehr rückgängig machen lässt, *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, S. 10; *Eschelbach* in *Satzger/Schluckebier/Widmaier*, StPO, 4. Aufl., 2020 § 100 b Rn. 6; *Roggan*, StV 2017, 821 (827). S. III. 2. b) bb).
36 *BVerfGE* 120, 274 (331) = NJW 2008, 822 (832) Rn. 257. Art. 10 GG selbst verlangt zwar keinen Richtervorbehalt. Ein solcher kann aber dazu beitragen, einen schwerwiegenden heimlichen Eingriff die hohe Hürde der Angemessenheit nehmen zu lassen, vgl. *BVerfGE* 125, 260 (337) = NJW 2010, 833 (844) Rn. 248. Für die Telekommunikationsüberwachung iSd § 100 a StPO ordnet § 100 e StPO einen Richtervorbehalt an.
37 *BVerfGE* 120, 274 (335) = NJW 2008, 822 (833) Rn. 270.
38 Zu den Eingriffsbefugnissen s. III. 1.
39 Der grundrechtliche Eingriff erreicht eine höhere Intensität als einzelne Datenerhebungen: Selbst wenn der Staat seine Erkenntnisse aus *Einzelerhebungen* zu einem Persönlichkeitsprofil zusammenführt, wiegt der Zugriff auf den *Gesamtbestand* schwerer, *Böckenförde*, JZ 2008, 925 (927 f.).
40 *BVerfGE* 120, 274 (309) = NJW 2008, 822 (826) Rn. 190.
41 Vgl. *Löffelmann* Überwachung des Brief-, Post- und Fernmeldeverkehrs in *Dietrich/Eiffler*, Handbuch des Rechts der Nachrichtendienste, 2017, S. 1159 (1231).
42 Alternativ wäre es jedoch denkbar, die Quellen-TKÜ als Eingriff in das IT-Grundrecht (mit geringeren Anforderungen) zu werten. Innerhalb der Eingriffsdogmatik für das IT-Grundrecht wäre es etwa möglich – im Ansatz vergleichbar mit der Drei-Stufen-Theorie zur Berufsfreiheit (*BVerfGE* 7, 377 [405 ff.] = NJW 1958, 1035 [1038]) bzw. der Sphärentheorie im Persönlichkeitsrecht (s. bspw. *BVerfGE* 80, 367 [373 ff.] = NJW 1990, 563) – nach unterschiedlichen Modalitäten des Zugriffs auf ein informationstechnisches System zu differenzieren. Der *tiefste Eingriff* ginge dann mit einem Vollzugriff auf alle Komponenten des Systems einher, bei dem die Behörde einen umfassenden Einblick in abgeschlossene und laufende Datenvorgänge erhielte. Auf einer *mittleren Stufe* könnte etwa ein Zugriff stehen, der sich auf bestimmte Zeiträume, in denen eine gesammelte Übertragung stattfindet, bestimmte Datenmengen oder bestimmte Systemkomponenten (etwa Datenspeicher vs. aktuell laufende Prozesse; Daten aus bestimmten Apps) beschränkt. Auf einer Stufe, die die *geringste Eingriffstiefe* repräsentiert, wäre dann die „laufende Kommunikation“ zu verorten, da mit dieser Eingriffsart kein Einblick in archivierte Persönlichkeitselemente verbunden ist. Eine gestufte Eingriffsdogmatik verunklart jedoch im Ergebnis die Schutzsphäre des IT-Grundrechts und verwischt die grundrechtsdogmatische Trennlinie zu Art. 10 GG. Richtete sich die Eingriffsschwere nämlich allgemein nach einer Einzelfallbewertung, welche Datenqualität und -quantität die Ermittler benötigen (also ob sie etwa nur die laufende Kommunikation abgreifen), bliebe der Aspekt unberücksichtigt, dass die Eingriffsschwere sich gerade daraus speist, auf den Gesamtdatenbestand zugreifen zu *können*. Zudem steht zu bezweifeln, dass es gelingt, die technischen Komponenten und Zugriffsmodalitäten eines informationstechnischen Systems mit normativen Wertungen des Schutzes der Privatsphäre zu synchronisieren. Quantitative Grenzen müssen insoweit von vornherein ausscheiden: Ein Bild, das nur 1 Megabyte groß ist, kann bereits intimste Geheimnisse offenlegen, während mehrere Terabyte an Blockbuster-Kinofilmen möglicherweise weniger Aussagekraft über die Persönlichkeit eines Menschen entfalten. Ebenso wenig lässt sich eine zuverlässige Aussage dazu treffen, ob bestimmte Systemkomponenten (etwa die Kamera oder der Datenspeicher) eine generelle persönlichkeitsrechtliche Relevanz aufweisen. Es bliebe letztlich nur eine Unterscheidung zwischen „*gespeicherten*“ *Inhalten* aus der Vergangenheit und dem Zugriff auf *aktuelle Verarbeitungsvorgänge*. Insofern vermag aber bereits die „laufende Kommunikation“ – auf deren Schutz Art. 10 GG gerade zugeschnitten ist – einen verlässlichen Anknüpfungspunkt zu bilden.
43 *Buermeyer*, StV 2013, 470 (473).

der Telefonüberwachung".[44] Die Trennlinie für den zunächst paradox anmutenden Ansatz, die Quellen-TKÜ mit der Wertung des Art. 10 GG zu verbinden, zugleich aber den Zugriff über das Endgerät in Art. 10 GG miteinzubeziehen, zieht dabei der Begriff „laufende Kommunikation".

Das Spannungsfeld der Quellen-TKÜ entlang dieser Vorgaben in grundrechtliche Strukturen zu übersetzen, überzeugt aber nur dann vollständig, wenn es auch tatsächlich gelingt, eine Beschränkung auf die „laufende Kommunikation" in der Vollzugsrealität zu verankern.[45] Dafür muss der Gesetzgeber hinreichend klare Vorgaben treffen, die der Erkenntnis Rechnung tragen, dass Art. 10 GG die Gefahren abzuwehren versucht, die *dem Übertragungsvorgang entspringen,* und seinen Schutz ausschließlich auf die *Dauer des Kommunikationsvorgangs* erstreckt – nicht aber auf umfassendere Erkenntnisse aus dem informationstechnischen System der Kommunikationsteilnehmer.

III. Einfachgesetzliche Umsetzung der Anforderungen

1. Geltende Befugnisnormen der Gefahrenabwehr und Strafverfolgung

Die gesetzlichen Befugnisnormen für die Quellen-TKÜ beschränken sich im Großen und Ganzen darauf, die abstrakten Vorgaben des *BVerfG* wiederzugeben, ohne sie näher zu konkretisieren: Die Zulässigkeit einer Quellen-TKÜ für Zwecke der *Gefahrenabwehr* knüpft der einfache (Bundes-) Gesetzgeber im Kern an die Vorgabe, dass die Ermittlungsbehörde *ausschließlich laufende Kommunikation* überwachen und aufzeichnen darf; der Eingriff muss ferner notwendig sein, um die Telekommunikationsüberwachung in unverschlüsselter Form zu ermöglichen (§ 51 II 1 BKAG). Einige Bundesländer sehen in ihren Polizeigesetzen eine vergleichbare Befugnis vor.[46]

Für die *repressive* Polizeiarbeit erlaubt § 100 a I 2 StPO, die Telekommunikation an der Quelle zu überwachen, soweit dies notwendig ist, um eine auch im Einzelfall schwerwiegende Straftat aufzuklären oder den Aufenthaltsort des Beschuldigten zu ermitteln – insbesondere um die Überwachung und Aufzeichnung in unverschlüsselter Form zu ermöglichen. *Wie* der Eingriff in das informationstechnische System erfolgt, dekretiert der Gesetzgeber indes nicht näher. Ebenso wie im Gefahrenabwehrrecht (§ 51 II 1 Nr. 1 BKAG) gibt er nur (aber immerhin auch hier) vor, technisch sicherzustellen, dass die Maßnahme nur die laufende Kommunikation überwacht und aufzeichnet (§ 100 a V 1 Nr. 1 a StPO).

Die Behörden dürfen die Quellen-TKÜ jeweils nicht kraft eigener Initiative vornehmen. Voraussetzung ist vielmehr eine richterliche Anordnung (§ 51 III BKAG, § 100 e I 1 StPO). Sie hat die Art, den Umfang und die Dauer der Maßnahme anzugeben (§ 51 V 2 Nr. 3 BKAG, § 100 e III 2 Nr. 3 StPO). Im Anschluss konfiguriert die Behörde das Programm im Einklang mit der richterlichen Anordnung bzw. dem Beschluss.

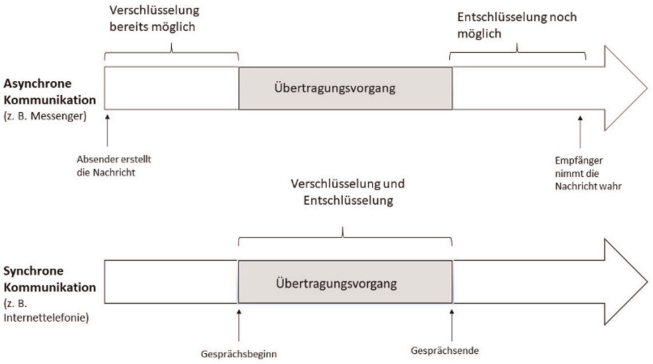
Veränderungen an dem informationstechnischen System gestatten die Gesetze nicht vorbehaltlos, sondern nur insoweit, als dies für die Datenerhebung unerlässlich ist. Nach Beendigung der Maßnahme sind sie, soweit technisch möglich, rückgängig zu machen (§ 51 II 2 iVm § 49 II 1 Nr. 2 BKAG; § 100 a V 1 Nr. 2, 3 StPO). Die Befugnisnormen schreiben zudem Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung vor (§ 51 VII BKAG, 100 d StPO).

Die StPO geht in ihrer Befugnisreichweite noch einen entscheidenden Schritt weiter als das BKAG: § 100 I 3 StPO gestattet es, auch *gespeicherte* Kommunikationsinhalte und -umstände zu überwachen und aufzuzeichnen, wenn die Maßnahme ebenso während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form möglich gewesen wäre.[47]

2. Begrenzung auf laufende Kommunikation

Um verfassungsrechtlich zulässig zu sein, müssen die gesetzlichen Regelungen zur Quellen-TKÜ die Trennlinie zwischen laufenden und sonstigen Kommunikationsdaten, die auf Speichermedien des Endgeräts archiviert sind, im Lichte der grundrechtlichen Vorgaben zutreffend markieren.

a) *Laufende Kommunikation als Dauer des Übertragungsvorgangs.* Ein Weg, die Grenzen zwischen laufender Kommunikation (Art. 10 GG) und alleiniger Herrschaftssphäre des Nutzers (IT-Grundrecht) klar abzustecken, kann darin bestehen, den Topos „laufende Kommunikation" als allein auf die *Dauer des technischen Übertragungsvorgangs* beschränkt zu sehen. In dieser Lesart dürfte die Überwachungssoftware die Telekommunikationsdaten nur abfangen, während der Übertragungsvorgang läuft. Sie erfasste dann ausschließlich solche Kommunikationsmittel (wie bspw. die Internettelefonie), bei denen Verschlüsselungs- und Übertragungsvorgang zeitlich zusammenfallen.[48] Übermittlungsformate, deren Inhalte *über den Zeitraum des Übertragungsvorgangs hinaus* (bereits oder noch) *verschlüsselt* sind, lägen demgegenüber außerhalb des Anwendungsbereichs der Quellen-TKÜ. Insbesondere Anwendungen, die eine sogenannte asynchrone Kommunikation ermöglichen (zB Messenger), wären nicht umfasst, wenn sie die Nachricht verschlüsseln, bevor der Übertragungsvorgang beginnt, und die Nachricht erst entschlüsseln, nachdem das Endgerät des Empfängers sie empfängt.[49]



44 *Stadler*, MMR 2012, 18 (20).
45 Krit. etwa *Skistims/Roßnagel*, ZD 2012, 3 (5 f.).
46 Dazu zählen Bayern (Art. 42 II PAG), Baden-Württemberg (§ 23 b II PolG), Hamburg (§ 24 PolDVG), Hessen (§ 15 b HSOG), Mecklenburg-Vorpommern (§ 33 d III SOG), Niedersachsen (§ 33 a II NPOG), Nordrhein-Westfalen (§ 20 c II PolG), Rheinland-Pfalz (§ 36 III POG) und Thüringen (§ 34 a II PAG). Medienberichten zufolge plant die Bundesregierung einen Gesetzesentwurf, der eine Ermächtigung der Bundespolizei zur Quellen-TKÜ enthält. *Krempl*, Bundespolizei: Hacken im Staatsauftrag mit Quellen-TKÜ und Staatstrojaner, heise online vom 30.11.2020.
47 Die ermittelnde Behörde muss dann technisch sicherstellen, dass die gespeicherten Inhalte und Umstände Gegenstand eines Übertragungsvorgangs waren, der ab dem Zeitpunkt der Anordnung der TKÜ-Maßnahme stattgefunden hat (§ 100 a V 1 Nr. 1 b StPO).
48 Vgl. BT-Drs. 18/12785, 49.
49 Der Gesetzgeber hat darauf reagiert, indem er den Zugriff auf gespeicherte Kommunikation erlaubt. S. BT-Drs. 18/12785, 49 f. Dazu im Einzelnen III. 2. b) bb).

b) *Laufende Kommunikation als Dauer der grundrechtstypischen Gefährdungslage.* So sehr es auf den ersten Blick einleuchtet, die laufende Kommunikation allein nach dem technischen Übertragungsvorgang zu bestimmen, so sehr greift eine solche Lesart im Lichte der Zwecksetzung der Quellen-TKÜ und der Grundrechtsdogmatik im Ergebnis zu kurz. Denn zum einen zielt die Quellen-TKÜ gerade auch auf verschlüsselte Messenger-Kommunikation, drohte also teilweise leerzulaufen, wenn sie diese nicht erfasst. Zum anderen schützt Art. 10 I GG die Vertraulichkeit der Fernkommunikation im Rahmen digitaler Kommunikationsformen, wie zB IMAP-E-Mails, nicht nur während des Übermittlungsvorgangs.[50] IMAP-E-Mails verbleiben auf dem Server des Providers, bis der Nutzer sie löscht.[51] Die Gefahr, dass der Provider auf die E-Mails zugreift, ist daher nicht schon in dem Moment gebannt, in dem die Nachricht im E-Mail-Postfach ankommt und damit der technische Vorgang der Übertragung beendet ist. IMAP-E-Mails erfasst Art. 10 I GG vielmehr so lange, wie sie im Postfach auf dem Server des Providers gespeichert sind (selbst wenn der Empfänger sie schon gelesen hat).[52]

Für die Abgrenzung, ob es sich um laufende Kommunikation im Sinne der Grundrechtsdogmatik handelt, ist insofern nicht allein entscheidend, ob der Übertragungsvorgang noch stattfindet, sondern ob die grundrechtsspezifische Gefährdungslage andauert.[53]

aa) *Anknüpfung an die Zugriffsgefahr durch den Kommunikationsmittler (E-Mail auf dem Server des Providers).* Die *übermittlungstypische* Gefährdungslage besteht, solange sich die Kommunikationsinhalte zum Zeitpunkt des staatlichen Zugriffs (noch) nicht im alleinigen Herrschaftsbereich des Empfängers (also ausschließlich auf seinem Endgerät) befinden – so etwa wenn sie (wie die IMAP-E-Mail) unverschlüsselt auf dem Server des Providers gespeichert sind.[54]

Sobald die Kommunikation sicher[55] Ende-zu-Ende-verschlüsselt ist, ist diese Gefährdungslage aufgehoben. Denn die Kommunikationsinhalte liegen dann auf dem Endgerät in der alleinigen Obhut des Empfängers. Sie sind auch dem Provider nicht zugänglich: Die Verschlüsselung schließt den Zugriff Dritter trotz des Übermittlungsvorgangs gerade aus. Sie macht ein aktives „Mitlesen" auf dem Transportweg unmöglich.

Die „laufende Kommunikation" auf den gesamten Vorgang zu erstrecken, in dem die Kommunikationsdaten auf dem Endgerät verbleiben, schösse daher – mit Blick auf die fehlende Gefährdungslage für Ende-zu-Ende verschlüsselte Kommunikationsdaten – über das Ziel hinaus. Weder die herkömmliche enge Begriffsbestimmung (technischer Übertragungsvorgang) noch das Festmachen an einer *übermittlungs*typischen Gefährdungslage sind deshalb im Ergebnis dazu in der Lage, das Phänomen der „laufenden Kommunikation" im Kontext der Quellen-TKÜ grundrechtsdogmatisch sauber zu erfassen.

bb) *Anknüpfung an den Zeitpunkt der Ende-zu-Ende-Verschlüsselung.* Erwächst die Gefahr für die Vertraulichkeit der Kommunikation im Falle der Ende-zu-Ende-Verschlüsselung gerade nicht aus dem Transport, ist der Dreh- und Angelpunkt für den Erfolg und die grundrechtliche Sensibilität der Quellen-TKÜ weniger der *Übertragungs-* als der *Verschlüsselungs*zeitpunkt. Um einen laufenden von einem abgeschlossenen Kommunikationsvorgang trennscharf abzugrenzen, sollte es im Falle der Quellen-TKÜ daher maßgeblich darauf ankommen, wann die Ende-zu-Ende-Verschlüsselung ansetzt, dh wann sich unverschlüsselte Inhalte ausleiten lassen. Denn ein Kommunikationsvorgang ist grundrechtlich nicht erst ab dem Moment *»abgeschlossen«*, in dem er im dauerhaften Speichermedium archiviert[56] ist, sondern auch, wenn dem Staat infolge der Verschlüsselung der Weg versperrt bleibt, die Angreifbarkeit des Übermittlungsvorgangs auszunutzen. Die Quellen-TKÜ erfasst insofern dann noch *laufende* Kommunikation, wenn die Ausleitung bei ausgehenden Nachrichten unmittelbar zu Beginn des Verschlüsselungsverfahrens bzw. bei eingehenden Nachrichten am Ende des Entschlüsselungsverfahrens ansetzt.[57]

Sie muss dabei aber zugleich garantieren, dass sich die Überwachung nicht auf jede Art verschlüsselter Nachrichten bezieht, sondern sich speziell auf Schutzmaßnahmen der Ende-zu-Ende-Verschlüsselung beschränkt, welche die Kommunikationspartner dazu nutzen, um die Vertraulichkeit während des Übertragungsvorgangs herzustellen.[58] Dafür muss der Ver- bzw. Entschlüsselungsvorgang klar einem Willensakt des Senders und Empfängers zugeordnet sein: Denn aus Sicht des Grundrechtsträgers beginnt der Kommunikationsvorgang mit dem „Senden" und endet mit dem „Öffnen" der übermittelten Information.

Diese Eigenart der Quellen-TKÜ hatte der Gesetzgeber auf den ersten Blick (obgleich er eine etwas andere Terminologie zugrunde legte)[59] auch vor Augen, als er § 100 a I 3 StPO schuf, um sicherzustellen, dass ein Ende-zu-Ende-verschlüsseltes Gespräch über Messenger-Dienste wie *WhatsApp* oder *Signal* nicht per se unverwertbar ist:[60] Der Gesetzgeber lässt dort zu, *gespeicherte* Inhalte und Umstände verschlüsselt erfolgender Telekommunikationsvorgänge („während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form") zu überwachen,

50 *BVerfGE* 124, 43 (55 f.) = NJW 2009, 2431 (2432 f.) Rn. 47 f.
51 *Heckmann*, jurisPK-Internetrecht, 6. Aufl., 2019 Kap. 7 Rn. 157.
52 Dem Schutzzweck des Art. 10 I GG entspricht es, die grundrechtliche Einhegung dieser drittvermittelten privaten Kommunikation von der technischen Signalübermittlung zu entkoppeln, vgl. *BVerfGE* 124, 43 (54 ff.) = NJW 2009, 2431 (2432) Rn. 45 ff.
53 *BVerfGE* 124, 43 (55 f.) = NJW 2009, 2431 (2432 Rn. 47 f.); zustimmend *Schwabenbauer*, AöR 137 (2012), 1 (16); *Hermes* in *Dreier*, GG, 3. Aufl., 2013 Art. 10 Rn. 38; krit. dagegen *Durner* in *Maunz/Dürig*, GG, 91. Erg.-Lfg. (April 2020) Art. 10 Rn. 128; *Krüger*, MMR 2009, 680 (682).
54 In dieses Schema fügt sich die Kommunikation via Messenger nur, wenn sie *nicht* Ende-zu-Ende-verschlüsselt ist. Denn dann kann der Anbieter die Nachrichten (ebenso wie im Fall der IMAP-E-Mail) einsehen, solange sie auf dem Server der Kommunikationsanwendung verbleiben. Der Schutz des Art. 10 I GG hält dann an, bis der Nutzer die Kommunikationsdaten aus dem Nachrichtenverlauf löscht und somit ausschließt, dass der Kommunikationsanbieter auf die Daten zugreift. Vgl. zur Herrschaftsbereichsdogmatik auch *BVerfGE* 115, 166 (184) = NJW 2006, 976 (978) Rn. 73; *BVerfGE* 120, 274 (307 f.) = NJW 2008, 822 (825) Rn. 185; 124, 43 (55) = NJW 2009, 2431 (2432) Rn. 45.
55 S. dazu VI.
56 In Abgrenzung dazu ist das Datum noch nicht in diesem Sinne „gespeichert", wenn es sich während der laufenden Kommunikation im Arbeitsspeicher befindet.
57 Bei vielen Messengern ist das bereits mit dem Drücken der „Senden"-Taste der Fall: Verschlüsselung und Versendung finden dann automatisch nacheinander statt. Bei OpenPGP-Verschlüsselungsverfahren – etwa mit dem AddOn *Enigmail* des EMail-Clients *Thunderbird* – muss der Nutzer nach der Betätigung der Senden-Taste hingegen zunächst noch ein Passwort eingeben, bevor die EMail endgültig (verschlüsselt) ihren Weg zum Empfänger antritt.
58 In eine ähnliche Richtung weist der Ansatz, nur die Transportverschlüsselung als Anwendungsfall der Quellen-TKÜ zu betrachten und die Inhaltsverschlüsselung auszuschließen, *Buermeyer*, StV 2013, 470 (474).
59 Mit laufender Telekommunikation (§ 100 a I 2 StPO) meint der Gesetzgeber – wie sich aus dem systematischen Zusammenhang (insbes. der Abgrenzung zu § 100 a I 3 StPO) ergibt – allein den technischen Übertragungsvorgang im öffentlichen Telekommunikationsnetz (ohne Rücksicht auf den Zeitpunkt der Ver- oder Entschlüsselung).
60 Vgl. BT-Drs. 18/12785, 50. Näher III. 2. a).

die hätten überwacht werden können, wenn sie unverschlüsselt erfolgt wären. Die Vorschrift lässt sich so deuten, dass es ihr im Kern darum bestellt ist, den zulässigen Zugriff auf die ermittlungsrelevanten Daten vom Übertragungsvorgang zu entkoppeln. Das ist durchaus auch grundrechtsdogmatisch konsequent. Denn sobald die Ende-zu-Ende-Verschlüsselung greift, besteht während des Übertragungsvorgangs keine grundrechtstypische Gefährdungslage mehr: Wenn der Übertragungsvorgang beginnt, sind die Nachrichten bereits verschlüsselt – und werden erst entschlüsselt, wenn der Übertragungsvorgang abgeschlossen ist.[61]

Ob die Befugnisnorm aber auch zuverlässig sicherstellt, dass kein Zugriff auf *vergangene* Kommunikation (etwa im Chatverlauf) erfolgt, gibt der Wortlaut nicht eindeutig zu erkennen. Er deckt auch den Zugriff auf *archivierte Daten*, also abgeschlossene Kommunikation, die in E-Mail-Postfächern oder Messenger-Konten liegen.[62] Für diese Deutung streitet zumindest Abs. 5 1 Nr. 1 b der Vorschrift: Er lässt die Aufzeichnung solcher Inhalte und Umstände der Kommunikation zu, „die ab dem Zeitpunkt der [richterlichen] Anordnung nach § 100 e I" hätten aufgezeichnet werden können. Die Vorschrift scheint es damit zu gestatten, den Nachrichtenverlauf rückwirkend ab dem Anordnungszeitpunkt auszulesen. Jedenfalls liegt zwischen Anordnung und Inbetriebnahme der Überwachungssoftware unvermeidlich ein Zeitabschnitt. In dieser Lesart gewährt die Norm für diesen Zeitabschnitt einen Blick in die Vergangenheit, genauer: in Nachrichtenarchive.

Dann überschreitet der Gesetzgeber jedoch die feine Linie, die das *BVerfG* als äußere Grenze einer Quellen-TKÜ gezogen hat, indem es die Überwachung ausdrücklich auf Daten aus einem laufenden Kommunikationsvorgang beschränkt hat.[63] Denn ein Datum, das auf einem dauerhaften Speichermedium archiviert ist, entstammt keinem aktuellen Kommunikationsvorgang mehr. Das erkennt auch die Begründung des Gesetzesentwurfes im Grundsatz an.[64] Dennoch sieht § 100 a StPO keine strengeren Anforderungen für die Überwachung der gespeicherten Kommunikation vor als für die laufende. Das ergebe sich aus der *funktionellen Äquivalenz* zur herkömmlichen Telekommunikationsüberwachung: Denn die Überwachung beschränke sich *in tatsächlicher Hinsicht* auf Kommunikationsinhalte, die *nach* dem Anordnungszeitpunkt übertragen wurden (§ 100 a V 1 Nr. 1 b StPO).[65] Mit dieser Einschränkung hat der Gesetzgeber versucht, eine vergleichbare Wertung wie das *BVerfG* vorzunehmen, als es die Quellen-TKÜ auf laufende Kommunikation beschränkte: Die Quantität und Qualität der erhobenen Daten soll wertungsmäßig den Daten gleichen, die eine herkömmliche Telekommunikationsüberwachung hervorbringt.[66]

Statt an den Topos der laufenden Kommunikation, also den gerade stattfindenden Kommunikationsvorgang, knüpft die Vorschrift aber letztlich an den vergangenen Übertragungsvorgang an. Es soll mithin genügen, den Kommunikationsvorgang zu rekonstruieren. Der Eingriffszweck der Maßnahme, die rückwirkend auf Nachrichtenarchive bis zum Datum der Anordnung zugreift, ist jedoch nicht mehr ohne weiteres mit der herkömmlichen Telekommunikationsüberwachung vergleichbar.[67] Denn auch Letztere erfasst nur Daten, die der Provider ab Implementierung der Maßnahme tatsächlich ausleitet, und wirkt nicht auf den Anordnungszeitpunkt zurück. Wenn eine Quellen-TKÜ auf archivierte Inhalte in Speichermedien zugreift, überschreitet sie mithin die Schwelle zur Online-Durchsuchung. Nur wenn ausgeschlossen ist, dass bloße Nachrichtenentwürfe oder archivierte Nachrichten gleichsam in das Schleppnetz der staatlichen Überwachung geraten und ein Zugriff auf sonstige Bereiche des Endgeräts nicht erfolgt, vollzieht sich die Quellen-TKÜ im Gleichlauf mit den traditionellen Formen der TKÜ (und damit in dem verfassungsrechtlichen Radius, den die Begrenzung auf „laufende Kommunikation" der Quellen-TKÜ zieht).[68]

§ 100 a StPO lässt sich bei engem Verständnis aber auch anders, nämlich womöglich verfassungskonform, lesen: „Gespeichert" kann auch die Ausleitung zu Beginn oder Ende des Verschlüsselungsverfahrens meinen, solange die Kommunikationssoftware die Daten aus technischen Gründen *kurzfristig (im Arbeitsspeicher) zwischenspeichert*.[69] Das Tatbestandsmerkmal „ab dem Zeitpunkt der Anordnung nach § 100 e Absatz 1" (§ 100 a V Nr. 1 lit. b StPO) ist in dieser Deutung so konzipiert, dass es das Aufzeichnungsspektrum zusätzlich begrenzt. Das entspricht auch der normativen Rationalität des Abs. 5 als technische Begrenzung der Überwachungs- und Aufzeichnungsermächtigung.

Jede verfassungskonforme Auslegung findet jedoch ihre Grenze in dem klar erkennbar geäußerten Willen des historischen Gesetzgebers.[70] Dieser zeigt in die genau entgegengesetzte Richtung: Die Beschlussempfehlung des Ausschusses für Recht und Verbraucherschutz zur Vorschrift bringt an zahlreichen Stellen zum Ausdruck, dass der Gesetzgeber auch von der Möglichkeit „rückwirkende[n] Ausleitens"[71] ab Erlass der richterlichen Anordnung ausgeht und dass dies „anhand der zu den einzelnen Textnachrichten hinterlegten Metadaten, die Absende-, Empfang- und Lesezeitpunkte enthalten",[72] zu ermitteln sei. Er wollte mithin ermöglichen, dass ab der richterlichen Anordnung auch rückwirkend verschlüsselte Nachrichten überwacht und ausgeleitet werden dürfen. Die Vorschrift lässt sich in diesem Lichte nicht anders auslegen, als dass sie auch eine Überwachung archivierter verschlüsselter Kommunikation gestattet. In der Sache erlaubt § 100 a I 3 iVm V Nr. 2

61 Das lassen jedenfalls die technischen Rahmenbedingungen zu; s. auch III. 2. a).
62 *Roggan*, StV 2017, 821 (824).
63 *Singelnstein/Derin*, NJW 2017, 2646 (2648).
64 Sie verweist darauf, dass es sich um keine laufende Kommunikation handele und deswegen der Eingriff nicht unmittelbar an Art. 10 GG, sondern am IT-Grundrecht sowie am informationellen Selbstbestimmungsrecht zu messen sei, BT-Drs. 18/12785, 50.
65 BT-Drs. 18/12785, 50.
66 Gegen die analoge Anwendung einer Schutzbereichsausnahme *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, 16.
67 Vgl. *Freiling/Safferling et al.*, JR 2018, 9 (21); *Großmann*, JA 2019, 241 (244); *Hauck* in *Löwe/Rosenberg*, StPO, 27. Aufl., 2019 § 100 a Rn. 147; *Roggan*, StV 2017, 821 (824); *Sinn*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 31.5. 2017, 5 ff.; iE auch *Singelnstein/Derin*, NJW 2017, 2646 (2648). Die Software müsste zudem *alle* Daten durchforsten, um anhand der Metadaten herauszufinden, welche Daten dem vorgegeben Zeitraum entsprungen sind, *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, 17; a. A. *Bär*, 28. Kapitel – EDV-Beweissicherung in *Wabnitz/Janovsky/Schmitt*, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl., 2020 Kap. 28, Rn. 92; *Krauß*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 31.5.2107, 9; *Ruppert*, Jura 2018, 994 (1001).
68 Dazu näher II. 2.
69 *Bär* in *Heintschel-Heinegg/Stöckel*, KMR StPO, 91. Erg.-Lfg. (1.6. 2019) § 100 a Rn. 44.
70 Vgl. bspw. *BVerfGE* 148, 69 (267) – st. Rspr.
71 BT-Drs. 18/12785, 52.
72 BT-Drs. 18/12785, 53.

StPO eine Online-Durchsuchung, die – trotz der vorgesehenen Schutzmechanismen, insbesondere der richterlichen Anordnung – nicht den Anforderungen an einen zulässigen Eingriff in das IT-Grundrecht genügt.[73] Denn § 100 a I 1 Nr. 1, 2 setzt „lediglich" eine schwere Straftat voraus. Sie verbürgt damit nicht das Höchstmaß an Tatschwere, das mit der Eingriffsintensität einer Online-Durchsuchung aber korrespondieren muss, damit der Eingriff verhältnismäßig ist.[74]

3. Konkretisierung der technischen und verfahrensrechtlichen Mittel, die eine Begrenzung auf laufende Kommunikation sicherstellen

Auch soweit sich Maßnahmen der Quellen-TKÜ nach dem *Wortlaut* der Regelungen auf laufende Kommunikationsvorgänge beschränken (vgl. § 100 a I 2 StPO, § 51 II 1 Nr. 1 BKAG), müssen die Vorschriften in hinreichend bestimmter Weise sicherstellen, dass der *praktische Vollzug* auch realiter ausschließlich die laufende Kommunikation erfasst. Wie konkret die Regelungen formuliert sein müssen, zeichnet insoweit der verfassungsrechtliche *Wesentlichkeitsvorbehalt* vor:[75] Wann laufende Kommunikation genau endet, entpuppt sich nicht lediglich als bloße Modalität der Umsetzung, sondern als eine grundrechtlich in hohem Maße sensible Trennlinie.[76] Denn von der Frage, ob und wie sich der Zugriff auf das Endgerät technisch begrenzen lässt, hängt es ab, ob die Maßnahme verfassungsrechtlich als Eingriff in Art. 10 GG oder das IT-Grundrecht einzuordnen ist. Sie markiert den Dreh- und Angelpunkt der verfassungsrechtlichen Bewertung staatlicher Schadsoftware zur Quellen-TKÜ auf Endgeräten.

Ob bzw. wie die Vorgabe umzusetzen ist, die Quellen-TKÜ in der Praxis der Ermittlungsbehörden *technisch auf laufende Kommunikation* zu begrenzen, lassen die einfachgesetzlichen Vorschriften jedoch im Wesentlichen offen.[77] Zwar sehen die Vorschriften eine Protokollpflicht (§ 100 a VI StPO, § 82 I, II Nr. 8 BKAG) ebenso wie einen Richtervorbehalt vor (§ 51 III BKAG, § 100 e I StPO). Die richterliche Anordnung spezifiziert jedoch nur Art, Umfang und Dauer der Maßnahme (§ 51 V 2 Nr. 3 BKAG, § 100 e III 2 Nr. 3 StPO), nicht aber notwendigerweise ihre technische Umsetzung. In der Praxis wirft aber exakt sie die entscheidenden Fragen auf. Das Landesverfassungsgericht Sachsen-Anhalt hielt der Landesregierung beispielsweise vor, sie habe kein technisches Mittel vorbringen können, mit dem es ihr möglich war, die Norm passgenau umzusetzen – und bescheinigte der landespolizeirechtlichen Befugnis zur Quellen-TKÜ (§ 17 c SOG LSA aF) daher ihre Verfassungswidrigkeit.[78]

Das *BVerfG* hat sich in seinem Urteil zum BKAG im Jahre 2016 hingegen zurückhaltender gezeigt: Es zog sich auf die „formale Position[...]"[79] zurück, dass das *Ob* und *Wie* der technischen Begrenzung nicht die *Gültigkeit*, sondern allein die verfassungsrechtlich zulässige *Anwendung* der Norm betreffe.[80] Selbst wenn eine Norm deshalb leerläuft, weil sich ihre Anforderungen technisch nicht umsetzen lassen, ist sie nach Auffassung des Gerichts nicht verfassungswidrig, sondern lediglich nicht anwendbar; immerhin könnten sich die technischen Voraussetzungen ja in Zukunft noch verändern.[81]

Der Gesetzgeber kommt jedoch nicht umhin, die einfachrechtlichen Anforderungen an die Begrenzung einer Quellen-TKÜ auf laufende Kommunikation im Gesetz zu konkretisieren, um die Vollzugspraxis der Ermittlungsbehörden in verfassungskonformer Weise vorzuzeichnen.

Nicht nur der Wesentlichkeitsvorbehalt, sondern auch das *Gebot der Normenklarheit* legt die Messlatte für die Befugnisnorm hoch: Soll Art. 10 GG wirksamen grundrechtlichen Schutz entfalten, muss die Ermächtigungsnorm die Grenzen des Eingriffs nach Art und Schwere bereichsspezifisch und präzise festlegen.[82] Selbst wenn Daten, die nicht zur laufenden Kommunikation gehören, nicht reflexartig dem unantastbaren Kernbereich privater Lebensgestaltung zuzuordnen sind, können sie gleichwohl einen tiefen Einblick in die Privatsphäre eröffnen.[83] Der Eingriff löst daher hohe Anforderungen an die Bestimmtheit und Klarheit der Norm aus.[84]

Soweit die geltenden Normen die Maßnahme auf „laufende Kommunikation" beschränken, spiegeln sie zwar die grundsätzlichen verfassungsrechtlichen Vorgaben wider. Um den Anforderungen des Wesentlichkeitsvorbehalts und der Normenklarheit zu genügen, müssen sie aber präzisieren, welche Vorkehrungen auf technischer und rechtlicher Ebene zu treffen sind, um zu verhindern, dass Inhalte außerhalb der laufenden Kommunikation in staatliche Hände geraten. Die grundsätzliche Spezifizierung der technischen Umsetzung einer Quellen-TKÜ muss ihren Weg also (jedenfalls ansatzweise) in die Ermächtigung finden.[85] Der Gesetzgeber hätte im einfachen Recht zumindest erkennbar und für die Vollzugspraxis handhabbar vorzeichnen müssen, mit welchen technischen Mitteln die Behörden sicherzustellen haben, dass ihre Quellen-TKÜ die Demarkationslinie zur laufenden Kommunikation nicht überschreiten.[86] Dies gilt umso mehr, als bereits unklar ist, ob es technisch überhaupt möglich ist, den Vorgaben des *BVerfG* wirksam Rechnung zu tragen.[87] Dass es der Gesetzgeber in der Ermächtigungsgrundlage zur Quellen-TKÜ vollständig offengelassen hat, wie die Maßnahme technisch umzusetzen ist, widerspricht daher im Ergebnis den verfassungsrechtlichen Anforderungen.[88]

IV. Technische Beschränkung

Welche einfachrechtlichen Maßgaben eine Überwachungsmaßnahme auf laufende Kommunikation beschränken kön-

73 *Großmann*, JA 2019, 241 (243 f.); *Roggan*, StV 2017, 821 (824).
74 Die Eingriffsintensität ist vergleichbar mit einem Eingriff in die Unverletzlichkeit der Wohnung. Dazu *BVerfGE* 141, 220 (269 f., 304) = NJW 2016, 1781 (1784) Rn. 105 ff.; (1794) Rn. 210; *Eschelbach* in *Satzger/Schluckebier/Widmaier*, StPO § 100 b Rn. 12; *Freiling/Safferling et al.*, JR 2018, 9 (21); *Roggan*, StV 2017, 821 (826).
75 *Grzeszick* in *Maunz/Dürig*, GG, 51. Erg.-Lfg. (Stand: Dez. 2007) Art. 20 Abschnitt VI Rn. 106.
76 Im Ergebnis ebenso *Tomerius*, NVwZ 2015, 412 (415).
77 Vgl. bereits *Brodowski* JR 2011, 532 (535) mwN; s. auch *Eschelbach* in *Satzger/Schluckebier/Widmaier*, StPO, 4. Aufl. 2020, § 100 a Rn. 43; *Hauck* in *Löwe/Rosenberg*, StPO § 100 a Rn. 129, 151; *Roggan*, StV 2017, 821 (822).
78 *SachsAnhVerfG*, Urt. v. 11.11.2014 – LVG 9/13, BeckRS 2014, 58392 Rn. 154.
79 *Brink/Mitsdörffer*, Communicatio Socialis 2018, 60 (65).
80 Vgl. *BVerfGE* 141, 220 (311) = NJW 2016, 1781 (1796 f.) Rn. 234.
81 *BVerfGE* 141, 220 (311) = NJW 2016, 1781 (1796 f.) Rn. 234; im Ergebnis auch BT-Drs. 18/12785, 53; zustimmend *Schlegel*, Normative Grenzen für internetbasierte Ermittlungsmethoden, 2019, 95 f.
82 *BVerfGE* 110, 33 (53) = NJW 2004, 2213 (2215).
83 S. II. 1.
84 Vgl. *BVerfGE* 110, 33 (55) = NJW 2004, 2213 (2216).
85 Für Details kann sie eine Verordnungsermächtigung vorhalten. Vgl. *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, 20.
86 S. auch *Sieber/Brodowski* in *Hoeren/Sieber/Holznagel*, Hdb Multimedia-Recht, 46. Erg.-Lfg. (Januar 2018) Teil 19.3 Rn. 150.
87 Vgl. bereits *Brodowski*, JR 2011, 532 (535) mwN; s. auch *Eschelbach* in *Satzger/Schluckebier/Widmaier*, StPO § 100 a Rn. 43; *Hauck* in *Löwe/Rosenberg*, StPO § 100 a Rn. 129, 151; *Roggan*, StV 2017, 821 (822).
88 Vgl. auch *Tomerius*, NVwZ 2015, 412 (415).

nen, richtet sich nach den technischen Möglichkeiten. Die Software erreicht dieses Ziel, wenn sie ihre Funktionalität darauf reduziert, nur die laufende Kommunikation anzuzapfen.

1. Beschränkende technische Vorkehrungen

Einen ersten denkbaren Ansatzpunkt, um den Zugriffsradius einer Überwachungssoftware auf dem Endgerät technisch zu begrenzen, eröffnet der Umstand, dass moderne Betriebssysteme über eine Zugriffskontrolle verfügen, um die Applikationen untereinander sowie den Betriebssystemkern zu schützen.[89] Welche Zugriffsrechte einem Nutzer bzw. einem Programm zustehen, hängt dabei von dem Modus ab, in dem das Programm läuft. Im *Benutzermodus* stehen der Software nicht alle Privilegien zur Verfügung.[90] Im *Kernelmodus* kann der Nutzer demgegenüber grundsätzlich unbeschränkt auf Hardware und Daten zugreifen; jeder Befehl ist also zur Ausführung zugelassen.[91]

Der Benutzermodus reicht durchaus aus, um Nutzerdaten lesen und schreiben zu können (d. h. auch für Kommunikationsinhalte und -umstände).[92] Eine Überwachungssoftware ist kraft ihres Funktionsauftrags aber zumindest teilweise auf den Kernelmodus angewiesen, muss also mit maximalen Rechten ausgestattet sein. Denn sie ist darauf angewiesen, ihren heimlichen Eingriff effektiv tarnen zu können – insbesondere um die eigene Aktivität aus dem Dateisystemlogbuch[93] zu entfernen (sofern ein solches vorhanden ist), oder um Abwehrsoftware (wie Antivirenprogramme oder eine Firewall) zu täuschen.[94] Im Nutzermodus ist dies nicht möglich.

Damit verbindet sich jedoch zugleich ein ungewollter Nebeneffekt: Im Kernelmodus verfügt die Software reflexartig auch über die Möglichkeit, jegliche Datenquellen wie Bildschirmanzeige, Kamera- und Mikrofondaten oder Mausbewegungen mitzuschneiden. Stehen der Software auf dieser Ebene maximale Rechte zu, ist sie technisch nicht wirksam beschränkt.[95] Genau diese Eigenschaft der Überwachungssoftware ist es aber, die ihre Nutzung besonders grundrechtssensibel macht. Es lässt sich nicht sicher ausschließen, dass eine Ermittlungsmaßnahme gleichsam als Quellen-TKÜ „springt“, aber missbräuchlich als Online-Durchsuchung des gesamten Endgeräts „landet“.

2. Rechtliche Beschränkung der technischen Funktionen

Lässt sich der Zugriff auf die laufende Kommunikation durch rein technische Maßnahmen nicht wirksam a priori beschränken, verbleiben *rechtliche* Zugriffsbeschränkungen, um sicherzustellen, dass die Maßnahmen verfassungsrechtlich zulässig sind. Solche rechtlichen Begrenzungen, die sich auf technische Funktionen beziehen, können im Verbund mit verfahrensrechtlichen Vorkehrungen[96] dazu beitragen, die Quellen-TKÜ einzuhegen, indem sie rechtlich ausschließen, dass der Anwender von anderen Funktionen Gebrauch macht. Die rechtlichen Vorgaben können in die Konfiguration der Software einfließen, etwa indem die Benutzeroberfläche für denjenigen, der die Überwachung unmittelbar durchführt, nur rechtlich zulässige Funktionen anbietet.[97]

a) *Gerätezugriff.* Um zu gewährleisten, dass sich die Aufzeichnung einer Überwachungssoftware ausschließlich auf laufende Kommunikation erstreckt, kann der Gesetzgeber den Gerätezugriff beschränken. Die Software ist dann rechtlich darauf limitiert, auf den Bildschirm, die Tastatur, die Kamera oder das Mikrofon zuzugreifen, während der Nutzer das jeweilige Gerät zur Kommunikation nutzt.[98]

Nicht alles, was ein Endgerät erfasst, betrifft jedoch Kommunikationsvorgänge – so etwa wenn die Software im 30-Sekunden-Takt einen *Screenshot* des Browser-Inhalts ausleitet.[99] Doch selbst wenn sich die Screenshots lediglich zum Zeitpunkt eines indizierten laufenden Telekommunikationsvorgangs – etwa während eines Videoanrufs – ausleiten ließen, stünde die Bildschirmaufnahme in keinem ausreichend engen Zusammenhang mit dem Kommunikationsvorgang. Denn auch während der Nutzer kommuniziert, kann er sich auf dem Bildschirm Inhalte ansehen, die in keiner Verbindung zu einem laufenden Kommunikationsvorgang stehen. So könnte er, während er einem Videotelefonat folgt, im Browser auch gesundheitliche Fragen und Antworten recherchieren.

Die gleiche Problematik stellt sich beim Einsatz eines Überwachungsprogramms ein, das die Tastenanschläge protokolliert (sog. *Keylogging*).[100] Bei Mehrzweckgeräten wie Laptops oder Smartphones, die sich oftmals durch eklektisches Nutzerverhalten auszeichnen, ist es – anders als etwa bei einem gewöhnlichen Telefon – in praxi unmöglich, auf dem Endgerät via Keylogging nur laufende Kommunikationsvorgänge anzuzapfen. Erkenntnisse aus Screenshots und Keyloggern zu gewinnen, sollte der Behörde daher ausdrücklich verboten sein.[101]

Den Ton mitzuschneiden oder eine Kameraaufnahme zu tätigen, steht dagegen in einem engeren Zusammenhang zu einem *Voice-over-IP*-Kommunikationsvorgang: Während eines Videotelefonats verwendet der Nutzer in der Regel die Kamera und das Mikrofon allein für sein laufendes Gespräch. Dennoch bestehen auch hier überschießende Überwachungsmöglichkeiten. Der Nutzer kann etwa während eines Videotelefonats die Tonübertragung ausschalten. Der Kommunikationspartner nimmt dann kein Wort davon wahr, was sein virtuelles Gegenüber spricht – die Überwachungssoftware hingegen schneidet weiterhin den Ton über das Mikrofon mit (und könnte dabei etwa ein privates Gespräch der verdächtigen Person mit Dritten aufzeichnen).[102] Auch die Kamera kann weiter aufnehmen und Bilder an die Ermittler ausleiten, während die Videoübertra-

89 *Glatz*, Betriebssysteme, 3. Aufl., 2015, 26.
90 *Mandl*, Grundkurs Betriebssysteme, 4. Aufl., 2014, 25.
91 *Glatz*, Betriebssysteme, 26.
92 *Rehak*, Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 2013, 24.
93 Ein Dateisystemlogbuch protokolliert alle oder spezifische Vorgänge auf einem Computersystem.
94 *Rehak*, Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 25.
95 Im Ergebnis auch *Neumann/Kurz et al.*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 31.5.2017, 10 f.
96 Dazu im Einzelnen unten in V.
97 Vgl. zur Funktionstrennung V. 2.
98 Die Aktivierung von Gerätefunktionalitäten ist selbst für die Online-Durchsuchung nicht erlaubt, vgl. *Soiné*, NStZ 2018, 497 (502).
99 *LG Landshut*, Beschl. v. 20.1.2011 – 4 Qs 346/10, BeckRS 2011, 2429; dazu *Brodowski*, JR 2011, 532 (536); *Skistims/Roßnagel*, ZD 2012, 3 (5).
100 *Skistims/Roßnagel*, ZD 2012, 3 (5). Endgeräte können darüber hinaus mit weiteren Sensoren ausgestattet sein, die bspw. die Herzfrequenz messen, und somit sehr sensible Daten generieren, vgl. *Herpig*, A Framework for Government Hacking in Criminal Investigations, October 2018, 19.
101 Implizit lässt sich das auch aus § 100 a V 1 Nr. 1 StPO herauslesen, *Bruns* in *Hannich*, KK StPO § 100 a Rn. 45.
102 *Rehak*, Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 44 f.

gung für den Kommunikationspartner ausgeschaltet ist. Zudem bergen Videoaufnahmen (noch mehr als Tonaufnahmen[103]) generell das Risiko, dass sie auch Aspekte mitschneiden, die in keinem Zusammenhang mit dem Kommunikationsvorgang stehen – etwa wenn die Hintergrundaufnahme Einblick in die private Wohnung, beispielsweise das Schlafzimmer des Kommunizierenden, gewährt. Erlaubt das Gesetz einen Zugriff auf Kamera und Mikrofon, muss es den damit einhergehenden spezifischen Gefährdungen für die Privatsphäre jedenfalls durch besondere Vorkehrungen Rechnung tragen.

Für Gespräche via Messenger, also asynchrone Kommunikation, kommt der Gerätezugriff ohnedies nicht infrage. Denn eine Nachricht aufzunehmen oder zu schreiben, ist der Entscheidung, die Nachricht zu verschlüsseln, um sie anschließend zu übertragen, immer zeitlich vorgelagert. Nur bei synchroner Kommunikation (z. B. VoIP-Telefonie) sind die Geräte gleichzeitig mit dem laufenden Kommunikationsvorgang aktiv.[104]

b) *Ausrichtung auf ein spezifisches Kommunikationsprogramm.* Zielsicherer, als auf *Eingabegeräte* zuzugreifen, ist es, eine Überwachungssoftware so auf ein bestimmtes Kommunikationsprogramm zuzuschneiden,[105] dass sie die *Programmabläufe* erkennt. Sie müsste dann anhand der Programmaktivitäten detektieren, wann der Betroffene das Kommunikationsprogramm zur laufenden Kommunikation und wann er es nur zur Vorbereitung nutzt, beispielsweise um Videonachrichten aufzunehmen:[106] Nur wenn das Programm einen Übertragungs- oder (bei asynchroner Kommunikation) einen Ende-zu-Ende-Verschlüsselungsvorgang in Gang setzt, leitet die Überwachungssoftware die unverschlüsselten Kommunikationsinhalte und -umstände aus.[107] Ebenso könnte sie feststellen, wann der Betroffene Kommunikationsinhalte empfängt, um sie dann unmittelbar auszuleiten, nachdem sie auf dem Endgerät entschlüsselt sind. In allen anderen Fällen dürfte die Software die Informationen nicht an die Ermittlungsbehörde weitergeben.[108]

Damit der „Staatstrojaner" auf Kommunikationsanwendungen gezielt aufsetzen kann, um Daten der laufenden Kommunikation auszuleiten, muss er aber auch mit der Softwareentwicklung Schritt halten. Sonst weichen Zielpersonen auf neuartige Messenger etc. aus oder greift die Software tiefer in das auszuspähende System ein als nötig. Zugleich lässt sich eine Überwachungssoftware, die sich stets wandelt, nicht leicht durch eine parlamentsgesetzliche Regelung einschränken. Für nicht grundrechtssensitive Einzelfragen steht dem Gesetzgeber aber der Weg offen, eine Verordnungsermächtigung vorzusehen, auf deren Grundlage die Exekutive die abstrakten technischen und verfahrensrechtlichen Rahmenbedingungen passgenau konkretisieren kann.

V. Verfahrensrechtliche Sicherungen

Die verfassungsrechtliche Vorgabe, den Zugriff einer Quellen-TKÜ auf die laufende Kommunikation zu beschränken, lässt sich ein Stück weit auch durch organisatorisch-prozedurale Maßnahmen einlösen.[109] Neben die rechtlichen Beschränkungen, die sich auf den technischen Funktionsradius beziehen, treten dann verfahrensrechtliche Sicherungen, die Defizite der technischen Begrenzung ausgleichen sollen.

Bei der Aufgabe, diese Prüfmechanismen im Detail auszugestalten, steht der Gesetzgeber zugleich vor der Herausforderung, die Geheimhaltungsbedürfnisse der Sicherheitsbehörden und die öffentlichen Kontrollbefugnisse in einen angemessenen Ausgleich zu bringen. Er genießt dafür einen weiten Regelungsspielraum – um beispielsweise zu regeln, ob und inwieweit der angewandte Exploit und die konkrete Verankerung der Software in dem Endgerät geheimhaltungsbedürftig sind. Funktionen, die es ermöglichen sollen, ausschließlich laufende Kommunikationsvorgänge auszuleiten, unterliegen demgegenüber einem größeren Kontrollbedarf.[110] Denn von ihnen hängt ab, ob die Ermittlungsmaßnahme den verfassungsrechtlichen Vorgaben im Einzelfall genügt. Ob eine Quellen-TKÜ in eine unzulässige Online-Durchsuchung umschlägt, muss in jedem Stadium überprüfbar und beeinflussbar bleiben.

1. Vorabkontrolle der Software

Ein verfahrensrechtlicher Kontrollmechanismus kann darin bestehen, eine unabhängige Stelle einzubinden. Sie prüft die Bestandteile der Überwachungssoftware, die ihre Funktionalität in der Praxis formen, vor ihrer Anwendung umfassend daraufhin, ob ihr Funktionsumfang im Einklang mit den rechtlichen Anforderungen steht. Der bzw. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat diese Rolle einer Ex-ante-Prüfung bisher übernommen und den Funktionsumfang einzelner Softwarebestandteile kontrolliert.[111] Außerdem hat ein externes Softwareprüflabor die „Rohversion" der Überwachungssoftware überprüft.[112]

a) *Veröffentlichung der Ergebnisse.* Die BfDI hat das Ergebnis ihrer Untersuchung aus dem Jahr 2016 nicht veröffentlicht.[113] Es liegt nur dem BKA und dem BMI vor. Eine öffentliche Kontrolle ist dadurch nur sehr eingeschränkt möglich. Pro futuro sollte der Gesetzgeber die Veröffentlichung der Kernergebnisse der Untersuchungen (soweit nicht zwingend geheimhaltungsbedürftig) – anders als bisher – explizit verankern.

b) *Kontrollinstrumente.* Soll die Prüfungsinstanz ihre Aufgaben sachgerecht wahrnehmen können, muss sie den Quellcode der Überwachungssoftware einsehen können und auch in der Lage sein, effektive Softwaretests (etwa mit Testdaten)[114] durchzuführen.[115]

103 In der Lesart der Rechtsprechung des *BGH* erfasst die herkömmliche Telekommunikationsüberwachung auch Raumgespräche, *BGH*, NStZ 2008, 473; krit. *Prittwitz*, StV 2009, 437 (442).
104 S. III. 2. a).
105 Vgl. auch BT-Drs. 18/12785, 53.
106 Vgl. *Brodowski*, JR 2011, 532 (536).
107 Vgl. *Bruns* in *Hannich*, KK StPO § 100 a Rn. 45; *Freiling/Safferling et al.*, JR 2018, 9 (17).
108 Die Version der „Remote Communication Interception Software" (RCIS), die das BKA anwendet, soll laut Medienberichten bspw. auf *Skype* in bestimmten Windows-Betriebssystemen zugeschnitten sein, *Flade*, Spähsoftware Bundestrojaner ist kaum brauchbar, welt.de vom 10.4.2016. S. zu der Entwicklung auch *Schlegel*, Normative Grenzen für internetbasierte Ermittlungsmethoden, 108. Die Bundesregierung stuft diese Details als geheimhaltungsbedürftig ein, BT-Drs. 19/1505, 9.
109 Vgl. *Braun*, jurisPR-ITR 2011, Anm. 3 (4); *Brodowski*, JR 2011, 532 (536).
110 S. III. 3.
111 Vgl. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2019, 54 f.
112 Vgl. BT-Drs. 19/1434, 5.
113 Vgl. *Beuth*, Der Staatstrojaner bleibt im Dunkeln, Spiegel Online vom 29.1.2018. Allerdings berichtete der BfDI von seinen Prüfungen gerafft in seinem Tätigkeitsbericht 2019, 54 f. Die Ergebnisse des externen Prüfungslabors stuft die Bundesregierung nahezu umfassend als geheim ein, vgl. BT-Drs. 18/13566, 2 ff.; 19/522, 6; 19/1434, 5. Eine Statistik- und Berichtspflicht trifft bislang nur die Behörden, welche die Quellen-TKÜ einsetzen (dazu V 3. b.).
114 S. auch *Herpig*, A Framework for Government Hacking in Criminal Investigations, 20.
115 Vgl. auch Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2019, 54 f.

Um dies uneingeschränkt sicherzustellen, sollte der Staat die einzelnen Bausteine der Überwachungssoftware im Idealfall selbst entwickeln.[116] Das BKA hat diesen Weg eingeschlagen: Verschiedene Versionen der eigens entwickelten „Remote Communication Interception Software" (RCIS) sind für die Quellen-TKÜ freigegeben.[117] Daneben setzen die Verantwortlichen aber weiterhin auf proprietäre Software privater Unternehmen[118] – in der Vergangenheit etwa des Anbieters *DigiTask*.[119] In diesem Fall ist es der Prüfungsinstanz nicht ohne weiteres möglich, Einblick in den Quellcode zu nehmen. *DigiTask* etwa wollte ihn nur herausgeben, wenn die Prüfungsinstanz eine Geheimhaltungsvereinbarung unterzeichnet und eine Gebühr entrichtet.[120]

Um dem vorzubeugen, hatten Bund und Länder im Jahr 2012 in der „standardisierenden Leistungsbeschreibung" (SLB) für die Quellen-TKÜ eine Transparenzpflicht vorgesehen: Die Anbieter bzw. Hersteller der Software mussten den Quellcode gegenüber der Prüfungsinstanz offenlegen.[121] Die im Jahr 2018 aktualisierte SLB enthält diese Vorgabe demgegenüber nicht mehr.[122] Pro futuro sollte die Rechtsordnung *gesetzlich* verbürgen, dass eine staatliche Prüfungsinstanz auch den Quellcode einsehen kann.[123] Da die Softwarebestandteile kontinuierlich weiterentwickelt werden, muss eine Kontrollinstanz sie darüber hinaus in festen Zyklen, jedenfalls aber im Anschluss an grundlegende Softwareveränderungen, kontrollieren und Tests vornehmen können, um die einzelnen Softwarekomponenten auf Herz und Nieren zu prüfen.[124] Denkbar ist es auch, der Kontrollinstanz eine Live-Schnittstelle einzurichten, über die sie ein Prüfverfahren mit den jeweils aktuellen Softwaremodulen durchführen kann.[125]

2. Kontrolle der konkreten Überwachungsmaßnahme

Als verfahrensrechtliche Schutzvorkehrung gegen eine überschießende Überwachungsreichweite der Quellen-TKÜ hat der Bundesgesetzgeber zwar angeordnet, dass die Behörden die Maßnahme auf der Grundlage des BKAG und der StPO nur vornehmen dürfen, wenn ein Gericht sie anordnet (§ 51 III BKAG, § 100 e I StPO).[126] Wie die fallspezifische Umsetzung und behördliche Konfiguration im Anschluss an die Anordnung erfolgt, unterliegt jedoch keiner unabhängigen technischen Kontrolle.[127]

Damit gehen Missbrauchsrisiken einher. Denn die eingesetzte Software ist individuell an den konkreten technischen Rahmen des zu infizierenden Geräts angepasst. Sie unterscheidet sich daher notwendig ein Stück weit von den Programmbausteinen, die nach der Vorabkontrolle freigegeben sind. Eine hinreichende technische Sicherung, die zuverlässig verhindert, dass die eingesetzte Überwachungssoftware unzulässig von der technischen Vorabkonfiguration abweicht, existiert derzeit nicht.

Das Kontrollregime sollte zudem darauf reagieren, dass Softwareupdates die zu überwachende Kommunikationssoftware modifizieren können.[128] Denn die Behörde kann die Überwachungssoftware jederzeit durch Aktualisierungen verändern, nachdem diese bereits auf dem System des Betroffenen aktiv ist.[129] Neben der punktuellen Vorabkontrolle ist es deshalb geboten, weitere verfahrensrechtliche Sicherungen während des Überwachungsverfahrens vorzusehen.[130]

Ein Schutzbaustein kann darin bestehen, das *Vier-Augen-Prinzip* gesetzlich zu verankern. Eine zweite Person innerhalb der Behörde kontrolliert dann die Ausführung des Überwachungsprogramms fortlaufend. Allerdings eignet sich dieses Verfahren eher für die Gegenkontrolle einzelner Entscheidungen, etwa Prüfungsentscheidungen – weniger demgegenüber, um einen komplexen und länger andauernden Prozess zu überprüfen. Dafür bietet sich eher eine *Funktionstrennung* an: Es kann sinnvoll sein, die Anpassung der Software an das konkrete Überwachungsverfahren einer anderen als derjenigen Stelle zuzuweisen, welche die Überwachungsmaßnahme selbst durchführt. Dieser bliebe dann die Möglichkeit versagt, die vorkonfigurierte Software (ohne Beteiligung der anderen Abteilung oder gar ohne neuen gerichtlichen Beschluss) zu verändern.

Denkbar ist darüber hinaus (in den Grenzen wirksamen Geheimnisschutzes) eine Kontrolle durch den intern zuständigen Datenschutzbeauftragten oder eine sonstige geeignete Instanz.[131] Externe, punktuelle Kontrollen durch eine eigens für diesen Zweck geschaffene Prüfungseinheit,[132] den BfDI oder das BSI könnten die internen Vorkehrungen flankieren. Der Kontrollinstanz könnte zudem das Recht zustehen, – vergleichbar mit § 100 d IV 4 StPO – eine richterliche Entscheidung herbeizuführen, wenn sie Zweifel an der Rechtmäßigkeit einer Maßnahme hat.

3. Ex-Post-Kontrolle

a) *Nachträgliche gerichtliche Kontrolle.* Ein wichtiger Baustein einer grundrechtskonformen Architektur der Quellen-TKÜ ist der wirksame Rechtsschutz. Um eine nachträgliche Kontrolle zu ermöglichen, hat die Behörde Betroffenen nach Abschluss des Eingriffs mitzuteilen, dass eine Quellen-TKÜ

116 *Kipker*, ZRP 2016, 88 (89).
117 Vgl. Landtag NRW Drs. 17/722; BT-Drs. 19/1505.
118 Vgl. BT-Drs. 19/1434, 6; *Kipker*, ZRP 2016, 88 (89).
119 *Lischka/Reißmann et al.*, Trojaner-Hersteller beliefert etliche Behörden und Bundesländer, Spiegel Online vom 11.10.2011.
120 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden, 14.8.2012 (29.10.2018). Damit verbinden sich indes keine unüberwindbaren Hindernisse. Einerseits kann das Prüfungsverfahren im Rahmen eines verwaltungsrechtlichen In-camera-Verfahrens stattfinden. Andererseits ließe sich das ggf. notwendige zusätzliche Entgelt bereits im Vergabeverfahren als Teil der Vergütung des Drittanbieters „einpreisen".
121 Bundeskriminalamt, Standardisierende Leistungsbeschreibung Quellen-TKÜ, fragdenstaat.de vom 2.10.2012.
122 Vgl. Bundeskriminalamt, Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, 5.10.2018.
123 Vgl. *Hauck* in *Löwe/Rosenberg*, StPO § 100 a Rn. 165; *Tinnefeld*, ZD 2012, 451 (452 f.). S. auch *Neumann/Kurz et al.*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 15.
124 S. auch *Neumann/Kurz et al.*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 16.
125 Vgl. zu einer Schnittstelle für Aufsichtsbehörden auch *Martini*, Blackbox Algorithmus, 2019, 256.
126 Vgl. zu dieser allgemeinen Voraussetzung für den heimlichen Zugriff in informationstechnische Systeme, bspw. *BVerfGE* 120, 274 (331) = NJW 2008, 822 (832) Rn. 257.
127 Krit. auch *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, Ausschuss-Drs. 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags, 19.
128 *Rehak*, Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 26.
129 Dies sieht auch die „standardisierende Leistungsbeschreibung" aus dem Jahr 2012 vor, Bundeskriminalamt (Fn. 123). Zu der Möglichkeit des Nachladens s. auch *Skistims/Roßnagel*, ZD 2012, 3 (6).
130 So auch *VfGH Österreich* 11.12.2019, G 72-74/2019, G 181-182/2019 (143) Rn. 192.
131 Bisher ist der behördliche Datenschutzbeauftragte innerhalb seiner allgemeinen gesetzlichen Kompetenzen eingebunden; vgl. BT-Drs. 12785, 52.
132 Der *VfGH Österreich* betont insofern zu Recht, dass die Kontrollinstanz die Maßnahme auch tatsächlich effektiv und unabhängig kontrollieren können muss. Dafür muss sie mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestattet sein. *VfGH Österreich* 11.12.2019, G 72-74/2019, G 181-182/2019 (144 f.) Rn. 193 f.

stattgefunden hat (§ 101 IV 1 Nr. 3 StPO, § 74 I 1 Nr. 8 BKAG). Beschreiten sie den Rechtsweg, muss das Gericht aber auch in der Lage sein, die Maßnahme *en détail* nachzuvollziehen. Auch die Strafverteidigung braucht ausreichende Informationen über die Überwachungsmaßnahme, damit ein faires Verfahren möglich ist.[133] Genau aus diesem Grund etablieren die einfachgesetzlichen Regeln bereits eine Protokollpflicht (§ 100 a VI StPO, § 82 I, II Nr. 8 BKAG). Zu protokollieren ist u. a. das eingesetzte technische Mittel (§ 100 a VI 1 Nr. 1 StPO, § 82 I Nr. 1 BKAG). Das einfache Recht verlangt dafür keine detaillierte technische Beschreibung, sondern Angaben, die für ein Gericht oder einen Betroffenen allgemein verständlich sind.[134] Statt der erlangten Daten sind *nur Metadaten* zu protokollieren, die zuverlässige Rückschlüsse auf die erhobenen Daten ermöglichen (vgl. § 100 a VI Nr. 3 StPO, § 82 I Nr. 3 BKAG).[135] Eine vollständige technische Dokumentation, die etwa Softwarekonfigurationen einschließt, wäre in der Lage, die Überprüfbarkeit – jedenfalls für IT-Sachverständige – zu steigern.[136] Um Rechtssicherheit zu gewährleisten, sollten die Anforderungen an die Dokumentation künftig zumindest in einer Rechtsverordnung verankert sein.

Damit von dem Protokolliermechanismus eine möglichst geringe Manipulationsgefahr ausgeht, sollte er unmittelbar in der Software verankert sein.[137] Außerdem ist es denkbar, dass die Software die Protokollierung automatisiert auf einen anderen, sicheren Server ausleitet, auf den die ausführende Stelle selbst keinen Zugriff hat.[138] Selbst dann ist die Protokollierung technisch aber nicht vollständig überprüfbar und bietet daher allein keine hinreichende Gewähr dafür, unbefugte Veränderungen aufzudecken.[139] Dennoch ist sie – im Verbund mit anderen Maßnahmen – eine taugliche *zusätzliche* verfahrensrechtliche Absicherung.

b) *Nachträgliche öffentliche Kontrolle.* Um die Überwachungsmaßnahmen für die Öffentlichkeit transparent zu machen, schreibt das einfache Recht bereits heute eine ergänzende Statistik- und Berichtspflicht vor (§ 88 BKAG, § 101 b StPO). Auf ihr könnte der Gesetzgeber aufbauen, um die Kontrollmechanismen weiter zu verfeinern. Er sollte beispielsweise eine regelmäßige und für die Öffentlichkeit transparente – insbes. technische – Evaluierung der Quellen-TKÜ verankern.[140] Denn ob sich die Quellen-TKÜ in ihrem begrenztem Rahmen erfolgreich umsetzen lässt, ist an die technischen Voraussetzungen geknüpft, die wiederum einem steten Wandel unterworfen sind.

VI. Verpflichtung der Dienstanbieter als bessere Alternative?

Je klarer sich abzeichnet, wie grundrechtsdogmatisch anspruchsvoll und technisch schwierig es ist, den verfassungsrechtlichen Anforderungen an eine Quellen-TKÜ zu genügen, umso emsiger läuft die Suche nach Alternativen. Eine Option kann darin bestehen, die Messenger und IP-Telefondienstanbieter in die Pflicht zu nehmen: Der Gesetzgeber könnte sie zwingen, Zugangswege für Sicherheitsbehörden in ihre Kommunikationssoftware (etwa die Verschlüsselungs-Algorithmen) einzubauen.

Ganz neu ist der Ansatz in der rechtspolitischen Arena nicht. Die Diskussion darum entflammte bereits im Jahr 1996. Zu jener Zeit ließ sich die Idee, abseits der Übertragungsschnittstellen bei den herkömmlichen Telekommunikationsdienstanbietern an Kommunikationsdaten zu gelangen, noch vergleichsweise einfach in die Tat umsetzen: Anbieter, die verschlüsseln, sollten Hintertüren („Backdoors") vorsehen, die dem Staat direkten Zugriff auf den Klartext erlauben.[141] Im Jahr 2008 verbreiteten sich etwa Hinweise auf ein Schlupfloch, das *Skype* in sein System eingebaut hatte, um Sicherheitsbehörden die Überwachung zu ermöglichen.[142] Die Enthüllungen *Edward Snowdens* erhärteten den Verdacht: Zumindest ab dem Jahr 2012 soll *Microsoft* dem größten Auslandsgeheimdienst der USA, der *National Security Agency* (NSA), direkten Zugang zu *Skype*-Anrufen und Metadaten gewährt haben.[143] Daneben standen seinerzeit ein mögliches Verbot starker Verschlüsselungsverfahren, ein behördlicher Genehmigungsvorbehalt sowie eine Pflicht, private Schlüssel[144] zu hinterlegen, zur Debatte.[145]

Nachdem die erste Welle solcher Vorschläge abgeebbt war,[146] erlebte die Krypto-Debatte in den letzten Jahren gleichsam eine Springflut.[147] Sie erlangt auch deshalb besondere Aktualität, weil die wachsenden Verschlüsselungsmöglichkeiten, die der Mobilfunkstandard 5G bietet, den Sicherheitsbehörden in Zukunft sogar gänzlich den Weg versperren könnten, Telefongespräche auf herkömmliche Weise abzuhören:[148] Bei einer vollständigen Ende-zu-Ende-Verschlüsselung des mobilen Datenverkehrs haben die Kommunikationsvermittler keinen Zugriff auf den Schlüssel zu dem ausgetauschten Informationsschatz. Weder sie noch staatliche Behörden können ihn entschlüsseln, um ermittlungsrelevante Informationen zu dechiffrieren.

Der Idee, den Schlüssel mittels Überwachungssoftware auf dem Endgerät auszulesen,[149] steht aus technischer Hinsicht

133 Vgl. *BVerfGE* 150, 244 (303, Rn. 157); s. auch *Mysegades*, NZV 2020, 119 (126).
134 Für die alte Fassung der Befugnis im BKAG (§ 20 k, 27 BKAG a. F.): BT-Drs. 16/10121, 30.
135 Vgl. BT-Drs- 19/1434, 8. Dazu krit. *Singelnstein/Derin*, NJW 2017, 2646 (2647).
136 Die „standardisierende Leistungsbeschreibung" aus dem Jahr 2012 zählte zu den zu dokumentierenden Daten den Quellcode, den Prozess der Programmerzeugung aus diesem Quellcode und das Programm selbst, um den Funktionsumfang nachvollziehen zu können. Bundeskriminalamt (Fn. 123), 6 f.; BT-Drs. 18/12785, 53.
137 Das Protokollierungssystem ProSys ist Bestandteil der Software RCIS, BT-Drs. 19/1434, 8. Dies empfiehlt auch *Herpig*, A Framework for Government Hacking in Criminal Investigations, 20.
138 Zumindest sind bereits heute unterschiedliche Einheiten des BKA damit betraut, die Maßnahme durchzuführen und zu protokollieren, vgl. BT-Drs. 18/12785, 52. Zu einem Verfahren, um die Unveränderbarkeit des Protokolls herzustellen, *Neumann/Kurz et al.*, Stellungnahme im Ausschuss für Recht und Verbraucherschutz zu BT-Drs. 18/11272, 16.
139 Der Mechanismus ist manipulierbar: Ein technisches Verfahren, das die Aktivitäten authentifiziert protokolliert, setzt die exklusive Kontrolle über das System voraus. *Rehak*, Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, 38.
140 So auch eco Verband der Internetwirtschaft e. V., Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, 30.6.2020, 8.
141 Vgl. *Brunst*, DuD 2012, 333 (335).
142 *Sokolov*, Spekulationen um Backdoor in Skype, heise online vom 24.7. 2008.
143 *Hauck*, Wie Microsoft der NSA Zugang zu Outlook.com und Skype ermöglicht, Süddeutsche Zeitung Online vom 12.7.2018.
144 Anders als die symmetrische Verschlüsselung verwendet die asymmetrische Verschlüsselung ein Schlüsselpaar mit verschiedenen Schlüsseln: Der öffentliche Schlüssel steht zur Verschlüsselung von Nachrichten oder zur Authentifizierung von Nachrichten des Schlüsselinhabers öffentlich zur Verfügung, während der private Schlüssel dazu dient, eine Nachricht an den Schlüsselinhaber zu entschlüsseln oder eine Nachricht des Inhabers zu authentifizieren, und ausschließlich beim Empfänger verbleibt.
145 *Meyn*, Verschlüsselung und Innere Sicherheit, 2003, 1 f; *Neymanns*, Verschlüsselung im Internet, 2001, 129.
146 Vgl. BT-Drs. 19/1434, 4.
147 Vgl. dazu *Hornung*, MMR 2015, 145 (145).
148 Der Umfang der Ende-zu-Ende-Verschlüsselung in 5G-Netzen ist im Detail noch offen, BT-Drs. 19/10535, 15.
149 Diese Methode kommt der herkömmlichen Telekommunikationsüberwachung nahe. Sie garantiert, dass die Behörde nur laufende Kommunikation erfasst. Vgl. *Freiling/Safferling et al.*, JR 2018, 9 (18).

der Standard *Perfect Forward Secrecy (PFS)* entgegen, den einige Anbieter inzwischen standardmäßig in der Verschlüsselung verwenden.[150] Den für die jeweilige Verbindung („session") generierten Schlüssel kann ein Dritter auch nicht rückwirkend bei dem Sender oder Empfänger aus einem Protokollmitschnitt gewinnen.[151] Eine nachträgliche Entschlüsselung ist deshalb bereits technisch ausgeschlossen. Vielmehr müsste die Behörde den Schlüssel für jede Verbindung während des laufenden Kommunikationsvorgangs extrahieren, was in der Sache dem Eingriff einer Quellen-TKÜ gleichkäme.

Ein Lösungsvorschlag, der trotz Ende-zu-Ende-Verschlüsselung umsetzbar ist, stammt von zwei Mitarbeitern des britischen Geheimdienstes *GCHQ*: Der Kommunikationsdienstanbieter solle die Möglichkeit vorsehen, einen weiteren Teilnehmer heimlich in einen laufenden Kommunikationsvorgang zuzuschalten, ohne dass dies für die anderen Personen sichtbar ist.[152] Die Methode ähnelt „*Man-in-the-Middle*-Angriffen", bei denen der Angreifer vortäuscht, der Kommunikationspartner zu sein. Dagegen gibt es allerdings Schutzschilder. So sind beispielsweise Authentifizierungsmechanismen im Einsatz, welche die Sicherheitsnummer des Empfängers prüfen, um sich vor Angriffen zu schützen. Auf einem „Man-in-the-Middle-Angriffen" ähnlichen Konzept beruht auch die Idee, heimlich weitere Geräte (zB eine Desktopanwendung) im Namen des Nutzers hinzuzufügen.[153] Ermittlern des BKA soll es auf diese Weise beispielsweise gelungen sein, WhatsApp-Chats mitzulesen: Hatten sie kurzfristig Zugriff auf das Endgerät, konnten sie die Chats mit einer Whats-App-Browser-Version synchronisieren.[154]

Authentifizierungsprozesse zu unterbinden, schwächt jedoch die Sicherheitsarchitektur der Kommunikationsanwendung insgesamt und kann das Vertrauen der Nutzer untergraben. Dieses Dilemma zieht sich wie ein roter Faden durch die Verschlüsselungsdebatte: Wo auch immer die Anbieter Softwareveränderungen vornehmen, um Kommunikationsdaten an die Sicherheitsbehörden auszuleiten, beeinträchtigen sie die Datensicherheit *aller Nutzer* auch *gegenüber Dritten*, die eine solche Sicherheitslücke etwa für kriminelle oder Spionagezwecke nutzen können. Vorzugswürdig erscheint es deshalb, dass der Anbieter eine geschwächte Softwareversion nur dem Betroffenen – etwa über ein Update – zuspielt. Dadurch sinkt aber zugleich das Vertrauen in Softwareupdates, die für die IT-Sicherheit große Bedeutung haben.

Die US-Regierung versucht unterdessen, das soziale Netzwerk *Facebook* (ohne ein konkretes technisches Verfahren zu dekretieren) gerichtlich dazu zu bewegen, seine Software so zu verändern, dass es auf Anfrage Kommunikationsdaten herausgeben kann.[155] In eine ähnliche Richtung geht eine Vereinbarung der Five-Eyes-Staaten[156] vom August 2018: Sie fordern die Kommunikationsanbieter dazu auf, freiwillig Zugangswege für Sicherheitsbehörden zu etablieren, und kündigen anderenfalls Zwangsmaßnahmen an.[157] Australien ist insoweit noch einen Schritt weiter gegangen: In *Down Under* dürfen Behörden Anbieter seit Dezember 2018 zwingen, Funktionen einzuführen, die eine Kommunikationsüberwachung ermöglichen.[158] Ebenso fällt indischen Behörden unterdessen das Recht zu, die Anbieter zu verpflichten, an der Überwachung und Entschlüsselung der Kommunikationsinhalte mitzuwirken.[159] In Brasilien haben Behörden *WhatsApp* sogar kurzerhand gesperrt, als das Unternehmen sich weigerte, Kommunikationsdaten herauszugeben.[160] Auch die EU-Kommission erwägt in ihrer neuen Sicherheitsstrategie, Messenger dazu zu verpflichten, die Kommunikation ihrer Nutzer, auch wenn sie verschlüsselt ist, aktiv nach sexuellem Kindesmissbrauch zu durchsuchen und Funde zu melden.[161] Der Ministerrat möchte noch weitergehen: Als Reaktion auf die islamischen Terroranschläge in Nizza sowie Wien plant er ein Gesetzespaket, das Anbieter verpflichtet, den Zugriff auf verschlüsselte Kommunikation zu ermöglichen.[162]

Die Bundesregierung hat es bislang stets ausgeschlossen, Anbieter gesetzlich zu verpflichten, Schlüssel herauszugeben oder Hintertüren zu implementieren. Denn ihre Kryptopolitik verfolgt das erklärte Ziel, Verschlüsselungsmechanismen zu stärken, statt das Vertrauen der Nutzer in die IT-Sicherheit zu schwächen.[163] Gleichwohl hat das BMI zwischenzeitlich einen Gesetzesentwurf vorgelegt, der vorsieht, dass Messenger-Dienste auf richterliche Anordnung Kommunikationsinhalte unverschlüsselt an Behörden weiterleiten müssen.[164] Die Anbieter sollen ihre Software umgestalten, um den behördlichen Anfragen zu entsprechen. Damit der Betreiber selbst auf verschlüsselte Kommunikationsdaten im Klartext zurückgreifen kann, müsste er aber eine Schwachstelle in sein System implementieren. Die Softwareanbieter müssten dann offiziell verlauten lassen, sichere Verschlüsselungsverfahren zu verwenden, heimlich aber Softwareveränderungen vornehmen. Das schwächt nicht nur das Vertrauen der Nutzer, sondern öffnet auch Missbrauchstüren, die unbefugte *Dritte* ausnutzen könnten.[165] Es droht nicht zuletzt solche Anbieter vom Markt zu verdrängen, die aus technischen Gründen keine Schwachstellen einbauen können – entweder weil sie keinen zentralen Betreiber haben oder beispielsweise wie *Signal* quelloffen sind. Wieder sieht sich der Staat in einem Dilemma gefangen. Denn beide Softwaremerkmale – Open Source und verteilte Architektur – sollen die IT-Sicherheit verbürgen und sind daher grundsätzlich im Interesse des Gemeinwohls.[166]

150 Die Messenger *Signal, WhatsApp* und *Telegram* verwenden bspw. Perfect Forward Secrecy; s. *Schüler/Tonekaboni*, Es muss nicht immer WhatsApp sein: Sieben Messenger-Alternativen im Vergleich, heise online vom 10.5.2019.

151 *Fox*, DuD 2013, 729.

152 *Levy/Robinson*, Principles for a More Informed Exceptional Access Debate, Lawfareblog.com vom 29.11.2018. Damit der Nutzer dies nicht bemerkt, darf das Kommunikationsprogramm den Nutzer nicht benachrichtigen, wenn ein neuer Kommunikationspartner in den Chat eintritt.

153 Dies schlug der Präsident des BKA in jüngerer Zeit vor, *Krempl*, Crypto Wars: BKA-Chef will „Frontdoor-Debatte" führen, heise online vom 23.11.2019.

154 *Flade/Tanriverdi*, BKA kann bei WhatsApp mitlesen, tagesschau.de vom 21.7.2020.

155 *Beuth*, Facebooks Verschlüsselung vor Gericht, Spiegel Online vom 21.8.2018.

156 Im Five-Eyes-Bündnis kooperieren die Geheimdienste der USA, Großbritannien, Kanada, Australien und Neuseeland.

157 *Beuth*, „Five Eyes" fordern freiwillige Hintertüren, Spiegel Online vom 4.9.2018.

158 *Wälterlin*, „Big Brother in WhatsApp" – Australien öffnet Messenger für Geheimdienste, Handelsblatt online vom 6.12.2018.

159 *Reuter*, Indien gibt zehn Behörden Freifahrtschein für Überwachung und Entschlüsselung, netzpolitik.org vom 21.12.2018.

160 Gericht beendet WhatsApp-Sperre in Brasilien, Spiegel Online vom 20.7.2016.

161 KOM (2020) 607 final, 20.

162 Draft Council Resolution on Encrytion vom 6.11.2020 12143/1/20.

163 BT-Drs. 19/1434, 4; BT-Drs. 18/12785, 48.

164 *Diehl/Knobbe et al.*, Angriff auf Whats-App, Spiegel vom 25.5.2019.

165 Vor der Gefahr, die davon ausgeht, dass Dritte die Schwachstelle ausnutzen, warnt ein offener Brief von mehr als hundert Organisationen und Personen an das BMI v. 11.6.2019, https://docs.google.com/document/d/17F-OxKJtR8DM9O8jiEfUhxDGguBnJoZ2-lvp9614CyM/edit# (5.9.2019).

166 Darüber hinaus müsste der Gesetzgeber mögliche Folgewirkungen und Durchsetzbarkeitsprobleme in seine Folgenabschätzung mit aufnehmen: Er hat zu klären, wie sich die Missbrauchsgefahr der Schwachstelle durch die Anbieter selbst und ausländische Dienste auf ein Minimum reduzieren ließe und wie eine vollständige Sperrung ausländischer Dienste (etwa *WeChat*) effektiv und rechtskonform umsetzbar wäre.

Gegenüber dem Weg, die Kommunikationsanbieter zu verpflichten, ihr Sicherheitsversprechen zu brechen, ist im Ergebnis die Quellen-TKÜ vorzuziehen. Denn unterbindet oder schwächt der Staat global starke Verschlüsselungsmechanismen, gefährdet er die IT-Sicherheit strukturell – während die Quellen-TKÜ, wenn sie *im Einzelfall* in gesetzlich kontrolliertem Rahmen zur Anwendung kommt, immerhin „nur" die IT-Sicherheit einzelner Systeme oder Programme betrifft.[167]

Statt einer Alternative schlägt ein Entwurf des BMI, der die Quellen-TKÜ den Nachrichtendiensten erlauben soll, nunmehr einen neuen Weg vor, um das Endgerät mit der Überwachungssoftware zu infiltrieren: Telekommunikationsdienstanbieter sollen die Installation „durch Unterstützung bei der Umleitung von Telekommunikation […] ermöglichen".[168] Da der Datenverkehr dann über Computer der Nachrichtendienste geleitet wird, bevor er an den Adressaten geht, lässt sich die Überwachungssoftware, wenn der Datenverkehr unverschlüsselt ist,[169] unbemerkt einschleusen. Allerdings hat auch dieses Vorgehen einen Haken: Es droht ebenso generell das Vertrauen der Nutzer in die Integrität der Kommunikationsdaten zu unterminieren.

VII. Fazit

Die verschlüsselte Kommunikation via Smartphone ist längst zu einer wichtigen Zielscheibe polizeilicher Ermittlungstätigkeit avanciert. Aus der Perspektive der Ermittler ruft sie mit besonderer Schärfe die Frage nach der Waffengleichheit zwischen Straftätern und ihren Verfolgern in der digitalen Welt auf den Plan. Denn ermittlungstaktisch relevante Informationen via Quellen-TKÜ abzugreifen, ist ebenso grundrechtssensibel wie technisch und rechtlich herausfordernd: Wenn sich Verdachtspersonen der technischen Möglichkeiten der Ende-zu-Ende-Verschlüsselung bedienen, um E-Mails auszutauschen, per (Video-)Telefonie miteinander zu sprechen oder sich Nachrichten via Messenger zuzuschicken, kann eine Behörde die Kommunikationsinhalte grundsätzlich nur auf dem Endgerät des Nutzers im Klartext abfangen. Um unentdeckt zur Quelle der Ermittlungsweisheit zu gelangen, verbleibt der *physische Zugang* zum IT-Gerät nur ausnahmsweise als Weg der Wahl. Denn es ist mit erheblichem Aufwand und Risiken verbunden, das Endgerät einer Zielperson – etwa im Rahmen einer Kontrolle bei der Flugabfertigung – zu beschlagnahmen, um darauf heimlich eine Überwachungssoftware zu installieren.

Dass gängige Endgeräte, die verdächtige Personen zur Kommunikation verwenden, an das Internet angeschlossen sind, bietet ermittlungstaktisch dagegen geradezu ideale Voraussetzungen, um *versteckt aus der Ferne* auf das Endgerät zuzugreifen. Sicherheitslücken in der verwendeten Soft- und Hardware, von denen der Nutzer nichts ahnt, und Täuschungsmanöver (etwa durch einen „verseuchten" E-Mail-Anhang) öffnen IT-Fachleuten in der Regel als praktikable Instrumente das Tor zur privaten Kommunikationswelt des Einzelnen. Sie auszunutzen, versetzt den Staat allerdings in ein grundrechtliches und ethisches Dilemma. Denn sein Interesse daran, Sicherheitslücken aufrechtzuerhalten, um die Endgeräte einer Zielperson infiltrieren zu können, läuft seiner Verpflichtung, die Bürger vor IT-Sicherheitsrisiken zu schützen, diametral zuwider. Sollen die Vorschriften zur Quellen-TKÜ verfassungsgemäß sein, sind daher gesetzliche Rahmenbedingungen erforderlich, die begrenzen, in welchem Umfang der Staat Sicherheitslücken ausnutzen darf.

Auf verfassungsrechtlicher Ebene hat das *BVerfG* eine klare Grenzlinie gezogen: Die Quellen-TKÜ darf nur laufende Kommunikationsvorgänge erfassen. Was dies für die Überwachung von Messengern wie *Signal* oder *WhatsApp* bedeutet, wenn sie die Kommunikationsdaten über den technischen Übertragungsvorgang hinaus verschlüsseln, ist jedoch weniger klar.

Um die verfassungsrechtliche Trennlinie zwischen dem Fernmeldegeheimnis und dem IT-Grundrecht zu wahren, sollte „laufende Kommunikation" sich nicht auf den Übertragungs-, sondern auf den vor- oder nachgelagerten Ver- oder Entschlüsselungsvorgang beziehen. Denn die sichere Ende-zu-Ende-Verschlüsselung beendet die übermittlungstypische Gefährdungslage, auf die sich der Schutz des Fernmeldegeheimnisses erstreckt. „Laufend" ist die Kommunikation daher noch im ersten bzw. letztmöglichen Moment, in dem unverschlüsselte Daten vorliegen.

Die Ermächtigung des Gesetzgebers, den Ermittlungsbehörden in § 100 a I 3 StPO zu erlauben, auf *gespeicherte* Kommunikationsvorgänge zuzugreifen, die Gegenstand eines Übertragungsvorgangs waren, um verschlüsselte Messenger-Kommunikation abgreifen zu können, steht mit dem GG nicht im Einklang. Sie lässt sich auch nicht verfassungskonform auslegen. Denn der historische Gesetzgeber wollte bewusst den Zugriff auf archivierte Kommunikationsdaten gestatten, die zwischen Anordnungszeitpunkt und Inbetriebnahme der Überwachungssoftware erfolgte (§ 100 a V 1 Nr. 1 lit. b StPO).

Selbst wenn die Quellen-TKÜ in ihrem normativen Anspruch archivierte Inhalte aus ihrem Zulässigkeitsradius ausgrenzt, bannt sie noch nicht hinreichend sicher die Gefahr, dass der Staat mehr als nur die laufenden Kommunikationsvorgänge ausliest. Die Kontrollmechanismen müssen das Restrisiko, dass eine Behörde auch auf vergangene Kommunikation oder private Bilder auf dem Speichermedium (und damit in der ausschließlichen Herrschaftssphäre des Grundrechtsträgers) zugreifen kann, in verfassungsrechtlich verantwortbare Bahnen lenken. Dem parlamentarischen Gesetzgeber kommt die Aufgabe und verfassungsrechtliche Pflicht zu, die Leitplanken für eine verhältnismäßige Befugnis zur Quellen-TKÜ rechtssicher und nachvollziehbar abzustecken. Bereits die gesetzliche Ermächtigungsnorm muss vorzeichnen, wie eine Quellen-TKÜ technisch umzusetzen ist[170] – etwa technische Funktionalitäten umreißen, die geeignet sind, um ausschließlich laufende Kommunikation zu überwachen.[171] Aus den verfügbaren technischen Möglichkeiten sollte die Behörde zudem stets diejenige Methode auswählen müssen, die ausreichend zuverlässig gewährleistet, dass sie lediglich die laufenden Kommunikationsvorgänge überwacht. In den Ermächtigungsnormen des BKAG und der StPO fehlen aber bislang hinreichende normative Rahmenbedingungen dafür, wie die Quellen-TKÜ konkret technisch und organisatorisch umzusetzen ist.

Ausdrücklich untersagt sein sollte den Behörden, Screenshots und Keylogger zu nutzen. Daneben sollten umfassende verfahrensrechtliche Vorkehrungen treten,[172] die nachprüfbar sicherstellen, dass die Konfiguration der Software den recht-

167 Vgl. *Geminn*, DuD 2015, 546 (547).
168 Bundesministerium des Innern, für Bau und Heimat, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, § 2 I a Nr. 4 Artikel 10-Gesetz (20.10.2020).
169 Ist der Datenverkehr dagegen verschlüsselt, sind die Behörden wiederum darauf angewiesen, Sicherheitslücken auszunutzen; *Brunsmann*, Internetprovider sollen Geheimdiensten künftig Daten zuspielen, dw.com vom 14.7.2020. S. dazu I. 1. b).
170 S. III. 3.
171 S. IV. 2.
172 S. V.

lichen Vorgaben tatsächlich entspricht. Die einzelnen Bestandteile der Überwachungssoftware sollten insbesondere vorab ein gesetzlich vorgesehenes Prüfungsverfahren durchlaufen müssen. Darüber hinaus sollte auch der konkrete Überwachungsprozess Kontrollmechanismen unterliegen – etwa einer Funktionstrennung zwischen ausführender und konfigurierender Stelle. Um eine effektive nachträgliche Kontrolle, insbesondere durch Gerichte, zu ermöglichen, sollte der Gesetzgeber die Programmabläufe einer Protokollierungspflicht auf getrennten Servern unterwerfen. Nicht zuletzt sollte er bereits vorhandene Erfahrungen und *Best Practices* der Ermittlungsbehörden, die sicherstellen, dass die Quellen-TKÜ tatsächlich auf die Überwachung laufender Kommunikation beschränkt ist, in einen konkreten Ausgestaltungsrahmen einbinden.

Der Gesetzgeber ist gut beraten, die vielen offenen rechtlichen, organisatorischen und technischen Fragen einer rechtssicheren Antwort zuzuführen, bevor er seinen – gegenwärtig gehegten – Plan realisiert, die Befugnis zur Quellen-TKÜ auf die Nachrichtendienste auszuweiten.[173] Denn anderenfalls erschließt sich das Handlungsinstrumentarium eine neue Dimension: Während die Befugnisse des BKA und der StPO unter Richtervorbehalt stehen (§ 51 III BKAG, § 100 e I StPO), operieren die Nachrichtendienste grundsätzlich im Geheimen.[174] Die diskutierten verfahrensrechtlichen Kontrollmechanismen wirken bei ihnen daher nur begrenzt.

So bleibt es im Ergebnis ein höchst anspruchsvolles Unterfangen, die Quellen-TKÜ verfassungskonform umzusetzen. Bislang erfreut sie sich in der Vollzugspraxis noch keiner großen Beliebtheit – nicht zuletzt aufgrund der erheblichen technischen Umsetzungshürden, insbesondere dem hohen Aufwand beim Aufspüren einer Sicherheitslücke und der heimlichen Infiltration des konkreten Endgeräts.[175] Das macht die Quellen-TKÜ zwar noch nicht zu einem Ermittlungs-Placebo. Sie bestätigt aber die alte Erkenntnis *Leonardo da Vincis*: „Die meisten Probleme entstehen bei ihrer Lösung."

173 Bundesministerium des Innern, für Bau und Heimat, Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, § 11 I a Artikel 10-Gesetz (20.10.2020).

174 Nur das Parlamentarische Kontrollgremium (PKG) und die G-10-Kommission (nicht aber die ordentliche Gerichtsbarkeit) kontrollieren de lege lata Befugnisse nach §§ 14, 15 G 10.

175 Vgl. etwa *Flade*, Der Bundestrojaner, den keiner nutzt, tagesschau.de vom 25.10.2019; s. auch *Bär*, 28. Kapitel – EDV-Beweissicherung in *Wabnitz/Janovsky/Schmitt*, Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 28, Rn. 92 b.