GEWERKSCHAFT
DER JOURNALISTINNEN
UND JOURNALISTEN
DEUTSCHER
JOURNALISTEN-
VERBAND

TORSTR. 49
10119 BERLIN
TELEFON 030-726279 20
TELEFAX 030-726279213
E-MAIL: DJV@DJV.DE
INTERNET: WWW.DJV.DE

27. Juli 2023

Stellungnahme
des Deutschen Journalisten-Verbandes e.V.
zur Verfassungsbeschwerde Az. 1 BvR 180/23

A. Einleitung

Der Deutsche Journalisten-Verband (DJV) bedankt sich dafür, im Rahmen des Verfahrens 1 BvR 180/23 Stellung nehmen zu können.

Der DJV schließt sich den Ausführungen der Beschwerdeführer hinsichtlich der Verletzung des Rechts auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 iVm Art. 1 Abs.1 GG an. Wir möchten ergänzend auf einen Aspekt hinweisen, der 2018 noch nicht relevant war: Daten können durch generative KI ausgewertet werden. Fotos, Videos und Aufnahmen der menschlichen Stimme können verfälscht werden. Jeder Mensch mit Internetzugang kann künstliche Intelligenz nutzen. Persönlichkeitsprofile über die intimsten Details eines Menschen können so auf eine Art genutzt werden, die 2018 noch nicht möglich war.
Darüber hinaus verletzen die angeführten Vorschriften zur Quellen-TKÜ und zur kleinen Online-Durchsuchung gemäß § 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO die Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG.

Diese Stellungnahme behandelt zunächst § 100a Abs. 1 Satz 3, Abs. 3 StPO (kleine Online-Durchsuchung), anschließend § 100a Abs. 1 Satz 2, Abs. 3 StPO (Quellen-TKÜ). Im Rahmen der kleinen Online-Durchsuchung wird im Hinblick auf Art. 5 Abs. 1 Satz 2 GG dargestellt, wie intensiv diese Eingriffsmaßnahmen im Redaktionsalltag wirken.

Anschließend wird im Rahmen der Angemessenheit dargestellt, warum der bisherige Mindestschutz der StPO für Journalist:innen bezüglich dieser Maßnahmen nicht mehr besteht. Dann wird auf die objektive Dimension von Art. 5 Abs. 1 Satz 2 GG eingegangen und schließlich auf die Rechtsprechung des EGMR zum Quellenschutz.

B. Verfassungswidrigkeit von § 100a Abs. 1 Satz 3, Abs. 3 StPO

Die Regelungen zur kleinen Online-Durchsuchung verletzen die Pressefreiheit gemäß Art. 5 Abs. 1 Satz 2 GG. Nach der Rechtsprechung des BVerfG umfasst die in Art. 5 Abs. 1 Satz 2 GG verbürgte Pressefreiheit die Eigenständigkeit der Presse von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen.[1] Darunter fällt die Vertraulichkeit der Redaktionsarbeit, wozu insbesondere der Informantenschutz und das Redaktionsgeheimnis zählen. Das Redaktionsgeheimnis wiederum umfasst unter anderem die Kommunikation zwischen Redakteur:innen und organisationsbezogene Unterlagen, aus denen sich redaktionelle Arbeitsabläufe oder die Identität der Mitarbeiter einer Redaktion ergeben.

I. Eingriffsintensität im Hinblick auf Art. 5 Abs. 1 Satz 2 GG

Der Beschwerdeführer zu 1. ist Journalist. Der Beschwerdeführer zu 5. ist Publizist und arbeitet somit journalistisch. Der persönliche Schutzbereich von Art. 5 Abs. 1 Satz 2 GG ist für beide eröffnet.

1. Redaktionsgeheimnis

Die Vertraulichkeit der Redaktionsarbeit umfasst die gesamte Kommunikation in einer Redaktion. Staatlichen Stellen ist es grundsätzlich verwehrt, sich Einblick in die Vorgänge zu verschaffen, die zur Entstehung von Nachrichten oder Beiträgen führen. Die von der Verfassungsbeschwerde angegriffenen Regelungen zur Online-Durchsuchung, zur kleinen Online-Durchsuchung und zur Quellen-TKÜ haben auf diese Vorgänge tiefgreifende Auswirkungen. Insbesondere die kleine Online-Durchsuchung gemäß § 100a Abs. 1 Satz 3, Abs. 3 StPO ermöglicht es, gespeicherte Kommunikationsinhalte und -umstände zu überwachen und aufzuzeichnen. Um die Eingriffsintensität nachvollziehbar darzustellen, wird zunächst kurz die journalistische

[1] Vgl. BVerfGE 10, 118 (121) – Berufsverbot I; 66, 116 (133) – Springer/Wallraff; 77, 65 (74) – Beschlagnahme von Filmmaterial.

Arbeitsweise beschrieben.

IT-Equipment und -Systeme wie Smartphones, Computer, Laptops, digitale Tonträger, USB-Sticks etc. sind zentrale journalistische Arbeitswerkzeuge. Die journalistische Berufsgruppe ist auf diese Werkzeuge angewiesen. Andere kommunikationsbezogene analoge Werkzeuge, z. B. Papier und Stift, sind hier zu vernachlässigen, sie spielen im journalistischen Arbeitsalltag keine erhebliche Rolle mehr. Sie werden kaum noch benötigt. Das gilt auch für andere Kommunikationsmittel: Der öffentlich-rechtliche Rundfunk beispielsweise schafft zurzeit herkömmliche Telefontechnik mitsamt der Telefonanlagen ab. Telefone werden dort durch IP-Telefonie ersetzt, das heißt, der Journalist kommuniziert über das Head-Set und benötigt keinen Telefonhörer und kein klassisches Telefonnetz mehr; seine Kommunikationsinhalte werden über ein internetgestütztes Datennetz übertragen.

Die journalistische Arbeitsweise zeichnet sich dadurch aus, dass Texte, Videos, Podcasts, Filme nicht mit einem Klick fertig sind. Journalistische Themen werden recherchiert. Jedes journalistische Produkt wird i.d.R. mehrfach überarbeitet. Recherche umfasst die Themenfindung, Materialsammlung und das Überprüfen von Informationen. Journalist:innen kommunizieren zu diesem Zweck mit anderen Menschen über die jeweiligen Themen, sie rufen z.B. bei Personen des öffentlichen Lebens an, um mit deren Originaltönen einen Beitrag anschaulich zu ergänzen, sie tauschen Emails mit Wissenschaftler:innen aus, um Behauptungen zu verifizieren, sie kommunizieren in sozialen Netzwerken mit Privatpersonen, um etwa herauszufinden, welche Themen für eine große Anzahl von Menschen relevant sind. Sie müssen Aussagen zusammenfassen, Fragen vorformulieren, Gespräche moderieren und Material wiederum anderen Personen zur Verfügung stellen, um deren Stellungnahmen oder widersprechende Informationen und Meinungen zu erhalten. Sie kommunizieren permanent miteinander.
Um hochwertiges, authentisches Material zu erhalten, müssen Journalist:innen mobil sein. Sie sind auf mobile IT-Systeme, wie das Smartphone, den Laptop oder digitale Aufnahme- und Speichergeräte angewiesen. Diese IT-Systeme enthalten alle journalistisch relevanten Programme, einen Internetbrowser für die Recherche, ein Schreibprogramm, Programme für die Bild- und Videobearbeitung, die Podcast-Erstellung, für die Aufzeichnung von O-Tönen, Programme für das Transkribieren von Aufzeichnungen, Übersetzungstools und Apps für die Organisationsstruktur der Recherche, für die Reiseorganisation, für den Datenaustausch, Programme für die

interne Organisation des IT-Systems, die unterschiedliche Programmabläufe miteinander verknüpfen und schließlich Apps für Email-Kommunikation, Videokommunikation und für die Kommunikation in sozialen oder redaktionsinternen Netzwerken.

All diese Programme sind oftmals mit dem Internet verbunden. Viele davon setzen Online-Profile voraus. Die kleine Online-Durchsuchung kann in die Funktion dieser Programme eingreifen und jeden Inhalt überwachen und aufzeichnen. Die Verfassungsbeschwerde führt auf Seite 70 f. zutreffend aus, dass der Telekommunikationsbegriff durch das BVerfG weit ausgelegt wird und unter anderem sogar das Surfen auf einer Website als willensgesteuerten Zugriff auf konkrete Kommunikationsinhalte erfasst.[2] Jeder Inhalt aus diesen Programmen kann insofern Teil eines Telekommunikationsvorgangs sein, da er in einer Cloud gespeichert werden kann und Journalist:innen, die in Rechercheverbünden vernetzt sind, regelmäßig auf gemeinsame Cloud-Systeme zugreifen.
Anfällig für Überwachungsmaßnahmen der dargestellten Art sind die genannten Werkzeuge vor allem auch, weil sie immer präsent sind. Journalist:innen führen sie permanent mit sich, weil etwa ein Smartphone in jede Hosentasche passt. Redaktionsarbeit findet auch innerhalb der Medienhäuser in einem erheblichen und nicht wegzudenkenden Umfang digital statt. Wenn ein Journalist ein Stockwerk über einem anderen arbeitet, kommunizieren sie z.B. über Video-Telefonie, über E-Mails, Social-Media-Kanäle etc. Auch die analoge Redaktionsarbeit, etwa das gemeinsame Bearbeiten eines Textes oder der gemeinsame Austausch von Ideen und Rechercheergebnissen in einem Raum kann darüber hinaus überwacht werden, da jede Person im Raum regelmäßig ein Smartphone bei sich trägt.
So kann der Stand einer Recherche abgefragt werden, bevor die Journalistin entscheidet, dass sie einen Artikel veröffentlicht. Sämtliche Kontaktdaten und damit Informationen über Informanten, Standortdaten und Bewegungsprofile, Inhalte von Gesprächen, Terminplanung, Kontakte zu anderen Journalisten und Redaktionen, bis hin zu Manuskripten mit genauen Formulierungen können aufgezeichnet werden. Möglich ist, aufzuzeichnen, mit wem eine Journalistin wo und wann über was gesprochen hat. Möglich ist, ein Persönlichkeitsprofil der Journalistin zu erstellen, um eine Recherche zu beeinflussen und das Verhalten der Journalistin vorherzusagen und zu manipulieren.

[2] Vgl. BVerfG NJW 2016, 3508, 3511 – Beschluss vom 06.07.2016 – 2 BvR 1454/1.

2. Kein ausreichender Informantenschutz

Eine Maßnahme gemäß § 100a Abs. 1 Satz 3, Abs. 3 StPO führt dazu, dass in dem Bereich der jeweiligen Straftatenkataloge kein ausreichender Informantenschutz mehr besteht.

Zunächst werden die Besonderheiten der investigativen Recherche beschrieben, um die Auswirkungen auf den Quellenschutz nachvollziehbarer zu machen.
Am Anfang einer investigativen Recherche sind viele Elemente des Sachverhaltes nicht bekannt. Die Redaktion muss daher den Zeitpunkt, mögliche Tatorte, involvierte Personen und das Ausmaß der Vorwürfe ermitteln. Erst mehrere Quellen geben die für eine Veröffentlichung nötige Gewissheit. Um bestimmte Recherchehypothesen zu prüfen, müssen diese in der Redaktion außerdem diskutiert werden, dabei müssen auch spontane, ins Unreine gesprochene und verfehlte, gleichwohl die Diskussion fördernde Äußerungen möglich sein.[3]
Angenommen, eine investigativ arbeitende Journalistin hat die Aufgabe, herauszufinden, ob strafrechtlich relevante Vorwürfe zutreffen. Sie kennt den Namen einer Person, die möglicherweise mehr über diese Vorgänge weiß. Die Journalistin kann nun über verschiedene Wege Informationen beschaffen. Sie kann der Person einen Brief schreiben. Sie kann mit dem möglichen Informanten telefonieren. Ihn persönlich treffen. Oder ihm eine Mail oder eine Nachricht in einem sozialen Netzwerk schreiben. Angenommen, sie schreibt einen Brief, um herauszufinden, ob er über mehr Informationen verfügt. Dieser Brief wird in der redaktionsinternen Dokumentenablage abgelegt. Falls die Polizei gegen den Informanten ermittelt: Den Brief in der Dokumentenablage kann sie wegen § 97 Abs. 5 Satz 1 StPO grundsätzlich nicht beschlagnahmen.
Die Journalistin kann den Informanten auch persönlich treffen und ihm in einem unmittelbaren Gespräch Fragen stellen. Kommt es später zu einem Ermittlungsverfahren, in dessen Rahmen die Journalistin als Zeugin vernommen wird, kann sie sich bezüglich seiner Identität und weiterer berufsbezogener Wahrnehmungen – grundsätzlich – auf ihr Zeugnisverweigerungsrecht gemäß § 53 Abs. 1 Satz 1 Nr. 5 StPO berufen. In beiden Fällen ist der Quellenschutz insoweit zumindest gewährleistet.
Hat sich die Journalistin dagegen dazu entschieden, dem Informanten eine Nachricht in einem (verschlüsselten) Messenger-Dienst zu schicken, kann im Rahmen der

[3] BVerfGE 66, 116 (134/135) = NJW 1984, 1741, 1742.

kleinen Online-Durchsuchung diese gespeicherte Nachricht ausgelesen werden. Wenn sie die Nachricht allerdings nur in einem Brief auf ihrer Dokumentenablage hinterlegt hat oder in einem USB-Stick abgespeichert hat, wäre nur eine offene Beschlagnahme in den Grenzen des § 97 Abs. 5 Satz 1 StPO möglich.
Recherchiert eine Journalistin zu besonders strafrechtssensiblen Themen, wie Extremismus, Waffenhandel, Korruption und Terrorismus, wird sie auch das Gespräch mit den handelnden Personen suchen, um das journalistische Produkt mit deren Ansichten ausgewogener, authentischer, mit Videos oder Fotos anschaulicher zu gestalten. Möglich ist, dass sie dafür auch bereits verurteilte Straftäter im Gefängnis besucht. Dies kann für deutsche Behörden Anlass genug für eine Überwachung sein. Beispielsweise hatte die Taz-Journalistin Marily Stroux gemeinsam mit dem Journalisten Roger Willemsen RAF-Mitglieder im Gefängnis besucht und ihnen nach dem Fototermin das Foto geschickt.[4] Dies war für den Hamburger Verfassungsschutz laut Akteneintrag Grund genug, davon auszugehen, dass sie „Briefkontakt mit terroristischen Gewalttätern unterhält." Sie wurde insgesamt 32 Jahre beobachtet.[5] Die Journalistin Andrea Röpke, die unter anderem für das ARD-Magazin Panorama arbeitete und als Sachverständige im NSU-Untersuchungsausschuss geladen war, wurde vom niedersächsischen Verfassungsschutz jahrelang beobachtet, wobei ihr insbesondere die Anwesenheit auf rechtsextremen Trauermärschen und Kinderlagern angelastet wurde.[6]
Auch aus Sicht von Ermittlungsbehörden stellt der digitale Kontakt zwischen Journalist:innen und Beschuldigten eine Informationsquelle dar. Dies zeigt beispielsweise der Fall des bayerischen Landeskriminalamts, das die Pressestelle der „Letzten Generation" überwacht hatte und so zahlreiche Anfragen von Journalist:innen per E-Mail oder Telefon ohne weiteren Erkenntnisgewinn aufzeichnete.[7]
In dieser für investigative Journalist:innen typischen Situation befindet sich insbesondere der Beschwerdeführer zu 1., der, wie in der Verfassungsbeschwerde auf Seite 26 beschrieben, von 1970 bis 2008 vom Verfassungsschutz – rechtswidrig – beobachtet wurde. Er kommt außerdem aufgrund seiner investigativen Recherchen mit Straftatverdächtigen in Kontakt und ebenso aufgrund seiner Arbeit für die Internationale Liga für Menschenrechte e. V. (1959 gegründet), in dessen Rahmen er häufig mit Gruppen und Personen Kontakt hat, die von Polizei oder Geheimdiensten im In- und Ausland verfolgt oder überwacht werden.

[4] https://taz.de/taz-Fotografin-ausgespaeht/!5337129/
[5] https://taz.de/Verfassungsschutz-muss-Daten-loeschen/!5705423/
[6] https://taz.de/Ueberwachte-Journalistin-wehrt-sich/!5049614/
[7] https://www.bjv.de/news/bjv-fordert-aufarbeitung-abhoeraktion-gegen-pressetelefon-letzen-generation; vgl. auch unten D. zu Überwachungsmaßnahmen in anderen Ländern.

Insofern besteht bereits im Vorfeld, also bevor es überhaupt ein Ermittlungsverfahren gibt, die Gefahr, dass Informanten davor zurückschrecken könnten, investigative Journalist:innen, wie den Beschwerdeführer zu 1., zu kontaktieren (chilling effect).

II. Zur Unverhältnismäßigkeit der Maßnahme nach § 100a Abs. 1 Satz 3, Abs. 3 StPO („kleine Online-Durchsuchung“)

1. Erforderlichkeit

Die Überwachung der von Journalist:innen eingesetzten IT-Systeme ist nicht erforderlich, weil den Ermittlungsbehörden mildere Ermittlungsmaßnahmen zur Verfügung stehen.

Der Grund für die strafprozessuale Ausweitung der heimlichen Überwachung liegt laut BT-Drucksache (18/12785, S. 48 f.)[8] darin, dass ein Großteil der Kommunikation inzwischen über VoIP- und Messenger-Dienste, die diese Kommunikationsinhalte verschlüsseln, erfolgt. Die Entschlüsselung sei wiederum nicht möglich oder zeit- und kostenintensiv. Ohne Telekommunikationsüberwachung oder Ausleitung der Inhalte vor der Verschlüsselung sei insofern eine effektive Strafverfolgung im Bereich der Katalogstraftaten nicht mehr gewährleistet.

Die Polizeibehörden können vor diesem Hintergrund mildere Ermittlungsmaßnahmen wählen, die weniger intensiv in die Pressefreiheit journalistischer Nachrichtenmittler eingreifen. Eine gegenüber der Anwendung der genannten heimlichen Ermittlungsinstrumente mildere Maßnahme wäre z.B. die Beschlagnahme des jeweiligen Kommunikationsinhaltes gemäß § 94 Abs. 1 StPO, denn auch digital gespeicherte Informationen gehören nach der Rechtsprechung des BVerfG zum strafprozessualen Gegenstandsbegriff.[9] Die Beschlagnahmemöglichkeit wird allerdings und aus guten Gründen durch §§ 53 Abs. 1 Satz 2, 97 Abs. 5 Satz 1 StPO begrenzt und umfasst insbesondere keine berufsbezogenen Aufzeichnungen. Wenn jedoch das Ermittlungsverfahren ein Verbrechen betrifft, enthält § 53 Abs. 2 Satz 2 Var. 1 StPO wiederum eine Ausnahme, die die Beschlagnahme auch eines berufsbezogenen Inhaltes ermöglicht. Betrifft das Ermittlungsverfahren ein Verbrechen, können

[8] https://dserver.bundestag.de/btd/18/127/1812785.pdf
[9] Meyer-Goßner/Köhler, StPO, § 94, Rn. 4.

Journalist:innen auch während einer Vernehmung die Aussage über berufsbezogene Wahrnehmungen nicht verweigern, § 53 Abs. 2 Satz 2 Var. 1 StPO.

Ebenso ist im Bereich der Vergehen (§§ 80a, 85, 87, 88, 95 auch i. V. m. §§ 97b, 97a, 98 bis 100a StGB sowie §§ 174 bis 176, 177 Abs. 2 Nr. 1 StGB, § 261 Abs. 1 bis 4 StGB) eine Vernehmung der Journalist:innen über berufsbezogene Wahrnehmungen gemäß § 53 Abs. 2 Satz 2 Var. 2 Nr. 1 bis 3 StPO möglich; genauso eine Beschlagnahme des insoweit relevanten berufsbezogenen Inhalts gemäß §§ 53 Abs. 2 Satz 2, 97 Abs. 5 StPO.

Diese offenen Maßnahmen sind milder, weil Journalist:innen diese sofort gerichtlich überprüfen lassen können. Verdeckte Maßnahmen können nicht sofort überprüft werden, weil der Nachrichtenmittler erst nach Abschluss der Maßnahme über sie informiert wird.[10] Außerdem können offene Maßnahmen medial begleitet werden, was bei verdeckten Maßnahmen nicht der Fall ist, da letztere bereits abgeschlossen sind.

2. Angemessenheit

Zunächst wird im Rahmen der Angemessenheit unter a) dargestellt, dass aus DJV-Sicht das bisherige strafprozessuale Schutzniveau für Journalist:innen bei Maßnahmen gemäß §§ 100a Abs. 1 Satz 3, Abs. 3, 160a StPO den verfassungsrechtlichen Anforderungen nicht entspricht und dem Schutzniveau von Maßnahmen gemäß §§ 94, 97 Abs. 5 StPO entsprechen sollte. Anschließend wird unter b) dargestellt, dass § 100a Abs. 1 Satz 3, Abs. 3 StPO selbst den Anforderungen nicht entspricht, die das BVerfG im BND-Urteil aus dem Jahr 2020 zur qualifizierten Eingriffsschwelle entwickelt hat.[11]

a) Kein ausreichender Mindestschutz aus Art. 5 Abs. 1 Satz 2 GG

Ausgangspunkt der verfassungsrechtlichen Bewertung durch den DJV ist die Entscheidung des BVerfG zu journalistischen Verbindungsdaten vom 12. März 2003.[12] Gegenstand dieser Entscheidung waren gerichtlich angeordnete

[10] Vgl. auch BVerfGE 124, 43 (65/66) – Beschlagnahme von E-Mails = NJW 2009, 2431, 2435.
[11] BVerfGE 154, 152ff – BND - Ausland-Ausland-Fernmeldeaufklärung = BVerfG NJW 2020, 2235.
[12] BVerfGE 107, 299ff – journalistische Verbindungsdaten.

Auskunftserteilungen eines Mobilfunkbetreibers über Verbindungsdaten zu Telefongesprächen, die im Rahmen journalistischer Tätigkeit geführt wurden. Das BVerfG kam damals zu dem Ergebnis, dass Art. 5 Abs. 1 Satz 2 GG nicht verletzt wurde. Abzuwägen habe der Gesetzgeber das staatliche Interesse an der Strafverfolgung und das Berichterstattungsinteresse der Medien und den damit verbundenen Informantenschutz, wobei es bei beiden Abwägungsgütern um Informationsbeschaffung gehe und keinem Abwägungsgut ein absoluter Vorrang zukomme. Das BVerfG weist darauf hin, dass der Gesetzgeber dementsprechend Sonderregelungen geschaffen habe, u.a. das Zeugnisverweigerungsrecht und das Beschlagnahmeverbot gemäß § 97 Abs. 5 Satz 1 StPO. Es betont in ständiger Rechtsprechung, dass diese Ausnahmeregelungen für Journalist:innen nicht abschließend sind. In der genannten Entscheidung aus dem Jahr 2003 formulierte es folgenden Vorbehalt:

> *Die Normen sind nach ständiger Rechtsprechung des Bundesverfassungsgerichts allerdings nicht notwendig abschließende Regelungen (vgl. BVerfGE 64, 108 [116]; 77, 65 [81 f.]). Für zusätzliche Vorkehrungen besteht dann kein Anlass, wenn dem durch Art.5 Abs.1 GG gebotenen Mindestschutz schon durch die allgemeinen Vorschriften ausreichend Rechnung getragen wird. Die hinreichende Berücksichtigung publizistischer Belange lässt sich nicht allein daran bemessen, ob es Sonderregeln für Medien gibt.*[13]

Wie in der aktuellen Verfassungsbeschwerde richtig dargelegt wurde, hat sich das Kommunikationsverhalten der Menschen durch eine technische Entwicklung vollkommen verändert. Speziell der journalistische Beruf hat sich der Digitalisierung vollständig angepasst. Für Journalist:innen, die mit Beschuldigten aus den genannten Straftatenkatalogen, insbesondere im Vergehensbereich, kommunizieren, besteht mithin das gegenüber analogen Vorgängen deutlich erhöhte Risiko, dass ihre gesamten journalistischen Telekommunikationsvorgänge, jeder Kontakt und jeder Stand der Recherche, sei es die Endfassung oder nur der erste Entwurf, aufgezeichnet werden kann. Das umfasst sogar Inhalte, die nicht veröffentlicht werden. Ebenso ist der Informantenschutz nicht mehr gewährleistet, obwohl selbst bei einer offenen Beschlagnahme im Verbrechensbereich Dokumente, die den Namen des Informanten oder Kontaktumstände zu diesem offenlegen, gemäß §§ 97 Abs. 5 Satz 1, 53 Abs. 2 Satz 3 StPO nicht beschlagnahmt werden können. Somit sind grundlegende

[13] BVerfGE 107, 299 (334) = NJW 2003, 1787, 1794.

Arbeitsvoraussetzungen des journalistischen Berufes nicht mehr gewährleistet.

In der damaligen Entscheidung betonte das BVerfG, dass die bisherigen Regelungen dem gebotenen Mindestschutz ausreichend Rechnung getragen haben. Zu den bisherigen Regelungen zählte § 97 Abs. 5 StPO, also eine Ausnahmeregelung für die offene Beschlagnahme von Gegenständen. Der § 97 Abs. 5 Satz 1 StPO begrenzt das Schutzniveau insofern auf Informationen, die durch die Betrachtung beschlagnahmter Gegenstände erlangt werden können. Ausgangspunkt der Bewertung, ob der Mindestschutz des Art. 5 Abs. 1 Satz 2 GG eingehalten ist, ist jedoch die Bewertung des Gewahrsamsmoments des § 97 Abs. 5 Satz 1 StPO:

> *Hiernach misst der Gesetzgeber dem Gewahrsamsmoment eine wichtige Bedeutung als Faktor der Schutzbedürftigkeit bei. Dieses aber fehlt im Hinblick auf die hier zu beurteilende Auskunft, da sich die Verbindungsdaten bei den Telekommunikationsdiensteanbietern und damit bei einem Dritten befinden. Der Informantenschutz ist auch bei der Recherche im Zusammenhang mit schweren Straftaten jedenfalls insoweit gewährleistet, als eine aktive Mitwirkung des Journalisten an der Aufdeckung der Identität eines Informanten von Strafverfolgungsbehörden nicht erzwungen wird. Auch Informantenunterlagen sind insoweit geschützt, als sie sich in der Herrschaftssphäre des Journalisten befinden. Hierauf kann ein Informant weiterhin vertrauen.*[14]

Mit dieser Formulierung verneint das BVerfG den Gewahrsam der Journalisten an Verbindungsdaten, jedoch nicht aus dem Grund, dass an Daten kein Gewahrsam bestehen kann, sondern deshalb, weil sich diese Daten in der Herrschaftsphäre eines Dritten, dem Telekommunikationsanbieter, befinden. Maßgeblich für die Beurteilung, ob das bisherige Schutzniveau eingehalten ist, ist das Gewahrsamsmoment beim Journalisten. Auch in der späteren Entscheidung BVerfGE 124, 43 ff. - Beschlagnahme von Emails - versteht das BVerfG als „Gegenstand des Zugriffs“ auch nichtkörperliche Gegenstände, wie Emails auf einem Server.[15] Im Rahmen der offenen Beschlagnahme nach §§ 94, 97 Abs. 5 Satz 1 StPO ist somit das Überspielen von Daten von einem Träger auf einen anderen Träger möglich. Das bedeutet, dass die Polizei im Redaktionsraum vom Datenträger eines Journalisten eine Datei auf einen

[14] BVerfGE 107, 299 (333/334), Rn. 11.
[15] BVerfGE 124, 43 (60/61).

Datenträger der Polizei überspielen kann, allerdings nur, wenn die Voraussetzungen des § 97 Abs. 5 Satz 1 StPO vorliegen.
Dieses Schutzniveau bei der Beschlagnahme von Gegenständen wird bei heimlichen Ermittlungsmaßnahmen nach § 100a Abs. 1 Satz 3, Abs. 3 StPO noch unterschritten. Hier gilt § 160a Abs. 2 StPO. § 160a Abs. 2 StPO enthält jedoch im Vergleich zu § 97 Abs. 5 StPO oder im Vergleich zu §§ 100b Abs. 1, Abs. 3 Satz 2, 100d Abs. 5 Satz 1 StPO nur ein deutlich abgeschwächtes Schutzniveau, z.B. ein relatives Beweisverwertungsverbot.

Jedoch wiegen nach der Rechtsprechung des BVerfG heimliche Maßnahmen im Vergleich zu offenen Maßnahmen schwerer:

> *Das besondere Gewicht grundrechtlichen Schutzes gegen heimliche Eingriffe in die Kommunikationsfreiheit beruht darauf, dass heimliche Maßnahmen spezifische Risiken für die Rechte der Betroffenen bergen; diese können sich gegen den Eingriff frühestens dann mit rechtlichen Mitteln wehren, wenn er bereits vollzogen ist, und auch dies nur, wenn sie über die Maßnahme informiert werden oder auf andere Weise Kenntnis erlangen. Demgegenüber bieten offene Maßnahmen dem Betroffenen die Möglichkeit, -- gegebenenfalls unter Hinzuziehung anwaltlichen Beistands -- bereits der Durchführung der Maßnahme entgegen zu treten, wenn es an den gesetzlichen Voraussetzungen fehlt, oder aber zumindest die Einhaltung der im Durchsuchungsbeschluss gezogenen Grenzen einschließlich der für die Beschlagnahme vorgegebenen Richtlinien selbst zu überwachen und Ausuferungen des Vollzugs der richterlichen Anordnungen entgegenzutreten.*[16]

Angesichts der oben dargestellten Digitalisierung im journalistischen Arbeitsalltag ist eine Unterscheidung zwischen Daten, die sich auf dem Computer des Journalisten befinden und durch eine offene Beschlagnahme erlangt werden können und Daten, die durch eine Software verdeckt ausgelesen werden können, jedenfalls im Hinblick auf das im Jahr 2003 für ausschlaggebend gehaltene Gewahrsamsmoment nicht mehr zeitgemäß. Daraus folgt nach Meinung des DJV, dass gegen Maßnahmen nach § 100a Abs. 1 Satz 3, Abs. 3 StPO ein Schutzniveau nötig ist, das mindestens dem von § 97 Abs. 5 StPO entspricht.

[16] BVerfGE 124, 43 (65/66), Rn. 76.

b) „Qualifizierte Eingriffsschwelle“ als neues Schutzniveau nach dem BND-Urteil

In dem BND-Urteil[17] aus dem Jahr 2020 formulierte das BVerfG erste Ansätze eines neuen Schutzniveaus. Doch selbst dieser Maßstab wird von der bestehenden Regelung des § 100a Abs. 1 Satz 3, Abs. 3 StPO nicht eingehalten.

§ 100a Abs. 1 Satz 3, Abs. 3 StPO ist im systematischen Zusammenhang mit § 160a StPO zu verstehen. § 160a Abs. 2 StPO schafft ein Zwei-Klassen-System von Berufsgeheimnisträgern, das den Informantenschutz bei Presse und Rundfunk und das Redaktionsgeheimnis nicht ausreichend gewährleistet. § 160a Abs. 2 enthält nur ein relatives Erhebungs- und Verwertungsverbot nach Maßgabe einer Verhältnismäßigkeitsprüfung. Die Abwägung darf die Strafverfolgungsbehörde selbst vornehmen. Diese Einschränkung macht § 53 Abs. 1 Nr. 5 StPO nicht. Somit können trotz eines nach § 53 Abs. 1 Nr. 5 StPO bestehenden Zeugnisverweigerungsrechtes Informanten aufgespürt und Recherchematerialien in einen Prozess eingeführt werden, weil die entsprechenden Kenntnisse bereits im Ermittlungsverfahren gewonnen wurden.
Das Bundesverfassungsgericht hat die Relativierung des starken Schutzes für Journalisten durch § 160a Abs. 2 StPO im Zusammenhang mit der „klassischen“ Telekommunikationsüberwachung sowie der Abfrage von Verbindungsdaten bisher zwar grundsätzlich gebilligt.[18] Jedoch existierte § 100a Abs. 1 Satz 2 und Satz 3, Abs. 3 StPO in der angegriffenen Fassung damals noch nicht. Dieses BVerfG-Urteil aus dem Jahr 2011 muss insofern im Lichte der damaligen Lebenswirklichkeit gelesen werden, zumal es - bezogen auf die Tätigkeit von Journalisten - gegenüber dem Urteil von 2003 keine neuen Entwicklungen aufnimmt. Viele der Ermittlungsmaßnahmen, die heute technisch möglich sind, sind damals im Zusammenhang mit Journalist:innen überhaupt nicht diskutiert worden. Die damalige Eingriffsintensität und die vom BVerfG 2003 bzw. 2011 aufgestellten Maßstäbe passen nicht mehr zu den technischen Überwachungsmöglichkeiten, die § 100a Abs. 1 Satz 3, Abs. 3 StPO bietet. Die digitale Kommunikation hatte damals noch nicht den hohen Stellenwert, den sie heute hat. Digitale Kommunikation ist nicht mehr die Ausnahme, sondern die Regel. Das Smartphone beispielsweise hat sich von einem besseren Telefon zu einem Produkt entwickelt, das sämtliche Lebensbereiche durchdringt, aufzeichnet und digital erweitert. Jede Fingerbewegung auf einem Display ermöglicht einen speicherbaren

[17] BVerfGE 154, 152ff.
[18] BVerfGE 129, 208 ff – TKÜ-Neuregelung = NJW 2012, 833, 840 f.

Kommunikationsinhalt. Cloudnutzungen steckten noch in den Kinderschuhen. Die sich rasant verändernden Nutzungsgewohnheiten machen eine analoge Arbeit partiell unmöglich. Gleichzeitig werden die Methoden der Datenauswertung durch unbegrenzte Speichermöglichkeiten und künstliche Intelligenz immer besser. Im BND-Urteil aus dem Jahr 2020 heißt es dazu:

> *Während damals[19] die Telekommunikationsüberwachung in tatsächlicher Hinsicht eng begrenzte, allein in spezifischen Situationen benutzte Telekommunikationsmittel betraf, werden heute schon quantitativ unvergleichbar größere Datenströme erfasst. Mit ihnen wird eine unübersehbare Zahl von Formen elektronischer Kommunikation transportiert und der Auswertung zugeführt. Angesichts der ubiquitären und vielfältigen Nutzung von Kommunikationsdiensten findet inzwischen zunehmend jede Art individuellen Handelns und zwischenmenschlicher Interaktion in elektronischen Signalen ihren Niederschlag und wird so der Telekommunikationsüberwachung zugänglich.[20]*

In der Entscheidung BVerfGE 154, 152 ff. wird die Zwei-Klassen- Systematik des § 160a StPO zwar nicht per se in Frage gestellt. Dennoch macht das BVerfG deutlich, dass für eine Überwachung der Presse zumindest höhere Anforderungen zu stellen sind, als sie in §§ 100a Abs. 1 Satz 3, Abs. 3, 160a Abs. 2 StPO formuliert sind. Das Gericht verlangt nunmehr eine „qualifizierte Eingriffsschwelle" um sicherzustellen,

> dass *das Eindringen in Vertraulichkeitsbeziehungen nur zur Aufklärung von im Einzelfall schwerwiegenden Gefahren und besonders schweren Straftaten beziehungsweise zur Ergreifung bestimmter gefährlicher Straftäter zulässig ist. Es bedarf hierfür belastbarer Erkenntnisse. Im Übrigen ist eine Überwachung und Auswertung nur nach Maßgabe einer Abwägung zulässig, wonach das öffentliche Interesse an der Information das Interesse der Betroffenen an dem Schutz der Vertraulichkeit im Einzelfall überwiegt. Der Gesetzgeber wird zu prüfen haben, ob und wieweit hier zwischen verschiedenen Vertraulichkeitsbeziehungen weiter zu differenzieren ist (vgl. § 160a StPO; dazu BVerfGE 129, 208, 259 f.). Abzusichern ist ihr Schutz jedenfalls grundsätzlich durch eine*

[19] Das Adverb „damals" bezieht sich auf BVerfGE 100, 313 (379) – TKÜ I aus dem Jahr 1999, die Ausführungen sind jedoch auch für die Jahre 2003 und 2011 teilweise noch zutreffend.
[20] BVerfGE 154, 152 (243) = BVerfG NJW 2020, 2235, 2248 f.

gerichtsähnliche ex ante-Kontrolle.[21]

Diesem Maßstab genügt § 100a Abs. 1 Satz 3, Abs. 3 StPO iVm § 160a StPO nicht.

aa) Besonders schwere Straftaten

§ 100a Abs. 2 StPO stellt einen Straftatenkatalog auf, der Straftaten enthält, die nicht unter den verfassungsrechtlichen Begriff der „besonders schweren Straftat" fallen. Im Jahr 2004 hat das BVerfG im Rahmen der Entscheidung „Großer Lauschangriff" zur Bedeutung der besonders schweren Straftat ausgeführt und nur Straftaten darunter gefasst, die mit einem höheren Höchstmaß als 5 Jahre bewehrt sind:

> *„Der verfassungsrechtliche Begriff der besonders schweren Straftat kann nicht mit dem strafprozessualen Begriff einer Straftat von erheblicher Bedeutung gleichgesetzt werden. In der Strafprozessordnung gibt es neben der akustischen Wohnraumüberwachung weitere Eingriffsmaßnahmen, die ein bestimmtes Gewicht der aufzuklärenden Tat voraussetzen. So sind der genetische Fingerabdruck (§ 81 g), die Rasterfahndung (§ 98 a), die Auskunft über Verbindungsdaten der Telekommunikation (§ 100 g) und der Einsatz eines verdeckten Ermittlers (§ 110 a) nur zulässig, wenn das zu verfolgende Delikt eine Straftat von erheblicher Bedeutung ist. Eine solche Straftat muss mindestens der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.*[22]
> *(…)*
> *Der Gesetzgeber verfügt über einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung, welche Straftaten Anlass für die akustische Wohnraumüberwachung sein sollen. Bezogen auf Art. 13 Abs. 3 GG muss es sich abstrakt um eine besonders schwere Straftat handeln. Dafür gibt der Strafrahmen einen maßgebenden Anhaltspunkt. Von der besonderen Schwere einer Straftat im Sinne des Art. 13 Abs. 3 GG ist nur auszugehen, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat. Nach der gesetzlichen Systematik wird in Tatbeständen mit einem fünf Jahre übersteigenden oberen Strafmaß sogleich eine Höchststrafe von zehn Jahren Freiheitsentzug oder mehr normiert. Sie ist*

[21] BVerfGE 154, 152 (260/261).
[22] BVerfGE 109, 279ff (344) – Großer Lauschangriff.

denjenigen Delikten vorbehalten, die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen." [23]

Dieser formale Teil der Eingriffsschwelle wird in vielen Fällen nicht eingehalten.[24] Insbesondere ist aufgrund der Einzelfallprüfung nach § 100a Abs. 1 Nr. 2 StPO nicht von vornerein anzunehmen, dass minder schwere Fälle ausgeschlossen werden, weil sich im Stadium des Ermittlungsverfahrens regelmäßig nicht absehen lässt, ob ein solcher Fall vorliegt.[25]

bb) „Belastbare Erkenntnisse" als Prognoseelement für die Nachrichtenmittler-Eigenschaft

§ 100a Abs. 3 StPO verstößt gegen das Bestimmtheitsgebot, weil unklar ist, unter welchen Voraussetzungen ein Journalist Nachrichtenmittler ist.

Das BVerfG hat zu den Anforderungen des Bestimmtheitsgebotes ausgeführt, dass an die Normenklarheit und Bestimmtheit von Ermächtigungen zur heimlichen Erhebung und Verarbeitung personenbezogener Daten in der Regel gesteigerte Anforderungen zu stellen sind, weil die Datenverarbeitung von den Betroffenen unbemerkt stattfindet und sich die Befugnisse somit nicht im Wechselspiel von behördlicher Einzelanordnung und gerichtlicher Kontrolle schrittweise konkretisieren können.[26]

---

[23] BVerfGE 109, 279ff (347).

[24] §100a Abs. 2 Nr. 1 a) StPO enthält mit §§ 80a, 84, 85, 88, 89, 95 Abs. 1, 96 Abs. 2, 97, 98 Abs. 1 Satz 1, 99 Abs. 1 StGB Straftaten, die im Höchstmaß nur mit 3 bzw. 5 Jahren bewehrt sind. Das Höchstmaß der fünf Jahre wird bei diesen Straftaten nicht überschritten. Dies trifft auch auf § 100a Abs. 2 Nr. 1 c), d) StPO zu bezüglich §§ 129, 130 StGB (Volksverhetzung), § 100a Abs. 2 i) StPO bzgl. § 232 StGB (Menschenhandel), § 100a Abs. 2 Nr. 1 k) StPO bzgl. § 253 Abs. 1 StGB (Erpressung), § 261 StGB (Geldwäsche), § 100a Abs. 2 Nr. 1 p) bzgl. §§ 265c, 265d, 265e StGB (Besonders schwere Fälle des Sportwettbetrugs und der Manipulation von berufssportlichen Wettbewerben), § 100a Abs. 2 Nr. 1 r) bzgl. § 267 Abs. 4 Var. 2 StGB (minder schwerer Fall der gewerbsmäßigen Urkundenfälschung, § 100a Abs. 2 Nr. 1 t) StPO bzgl. § 298 StGB (Wettbewerbsbeschränkende Absprachen bei Ausschreibungen) und bezgl. §§ 299, 300 Satz 2 StGB (Besonders schwerer Fall der Bestechlichkeit und Bestechung im geschäftlichen Verkehr), § 100a Abs. 2 Nr. 1 u) bzgl. § 310 Abs. 1 Nr. 2, 3 und 4 StGB (Vorbereitung eines Explosions- und Strahlungsverbrechens), § 100a Abs. 2 Nr. 1 v) StPO bzgl. § 332 StGB (Bestechlichkeit) § 334 StGB (Bestechung). § 100a Abs. 2 Nr. 2 b) StPO aus der Abgabenordnung § 373 Abs. 1 Var. 2 AO (Minder schwerer Fall des gewerbsmäßigen Schmuggels), § 100a Abs. 2 Nr. 2 c) bzgl. § 374 Abs. 2 Satz 2 AO (minder schwerer Fall der Steuerhehlerei), § 100a Abs. 2 Nr. 5a StPO bzgl. § 13 Abs. 3 AusgStG (gewerbsmäßige, bandenmäßige Vermarktung von Ausgangsstoffen für Explosivstoffe), § 100a Abs. 2 Nr. 6 bzgl. § 17 Abs. 4 AWG sowie bzgl. § 18 Abs. 1 bis 5b AWG, § 100a Abs. 2 Nr. 9 a) bzgl. § 19 Abs. 1 und 3, 20 Abs. 2, 20a Abs. 1 KrWaffKontrG und § 100a Abs. 2 Nr. 9 b) bzgl. 22a Abs. 1 und 3 KrWaffKontrG, § 100a Abs. 2 Nr. 10 c) bzgl. § 8 Abs. 5 Var. 3 VStGB (minder schwerer Fall von Kriegsverbrechen gegen Personen gemäß § 8 Abs. 1 Nr. 6 und § 8 Abs. 3 Nr. 1 VStGB), § 100a Abs. 2 Nr. 11 a) bzgl. § 51 Abs. 1 und Abs. 3 Waffengesetz, § 100a Abs. 2 Nr. 11 b) bzgl. 52 Abs. 1 Nr. 1 und 2 c), d) und Abs. 6 Waffengesetz.

[25] BeckOK StPO/Graf StPO § 100a Rn. 110.

[26] BVerfGE 154, 152 (237/238) = NJW 2020, 2235, 2247.

Der Wortlaut des § 100a Abs. 3 StPO enthält zwar eine Formulierung, die die Prognose betrifft, ob jemand ein sogenannter Nachrichtenmittler ist: „Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben." Bereits im Rahmen einer regulären Telekommunikationsüberwachung, die keine Journalist:innen betrifft, ist nach der Rechtsprechung des BVerfG für die Annahme der Nachrichtenmittler-Eigenschaft gemäß § 100a Abs. 3 StPO eine gesicherte Tatsachenbasis unerlässlich. Das Gewicht des Eingriffs verlangt Verdachtsgründe, die über vage Anhaltspunkte und bloße Vermutungen hinausreichen. Bloßes Gerede, nicht überprüfte Gerüchte und Vermutungen reichen nicht aus. Erforderlich ist, dass aufgrund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus Zeugenaussagen, Observationen oder anderen sachlichen Beweisanzeichen auf die Eigenschaft als Nachrichtenmittler geschlossen werden kann.[27]

Journalist:innen sind jedoch bereits aufgrund ihres Berufes verpflichtet, mit Beschuldigten Kontakt aufzunehmen, wenn sie über sie berichten wollen, beispielsweise im Vorfeld einer Verdachtsberichterstattung oder wenn sie Informationen von einem Beschuldigten als Informanten benötigen. Insofern darf nicht lediglich aus der Eigenschaft, Journalist zu sein, die Nachrichtenmittler-Eigenschaft geschlossen werden. Welche anderen Umstände jedoch für die Einstufung eines Journalisten als Nachrichtenmittler in Betracht kommen, ist unklar. Besonders für eine Berufsgruppe, die auf die digitale Übermittlung von Nachrichten angewiesen ist, sind insofern klare, voraussehbare Kriterien notwendig. Im genannten BND-Urteil formuliert das BVerfG zwar das Prognoseelement der „belastbaren Erkenntnisse",[28] wobei auch hier unklar bleibt, ob sich dieses vor dem Hintergrund des § 100a Abs. 1 Satz 3, Abs. 3 StPO auf die zu prognostizierende Eigenschaft als Nachrichtenmittler oder auf die Beschuldigteneigenschaft bezieht.
Diese Formulierung lässt Raum für Interpretation. Der Unterschied zur „gesicherten Tatsachenbasis" ist nicht geklärt. Nach dem Wortlaut könnte die Formulierung „belastbare Erkenntnisse" ein höherer Verdachtsgrad sein als „gesicherte Tatsachenbasis", weil in ersterer auch eine bildlich-körperliche Assoziation steckt und in letzterer nur eine abstrakte. Darüber hinaus weist der Begriff der Erkenntnis nach dem allgemeinen Sprachgebrauch darauf hin, dass bereits eine Einsicht durch die Verarbeitung von Eindrücken und Erfahrungen gewonnen wurde. Wohingegen der Begriff

[27] BVerfG NJW 2023, 1645, 1647 – Beschluss vom 21.3.2023 – 2 BvR 626/20.
[28] BVerfGE 154, 152 (260).

„Tatsachenbasis“ nur eine Zusammenstellung von Tatsachen ist.

Da § 100a Abs. 3 StPO für Journalist:innen hinsichtlich des Verdachtsgrades zur Einstufung als Nachrichtenmittler nicht differenziert, verstößt § 100a Abs. 3 StPO gegen das Bestimmtheitsgebot.

cc) Gerichtsähnliche ex-ante Kontrolle

Eine gerichtsähnliche ex-ante Kontrolle erfolgt nicht. Das Verfahren für Maßnahmen nach § 100a Abs. 1 Satz 3, Abs. 3 StPO ist in § 100e StPO geregelt. Bei Gefahr im Verzug kann die Anordnung gemäß § 100e Abs. 1 Satz 2 StPO auch durch die Staatsanwaltschaft geschehen. Die Staatsanwaltschaft ermöglicht keine gerichtsähnliche ex-ante Kontrolle, weil ihre Aufgabe die Strafverfolgung ist.[29]

C. Verfassungswidrigkeit von § 100a Abs. 1 Satz 2, Abs. 3 StPO

I. Eingriffsintensität

Die Quellen-TKÜ unterscheidet sich zur kleinen Online-Durchsuchung lediglich dadurch, dass nach Anordnungszeitpunkt laufende Telekommunikation ausgelesen werden kann.

II. Unverhältnismäßigkeit

Die Ausführungen der Verfassungsbeschwerde auf den Seiten 75 und 76 zu der technischen Unmöglichkeit, sicherzustellen, dass eine Software nur laufende Kommunikation ausliest, sind zutreffend. Eine Maßnahme nach § 100a Abs. 1 Satz 2 StPO steht somit im technischen Zusammenhang mit § 100a Abs. 1 Satz 3 StPO. § 100a Abs. 1 Satz 2, Abs. 3 StPO ist aus den gleichen Gründen unverhältnismäßig.
Die vom BVerfG geforderte, qualifizierte Eingriffsschwelle bezüglich der oben unter Fußnote 24 genannten Katalogstraftaten wird auch im Hinblick auf § 100a Abs. 1 Satz 2, Abs. 3 StPO nicht erreicht. Ebenso greifen die Argumente hinsichtlich des Verstoßes gegen das Bestimmtheitsgebot auf Seite 15 bis 17 unter bb) und hinsichtlich der

[29] Dass die Staatsanwaltschaft keine gerichtsähnliche Kontrolle in diesem Sinne bietet, entspricht der Rechtsprechung des EGMR, vgl. EGMR Urteil vom 14.09.2010 (38224/03) Case of Sanoma Uitgevers B.V. v. The Netherlands, Rn. 93.

fehlenden, gerichtsähnlichen Kontrolle auf Seite 17 unter cc).

D. Verletzung von Art. 5 Abs. 1 Satz 2 GG in seiner objektiven Dimension

Ermittlungsbehörden können eine Überwachungssoftware nur dann auf ein IT-System überspielen, wenn das IT-System selbst eine Sicherheitslücke aufweist, die es ermöglicht, solche eine Überwachungssoftware aufzuspielen. Ermittlungsbehörden haben somit ein Interesse daran, dass IT-Systeme eine Sicherheitslücke haben. Diese Sicherheitslücke kann auch von anderen Akteuren genutzt werden, wie von Unternehmen oder Geheimdiensten anderer Staaten. Wer genug Geld investiert, weiß jederzeit, welche Journalist:innen welche Themen bearbeiten, wie der Stand einer Recherche ist und was, wann und auf welchem Weg veröffentlicht werden soll.[30] Mithilfe des Staatstrojaners Pegasus der israelischen Firma NSO wurden beispielsweise in Ungarn Journalist:innen überwacht.[31] Bei NSO arbeiten mehr als 860 Programmierer:innen daran, Sicherheitslücken in Smartphones zu finden.[32] Mindestens 74 Regierungen haben laut einer Datenbank des US-Thinktanks Carnegie Endowment zwischen 2011 und 2023 Spyware gekauft, darunter hauptsächlich von NSO.[33] Es besteht das Risiko, dass die Recherche komplett manipuliert oder die Veröffentlichung verhindert wird. Redaktionen arbeiten heutzutage immer vernetzter und recherchieren in internationalen Rechercheverbünden zu Themen, die mehrere Staaten betreffen; gerade im Hinblick auf internationale Unternehmen und im Hinblick auf gesellschaftliche Missstände mit internationalen Bezügen kann die Presse nicht mehr frei arbeiten. Insofern wird in der Verfassungsbeschwerde zurecht darauf hingewiesen, dass der Staat durch diese Maßnahmen Schutzlücken für die IT-Sicherheit schafft. Damit ist ein weiteres Gefährdungspotential für Informantenschutz und Redaktionsarbeit gegeben.

[30] Die Überwachungssoftware wird von der Firma NSO verkauft, vgl. https://www.zeit.de/digital/datenschutz/2020-06/spionage-ueberwachung-nso-marokko-journalist-pegasus
[31] https://www.zeit.de/politik/ausland/2021-07/pressefreiheit-ungarn-ueberwachung-journalisten-spionage-software-pegasus-cyberwaffe
[32] https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handydaten-rechtsstaat/komplettansicht
[33] https://www.journalist.de/startseite/detail/article/die-spyware-jagd; https://carnegieendowment.org/programs/democracy/commercialspyware

E. Verletzung von Art. 10 Abs. 2 EMRK durch §§ 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO

§§ 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO genügen auch den Voraussetzungen der EGMR-Rechtsprechung bezüglich eines Eingriffes in das Redaktionsgeheimnis und in den Quellenschutz aus Art. 10 Abs. 2 EMRK nicht.
Der EGMR hat in mehreren grundlegenden Urteilen die Reichweite und den Umfang des Schutzes der journalistischen Quellen auf der Grundlage des Art. 10 EMRK bestimmt und die Bedeutung des journalistischen Quellenschutzes als eine der Grundvoraussetzungen der Pressefreiheit herausgestellt. Der Gerichtshof betont, dass ohne den Schutz der Quellen die wichtige öffentliche Kontrollfunktion der Presse untergraben werden könnte und die Fähigkeit der Presse, genaue und verlässliche Informationen zu liefern, negativ beeinflusst werden könnte.[34] Der EGMR führt darüber hinaus aus, dass das Recht auf Quellenschutz durch Verfahrensgarantien sichergestellt werden muss, die der Bedeutung dieses Schutzes für die Pressefreiheit entsprechen. Unter den notwendigen Verfahrensgarantien einer Rechtsordnung sei zuerst und vor allem die Garantie notwendig, dass ein Richter oder eine unabhängige und unparteiische Stelle angerufen werden kann, bevor die Polizei oder der Staatsanwalt Zugang zu den Quellen erhält.[35] Die unabhängige und unparteiische Stelle muss mit den nötigen Befugnissen ausgestattet sein, um das Überwiegen des einen oder des anderen öffentlichen Interesses unter Beachtung der Bedeutung der Pressefreiheit festzustellen und ggf. einem unnötigen Zugang zu geschützten Informationen vorzubeugen, der geeignet ist, die Identität der Quellen preiszugeben, wenn das

[34] Case of Goodwin v. The United Kingdom, no. 17488/90, judgment 27/03/1996, Rn. 39: "Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected."

[35] Case of Sanoma Uitgevers B.V. v. The Netherlands, Rn. 90: "First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body.", Rn. 92: "Given the preventive nature of such review the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed." und Rn. 94: "According to the guideline of 19 May 1988, under B (see paragraph 37 above), the lawful seizure of journalistic materials required the opening of a preliminary judicial investigation and an order of an investigating judge."

öffentliche Interesse an der Strafverfolgung nicht überwiegt.[36] Obwohl auch der Staatsanwalt an Recht und Gesetz gebunden sei, stelle er doch, was das Ermittlungsverfahren anbelangt, eine Partei dar, die Interessen vertrete, die möglicherweise nicht mit dem journalistischen Quellenschutz vereinbar seien. Er könne daher nicht als objektive und unparteiische Partei angesehen werden, die die notwendige Bewertung der konkurrierenden Interessen vornimmt.[37] §§ 100a Abs. 1 Satz 2 und 3, Abs. 3, 100e Abs. 1 Satz 2 StPO bestimmt jedoch eine Anordnungsbefugnis der Staatsanwaltschaft und verstößt somit gegen diese Rechtsprechung.

§ 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO ist außerdem nicht mit der Rechtsprechung des EGMR bezüglich des Ermessensspielraums vereinbar. Der EGMR verlangt nicht nur, dass ein Gericht die Möglichkeit hat, über das „Ob“ und ggf. auch die Reichweite des Eingriffs in den Informantenschutz zu entscheiden.[38] Der Gerichtshof macht auch deutlich, dass im Gesetz mit ausreichender Klarheit der Umfang des Ermessensspielraums, der den zuständigen Behörden eingeräumt wird und die Art und Weise seiner Ausübung festgeschrieben werden müssen.[39] Das ist in §§ 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO nicht der Fall. Denn die Voraussetzungen für die Nachrichtenmittler-Eigenschaft sind, wie oben unter (2) auf Seite 15 dargestellt, zu unbestimmt.

Die Berücksichtigung dieser EGMR-Rechtsprechung hinsichtlich der gerichtlichen Kontrolle und hinsichtlich der Anforderungen an die Klarheit des

---

[36] Case of Sanoma Uitgevers B.V. v. The Netherlands, Rn. 90: "The requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not."

[37] Case of Sanoma Uitgevers B.V. v. The Netherlands, Rn. 93: "Although the public prosecutor, like any public official, is bound by requirements of basic integrity, in terms of procedure he or she is a “party” defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests."

[38] Case of Sanoma Uitgevers v. The Netherlands, Rn. 90: " In such situations an independent review carried out at the very least prior to the access and use of obtained materials should be sufficient to determine whether any issue of confidentiality arises, and if so, whether in the particular circumstances of the case the public interest invoked by the investigating or prosecuting authorities outweighs the general public interest of source protection."

[39] Case of Sanoma Uitgevers v. The Netherlands, Rn. 82: "For domestic law to meet these requirements it must afford a measure of legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise (see, among many other authorities, the Sunday Times v. the United Kingdom (no. 1) judgment of 26 April 1979, Series A no. 30, § 49; Tolstoy Miloslavsky v. the United Kingdom, 13 July 1995, § 37, Series A no. 316-B; Rotaru v. Romania [GC], no. 28341/95, § 52, ECHR 2000-V; Hasan and Chaush v. Bulgaria [GC], no. 30985/96, § 84, ECHR 2000-XI; and Maestri v. Italy [GC], no. 39748/98, § 30, ECHR 2004-I)."

Ermessensspielraums bewegt sich auch innerhalb der vom BVerfG im BND-Urteil entwickelten Anforderungen einer „qualifizierten Eingriffsschwelle“ und innerhalb der Anforderungen des Bestimmtheitsgebotes. Ihre Berücksichtigung stünde insofern im Einklang mit dem deutschen Verfassungsrecht.[40]

F. Zusammenfassung

Da das Vertrauensverhältnis zwischen Journalist:innen und ihren Informant:innen geschützt ist, kann verfassungsrechtlich nicht entscheidend sein, ob sich beide Personen im Gespräch gegenübersitzen, über Mobilfunk telefonieren oder per Mail, Videotelefonie oder in einem sozialen Netzwerk kommunizieren. Je öffentlicher die Ermittlungsmaßnahme analoge Arbeitskontexte von Journalist:innen betrifft, desto höher sind zurzeit ihre rechtlichen Schutzvoraussetzungen. Heute kommuniziert diese Berufsgruppe jedoch nicht per Brief, sondern digital. Das bisherige Schutzniveau für offene Überwachungsmaßnahmen muss auch für heimliche Überwachungsmaßnahmen gelten.

Aus Sicht des DJV ist § 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO verfassungswidrig, weil diese Regelung nicht den Anforderungen der qualifizierten Eingriffsschwelle entspricht.[41] Somit wird nicht nur das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt, sondern hinsichtlich § 100a Abs. 1 Satz 2 und 3, Abs. 3 StPO auch die Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG. Der Verfassungsbeschwerde sollte auch aus diesem Grund stattgegeben werden.

Hanna Möllers
- Justiziarin -

Christoph Brill
- Referent des Justiziariats -

[40] Vgl. BVerfGE 111, 307 (328) – EGMR-Entscheidungen.
[41] Dies gilt auch für § 100a Abs. 1 Satz 1, Abs. 3 StPO, denn auch diese Maßnahme ist ein Eingriff in Vertraulichkeitsbeziehungen, der die qualifizierte Eingriffsschwelle nicht erreicht. § 100a Abs. 1 Satz 1 StPO ist jedoch nicht Gegenstand der Verfassungsbeschwerde. § 100b Abs. 1, Abs. 3 Satz 2 StPO dagegen genügt jedenfalls der qualifizierten Eingriffsschwelle im Rahmen von Art. 5 Abs. 1 Satz 2 GG, weil § 100d Abs. 5 Satz 1 StPO ein absolutes Beweiserhebungsverbot enthält, das sich am Schutzniveau des § 53 StPO orientiert.