ARD Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten
BDZV Bundesverband Digitalpublisher und Zeitungsverleger
Deutschlandradio
DJV Deutscher Journalisten-Verband
dju Deutsche Journalistinnen- und Journalisten-Union
Deutscher Presserat
MVFP Medienverband der freien Presse
VAUNET – Verband Privater Medien
ZDF Zweites Deutsches Fernsehen

Stellungnahme zum Referentenentwurf „Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“

A. Einleitung

Der Entwurf verringert das Schutzniveau für journalistische Berufsgeheimnisträger in Deutschland und stößt damit auf erhebliche verfassungsrechtliche Bedenken. Die Presse- und Rundfunkfreiheit schützt journalistische Tätigkeit von der Beschaffung von Informationen bis zur Verbreitung der Nachricht und der Meinung. Das Bundesverfassungsgericht betont in seiner ständigen Rechtsprechung insbesondere, dass die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse bzw. Rundfunk und Informanten von Art. 5 Abs. 1 Satz 2 GG geschützt sind. Dieser Schutz ist demnach unentbehrlich, weil Medien auf private Mitteilungen nicht verzichten können, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann.[1] Der vorliegende Referentenentwurf geht indes mit keinem Wort auf die Eingriffsqualität für die Presse- und Rundfunkfreiheit ein und zeigt damit, dass die Grundrechtsrelevanz der Vorschläge verkannt wird.

[1] BVerfG, Beschluss vom 13.7.2015 - 1 BvR 1089/13, 1 BvR 1090/13, Rn. 15.

Gerade wenn das Berufsgeheimnis betroffen ist, sollte das Justizministerium den betroffenen Verbänden auch Gelegenheit geben, effektiv Stellung zu nehmen. Die meisten Mitglieder des Medienbündnisses waren nicht auf der Verteilerliste des BMJV. Sie haben daher von dem Entwurf erst kurz vor Fristende erfahren.

Das Medienbündnis geht daher in aller Kürze auf das verringerte Schutzniveau ein (B.), anschließend auf die Erhebung von Nutzungsdaten (C.), auf die Möglichkeit, Bewegungsprofile zu erstellen (D.), auf die Sicherungsanordnung (E.) und schließlich auf die Unvereinbarkeit einiger Verfahrensregelungen mit dem European Media Freedom Act und der Rechtsprechung des EGMR (F.).

B. Verringertes Schutzniveau für Journalist:innen

Das Medienbündnis bemängelt, dass der Entwurf den Berufsgeheimnisschutz für Journalist:innen besorgniserregend reduziert. Die Strafverfolgungsbehörden könnten danach beim Telekommunikationsdiensteanbieter Verkehrsdaten über Journalist:innen erheben, sobald sie sog. Nachrichtenmittler sind.[2]

Bisher verbietet § 100g Abs. 4 StPO die Erhebung von Verkehrsdaten bei Journalist:innen, sogar unabhängig davon, ob sie Nachrichtenmittler sind. Dieser bisherige § 100g Abs. 4 StPO wird gestrichen, was der Entwurf auf Seite 28 damit begründet, dass die Polizei aus der IP-Adresse keine Erkenntnisse darüber erhalte, mit wem Berufsgeheimnisträger kommuniziert hätten.

Das mag zutreffen in Bezug auf die IP-Adresse an sich – losgelöst von anderen Maßnahmen. Eine Verkehrsdatenerhebung, die den Anschlussinhaber einer IP-Adresse abfragt, findet jedoch in der Regel im Zusammenhang mit anderen Maßnahmen statt. Wenn man sich den regelmäßigen Ermittlungsstand sowie die parallel möglichen Datenerhebungsmaßnahmen verdeutlicht, wird nachvollziehbar, warum die Annahme nicht zutrifft. Die hier einzuführenden Datenerhebungsmaßnahmen kommen im Regelfall zu einem Ermittlungszeitpunkt zum Einsatz, bei dem die Polizei bereits weiß, dass sich jemand strafbar z.B. im Internet verhalten hat. Etwaige Opfer könnten ihr sogar Screenshots der Tat liefern. Die Polizei kennt dann den regelmäßig anonym agierenden Täter nicht. Sie wird dann zunächst Nutzungsdaten (wozu die IP-Adresse gehört) bei digitalen Diensten erheben, z.B. anfragen, zu welcher IP-Adresse ein bestimmtes Social-Media-Profil gehört. Nach dem Erfolg dieser Maßnahme kann sie die erlangte IP-Adresse bei einem Telekommunikationsanbieter nach § 100g Abs. 1 StPO-E mit dem Anschlussinhaber abgleichen.

[2] Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben.

Der Abgleich ist insbesondere bei Kommunikationsinhalten vor dem Hintergrund des Quellenschutzes problematisch. Wenn die Polizei über einen Screenshot zu einem Kommunikationsinhalt verfügt, der Anhaltspunkte dafür enthält, dass jemand eine Katalog-Straftat begangen hat, den Inhalt aber weder einem Empfänger noch einem Absender zuordnen kann, kann sie nach § 100g Abs. 1 Satz 2 StPO-E[3] die Verkehrsdaten von Journalist:innen als betroffene Nachrichtenmittler erheben und so auch herausfinden, mit wem ein Journalist kommuniziert hat. Ein Beispiel soll dies verdeutlichen:

> B betreibt einen Online-Shop. Er verkauft Laptops, liefert wissentlich beschädigte Ware und weist seine Mitarbeiter an, Nacherfüllung kategorisch zu verweigern und eine Beschädigung beim Transport zu behaupten. Mitwirkender M bekommt Gewissensbisse und informiert eine anonyme Journalistin J. Er nutzt dafür den Social-Media-Account des Online-Shops über einen PC in den Geschäftsräumen des B. Die Polizei entdeckt die Geschäftsräume und findet den Chat auf dem Account. Sie kennt aber weder die Identität des B, M noch der J.

Hier könnte die Polizei gemäß § 100k Abs. 1 StPO-E zunächst bei dem Social-Media-Betreiber als digitalen Dienst die sog. Nutzungsdaten[4] erheben, die der Dienst zu dem Profil von J gespeichert hat. Die IP-Adresse könnte die Polizei wiederum nutzen, um beim Telekommunikationsanbieter gemäß § 100g Abs. 1 StPO-E die Verkehrsdaten zu erheben, wozu insbesondere die Zuordnung eines Anschlussinhabers zu einer IP-Adresse gehört. Es steht zu befürchten, dass die Polizei wegen § 100g Abs. 1 S. 2 StPO-E so ebenfalls den Namen von J erfahren kann und auch, dass sie als journalistische Berufsgeheimnisträgerin mit einem Informanten kommuniziert hat. Die Annahme, die Strafverfolgungsbehörde könne nicht erfahren, mit wem ein Berufsgeheimnisträger kommuniziert habe, ist also unzutreffend. Diese Verkehrsdatenerhebung verstößt ebenfalls gegen die Vorgaben des European Media Freedom Act (EMFA). Der EMFA verbietet explizit Maßnahmen, die darauf abzielen, Informationen zu erlangen, die mit journalistischen Quellen oder vertraulicher Kommunikation im Zusammenhang stehen oder diese identifizieren können. Die vorgesehene Möglichkeit, über die Verkehrsdatenerhebung Rückschlüsse auf die Kommunikationspartner von Journalisten zu ziehen, stellt einen Verstoß gegen die europarechtlichen Schutzgarantien dar.

Die Datenerhebung bei Journalist:innen ist aus Sicht des Medienbündnisses außerdem nicht angemessen im Sinne von § 100g Abs. 1 Satz 1 Nr. 3 StPO-E und auch nicht verhältnismäßig im Sinne von § 160a Abs. 2 StPO, weil der Informationswert für die Ermittlung in der Regel gering ist. Die Anschlussinhaberschaft, also der schlichte Name

[3] StPO-E bzw. TKG-E meint die entsprechende Regelung aus dem Entwurf.
[4] Nutzungsdaten sind in § 3 Abs. 2 Nr. 3 TDDDG nicht abschließend definiert. Dazu gehört insbesondere die IP-Adresse, Angaben über Beginn und Ende sowie Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste. Aber auch der Umfang der Nutzung, mehr dazu unter C.

der Journalistin, bringt die Ermittlungen im obigen Fall zu M oder B nicht weiter. Die Polizei wäre darauf angewiesen in einem zweiten Schritt, die Journalistin zur Identität von M oder B zu vernehmen. Dann könnte sich die Berufsgeheimnisträgerin bereits auf ihr Zeugnisverweigerungsrecht aus § 53 Abs. 1 Satz 1 Nr. 5, Satz 2 StPO berufen, weil ihr im Hinblick auf ihre journalistische Tätigkeit eine Mitteilung gemacht wurde. Daher wäre eine Ermittlungsmaßnahme, die sowieso am Zeugnisverweigerungsrecht scheitert, nicht angemessen im Sinne von § 100g Abs. 1 Satz 1 Nr. 2 StPO-E. Sie wäre aus diesem Grund auch nicht verhältnismäßig im Sinne von § 160a Abs. 2 StPO, da bei der Verhältnismäßigkeitsprüfung insbesondere das Informationsinteresse der Öffentlichkeit und der für die Aufgabenerfüllung der Medien unerlässliche Quellenschutz mit dem Strafverfolgungsinteresse abgewogen werden muss und letzteres geringer ist, wenn die Journalistin sich bei einer Vernehmung auf ihr Zeugnisverweigerungsrecht berufen kann. Warum dann der bisherige Berufsgeheimnisschutz auf dem Schutzniveau von § 100g Abs. 4 StPO nicht beibehalten werden kann, ist nicht nachvollziehbar.

Der Entwurf begründet die Streichung des § 100g Abs. 4 StPO darüber hinaus auf Seite 28 damit, dass sich die Speicherpflicht zukünftig allein auf IP-Adressen beziehe. Auch diese Annahme ist in dieser Absolutheit unzutreffend. Verkehrsdaten erfassen mehr als nur die IP-Adresse, vgl. § 3 Nr. 70 TKG, wonach das Daten sind, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Dieser weiten Erhebungsbefugnis korrespondiert eine – ebenfalls der Entwurfsbegründung widersprechende – viel zu weite Speicherungspflicht der Telekommunikationsanbieter in § 176 TKG-E, wonach sie mehr speichern müssen, als die IP-Adresse, weil sie nach § 176 Abs. 1 Satz 1 Nr. 4 TKG-E auch weitere Verkehrsdaten speichern müssen, *soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind.* Welche Verkehrsdaten dafür neben den Daten aus Nr. 1 bis 3 noch erforderlich sind, wird nicht weiter ausgeführt.

Schließlich sei nach der Entwurfsbegründung der Schutz von Berufsgeheimnisträgern über § 160a StPO gewährleistet. Das absolute Beweiserhebungsverbot des § 160 Abs. 1 StPO erfasst Journalist:innen jedoch nicht. Der relative Schutz aus § 160a Abs. 2 StPO, der auch für Journalist:innen gilt, setzt lediglich eine Abwägung voraus, was letztlich bedeutet, dass jene nicht sicher sein können, ob ein Gericht das Strafverfolgungsinteresse nicht höher einschätzt als das Informationsinteresse der Öffentlichkeit. Gerade für den Berufsgeheimnisschutz sollten die Berufsgeheimnisträger jedoch wissen, unter welchen Bedingungen ihre Kommunikation Gegenstand einer Strafverfolgungsmaßnahme sein kann. Mit der weiter zunehmenden Digitalisierung werden immer mehr Strafverfolgungsmaßnahmen in den digitalen Raum verlagert, wo gleichzeitig immer

mehr journalistische Recherchen und Kommunikation stattfindet. All dies kann dazu führen, dass Journalist:innen von etwaigen Investigativ-Recherchen insbesondere zu Missständen in Behörden Abstand nehmen. Auch ist zu befürchten, dass potenzielle Quellen aus Angst vor der Identifikation von einer Kontaktaufnahme zu Journalist:innen absehen (chilling effect). Dies hätte jedoch fatale Auswirkungen für die Kernaufgabe der Medien, die Aufdeckung von Missständen.

Der bisherige journalistische Berufsgeheimnisschutz sollte daher insbesondere für die Verkehrsdatenerhebung beibehalten werden.

C. Erhebung von Nutzungsdaten von Nachrichtenmittlern bei digitalen Diensten, § 100k Abs. 1 Satz 2 iVm § 100g Abs. 1 Satz 2 StPO-E

Das Medienbündnis beanstandet außerdem, dass mit der Erhebung von Nutzungsdaten bei einem digitalen Dienst auch Rechercheinhalte von Journalist:innen als Nachrichtenmittler erhoben werden können. Wenn nach dem bisherigen § 100g Abs. 4 StPO journalistische Berufsgeheimnisträger schon bei der Verkehrsdatenerhebung geschützt sind, dann sollte sich das Verbot erst recht auf die Nutzungsdatenerhebung beziehen, da die Nutzungsdaten im Gegensatz zu den Verkehrsdaten auch detaillierte Rechercheinhalte umfassen können.

Zu den Nutzungsdaten gehört auch der Umfang der Nutzung, was inhaltsbezogene Daten, z.B. Formulareingaben oder Internetadressen umfasst.[5] Journalist:innen müssen bei investigativen Recherchen regelmäßig Webseiten, Foren oder Chats besuchen. Ihre Aktivität dort kann inklusive ihrer Nachrichten erhoben werden, wenn die Polizei beim digitalen Dienst, dem Betreiber der Webseite, auf der sich der Chat oder das Forum befindet, Nutzungsdaten der Journalistin nach §§ 100k Abs. 1, 100g Abs. 1 Satz 2 StPO-E iVm § 160a Abs. 2 StPO erhebt. Hätte die Journalistin J im obigen Beispiel den Online-Shop von B besucht und dort Daten eingegeben, kann die Polizei vom Webseitenbetreiber diese Daten erheben.

D. Bewegungsprofile, § 100g Abs. 3 StPO-E

Des Weiteren stößt die Befugnis zur Erhebung von Standortdaten aus § 100g Abs. 3 StPO-E auf erhebliche Bedenken. Diese Befugnis ermöglicht es der Polizei, Bewegungsprofile von Journalist:innen zu erstellen. Die Entwurfsbegründung zu § 100g Abs. 3 StPO-E geht auf Seite 30 davon aus, dass Standortdaten in der Regel nach 7 Tagen gelöscht würden, was zu kurz sei, um Bewegungsprofile zu erstellen. Dem ist nicht zuzustimmen. Darüber hinaus vermutet der Referentenentwurf nur, dass Standortdaten 7 Tage lang gespeichert würden. Tatsächlich korrespondiert zu dieser Erhebungsbefugnis

[5] Ferner, BeckOK StPO, 58. Edition, § 2 TDDDG, Rn. 29, 30.

im Entwurf keine genaue Speicherungspflicht. § 13 TDDDG überlässt bestimmten Telekommunikationsdiensten, wozu inzwischen insbesondere webbasierte Email-Dienste und Messengerdienste zählen,[6] den Umfang der gespeicherten Standortdaten.[7] Dabei scheint der Referentenentwurf darauf zu bauen, dass die Anbieter schon ein eigenes (finanzielles) Interesse daran haben, Standortdaten ihrer Nutzer:innen zu speichern.[8] Für Journalist:innen und andere Berufsgeheimnisträger wäre es fatal, wenn Polizeibehörden den Rechercheschwerpunkt der Journalist:innen nach geografischen Daten ordnen könnten, weil sie so gezielt Recherchen von vornerein beeinflussen können.

Daher sollte der Berufsgeheimnisschutz ebenfalls auf § 100g Abs. 3 StPO-E bezogen werden.

E. Sicherungsanordnung, § 100g Abs. 7 StPO-E

Der Entwurf ermöglicht außerdem eine Sicherungsanordnung, die gezielt die Verkehrsdaten von Betroffenen sichern soll, wobei für die Betroffenheit bereits ein persönlicher oder räumlicher Bezug einer Person zu einer Straftat ausreicht. Wenn sich also ein Journalist am Tatort befand, können seine Verkehrsdaten erhoben werden in den relativen Grenzen des § 160a Abs. 2 StPO. In einem zweiten Schritt soll dann die Erhebung nach § 100g Abs. 1 bis 4 StPO-E erfolgen. Zweck dieser Sicherungsanordnung, die an das Quick Freeze-Verfahren erinnert, ist es, die Verkehrsdatenspeicherung punktuell zu verlängern, da die Verkehrsdaten wegen § 176 TKG-E nur drei Monate gespeichert werden. Wenn jedoch bisher der journalistische Berufsgeheimnisträgerschutz aus § 100g Abs. 4 StPO schon bei der Erhebung angesetzt hat, sollte er erst recht auf die Sicherungsanordnung bezogen werden. Wie oben unter B. dargestellt, enthält die Information über eine Anschlussinhaberschaft (aus den Verkehrsdaten) in der Regel keinen hohen Mehrwert, sodass die Polizei auf eine Vernehmung angewiesen wäre, für die sich der betroffene Journalist auf sein Zeugnisverweigerungsrecht berufen kann.

F. Unvereinbarkeit der Verfahrensregelungen mit Art. 4 Abs. 4 d) EMFA

Schließlich sind einige Verfahrensregelungen des Entwurfes nicht mit EU-Recht vereinbar.

I. § 101a Abs. 1 StPO-E

Zunächst ist die dreitägige Frist für die nachträgliche, gerichtliche Kontrolle bestimmter Datenerhebungsmaßnahmen nicht mit dem EMFA vereinbar.

---

[6] Eckhardt, Spindler/Schuster/Kaesling, Recht der elektronischen Medien, 5. Auflage 2026, § 3 TDDDG, Rn. 76.
[7] Voraussetzung wäre eine Einwilligung des Nutzers.
[8] Vgl. zur finanziellen Seite der Standortdaten: https://www1.wdr.de/nachrichten/standortdaten-adver-tiser-id-datenbroker-100.html

Die Verfahrensregelung aus § 101a Abs. 1 StPO-E zu den Maßnahmen aus § 100g StPO-E (Verkehrs- und Standortdaten), § 100k StPO-E (Nutzungsdaten) sowie § 100e Abs. 1 StPO (aktuelle Fassung) hält die Ausnahmen aus Art. 4 Abs. 4 d) EMFA[9] nicht ein. Die Erhebung der Verkehrsdaten, Standortdaten und Nutzungsdaten bei Nachrichtenmittlern ist aus Sicht des Medienbündnisses eine Überwachungshandlung im Sinne des Art. 4 Abs. 3 EMFA, aus der sich wie oben unter B. dargestellt, Informationen ergeben, die mit journalistischen Quellen oder vertraulicher Kommunikation im Zusammenhang stehen. Daher müsste ein Gericht diese Abfrage bei Gefahr im Verzug nachträglich unverzüglich gemäß Art. 4 Abs. 4 d) EMFA genehmigen. Nach § 100e Abs. 1 Satz 3 StPO (aktuelle Fassung) reichen aber drei Tage. Anders als im deutschen Recht gibt es noch keine feste Rechtspraxis dazu, wie der Begriff „unverzüglich“ aus Art. 4 Abs. 4 d) EMFA auszulegen ist. Der Begriff “unverzüglich” erfordert eine Kontrolle ohne schuldhaftes Zögern. Die europarechtliche Vorgabe zielt darauf ab, den Schutz journalistischer Quellen durch eine sehr zeitnahe richterliche Überprüfung zu gewährleisten. Eine (starre) dreitätige Frist verfehlt dieses Ziel und führt zur unzulässigen Verzögerung des Rechtsschutzes für Medien und Journalisten. Drei Tage ist daher aus Sicht des Medienbündnisses jedenfalls länger als unverzüglich und damit nicht mit dem EMFA vereinbar.

II. Keine gerichtliche Kontrolle der Maßnahme aus § 100g Abs. 5 StPO-E

Weiterhin existiert für die Erhebung der IP-Adresse und weiterer Verkehrsdaten bei der Nutzung von Diensten wie z.B. WhatsApp gemäß § 100g Abs. 5 StPO-E überhaupt keine nachträgliche gerichtliche Kontrolle, weil § 101a StPO-E den § 100g Abs. 5 StPO-E nicht in Bezug nimmt. Das verstößt ebenfalls gegen Art. 4 Abs. 4 d) EMFA, der eine gerichtliche Kontrolle voraussetzt.

III. Keine gerichtliche Kontrolle der Sicherungsanordnung, § 101a Abs. 1 Satz 1 Nr. 3a StPO-E

Darüber hinaus ist die Verfahrensregelung zur Sicherungsanordnung aus § 101a Abs. 1 Satz 1 Nr. 3 a) StPO-E iVm § 100g Abs. 7 StPO-E nicht mit Art. 4 Abs. 4 d) EMFA und der Rechtsprechung des EGMR vereinbar.

Die Verfahrensregelung des Entwurfes sieht vor, dass die Staatsanwaltschaft oder ihre Ermittlungspersonen eine Sicherungsanordnung gegenüber einem Telekommunikationsanbieter im Hinblick auf Verkehrsdaten von Journalist:innen auf drei Monate anordnen kann, ohne dass die Anordnung von einem Gericht überhaupt nachträglich

[9] Die Ausnahme aus Art. 4 Abs. 4 d) EMFA setzt u.a. voraus, dass der Überwachungsmaßnahme vorab von einer Justizbehörde oder einem unabhängigen und unparteiischen Entscheidungsgremium zugestimmt worden ist oder, in hinreichend gerechtfertigten und dringenden Ausnahmefällen, **nachträglich unverzüglich** durch eine solche Behörde oder ein solches Gremium genehmigt worden ist.

kontrolliert werden muss. Die gesamte Anordnungsbefugnis des Gerichtes aus § 100e Abs. 1 Satz 3 StPO wird schlicht ersetzt mit einer Anordnungsbefugnis der Staatsanwaltschaft, die dann sogar noch eine Verlängerung der Maßnahme durch das Gericht beantragen kann, wenn sie das möchte. Das ist mit Art. 4 Abs. 4 d) EMFA nicht vereinbar, der bei Gefahr im Verzug mindestens eine unverzügliche, nachträgliche gerichtliche Kontrolle fordert. Im Entwurf ist keine automatische nachgeschaltete Kontrolle vorgesehen. Die nicht überzeugende Begründung auf Seite 41 stellt darauf ab, dass die Daten noch nicht von der Polizei erhoben werden, sondern nur von den Telekommunikationsdiensten gespeichert werden; eine gerichtliche Kontrolle sei daher nicht nötig. Diese Zweistufigkeit ändert nichts daran, dass der Telekommunikationsdienst gesetzlich verpflichtet wäre, nach einer Sicherungsanordnung genaue Verkehrsdaten der Journalist:innen zu speichern und zu sammeln, um sie später der Strafverfolgungsbehörde zur Verfügung zu stellen. Diese Sicherungsanordnung ist aus Sicht des Medienbündnisses bereits eine Überwachungshandlung nach Art. 4 Abs. 3 Satz 2 b) EMFA, da es dafür nicht darauf ankommen kann, ob es für den staatlichen Zugriff zur gesammelten Information noch weiterer Durchsetzungsmaßnahmen bedarf.

Nach Art. 4 Abs. 4 b) EMFA müssen die Ausnahmen außerdem stets mit Artikel 52 Absatz 1 der Charta und anderem Unionsrecht im Einklang stehen. Damit sind auch die Vorgaben des Art. 10 Abs. 2 EMRK einzuhalten. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat in mehreren grundlegenden Urteilen die Reichweite und den Umfang des Schutzes journalistischer Quellen festgelegt.[10]

Eine bloße Anordnungsbefugnis der Staatsanwaltschaft widerspricht dieser Rechtsprechung. Der EGMR führt in diesem Zusammenhang aus, dass das Recht auf Quellenschutz durch Verfahrensgarantien sichergestellt werden müsse, die der Bedeutung dieses Schutzes für die Pressefreiheit entsprächen. 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 könne, vor jeder Offenlegung der Quellen.[11] Obwohl auch der Staatsanwalt an Recht und Gesetz

[10] Case of Goodwin v. The United Kingdom, no. 17488/90, 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."

[11] Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/03, 14.09.2010, Rn. 90: "First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial

gebunden sei, stelle er nach Ansicht des Gerichts jedoch, 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 Stelle angesehen werden, die die notwendige Bewertung der konkurrierenden Interessen vornimmt.[12]

G. Zusammenfassung

Insgesamt fordert das Medienbündnis im Sinne der grundrechtlich verbürgten Presse- und Rundfunkfreiheit, den bisherigen Berufsgeheimnisschutz für Journalist:innen aus dem aktuellen § 100g Abs. 4 StPO für die Verkehrsdatenerhebung aus § 100g Abs. 1, Abs. 5 StPO-E, für die Standortdatenerhebung aus § 100g Abs. 3 StPO-E sowie für die Funkzellenabfrage aus § 100g Abs. 4 StPO-E beizubehalten sowie auf die Nutzungsdatenerhebung bei digitalen Diensten aus § 100k StPO-E zu beziehen. Außerdem sollte der Berufsgeheimnisträgerschutz sich auch auf die Sicherungsanordnung aus § 100g Abs. 7 StPO-E beziehen.

Schließlich müssen die verfahrensrechtlichen Regelungen zur **gerichtlichen** Kontrolle überarbeitet werden, weil sie mit Art. 4 Abs. 4 d) EMFA bzw. der EGMR-Rechtsprechung zum Quellenschutz nicht vereinbar sind.

---

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."

[12] 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."

Kontakt:

Dr. Susanne Pfab
ARD-Generalsekretariat
Masurenallee 8-14
14057 Berlin
Tel: 030/890431311
Susanne.pfab@ard-gs.de

Helmut Verdenhalven
BDZV
Haus der Presse
Markgrafenstraße 15
10969 Berlin
Tel: 030/726298203
verdenhalven@bdzv.de

Dr. Markus Höppener
Deutschlandradio
Raderberggürtel 40
50968 Köln
Tel. 0221/3453500
markus.hoeppener@deutschlandradio.de

Christoph Brill
DJV
Torstr. 49
10119 Berlin
Tel: 030/72627920
brill@djv.de

Bettina Hesse
dju in ver.di
Paula-Thiede-Ufer 10
10179 Berlin
Tel: 030/69562322
Bettina.Hesse@verdi.de

Roman Portack
Deutscher Presserat
Fritschestraße 27/28
10585 Berlin
Tel: 030/3670070
portack@presserat.de

Tim Steinhauer
VAUNET
Stromstraße 1
10555 Berlin
Tel: 030/39880100
steinhauer@vau.net

Prof. Dr. Christoph Fiedler
MVFP
Haus der Presse
Markgrafenstraße 15
10969 Berlin
Tel: 030/726298120
christoph.fiedler@mvfp.de

Felix Mai
ZDF
ZDF-Straße 1
55127 Mainz
Tel: 06131/7014100
Mai.F@zdf.de

Berlin, 30.01.2026