Entscheidungsbesprechung

BVerfG (2. Kammer des Ersten Senats), Beschl. v. 25.11.2025 – 1 BvR 2317/25[1]

DNS-Überwachung

Die auf § 100a StPO gestützte Anordnung, wonach ein Telekommunikationsdienstleister einen DNS-Server überwachen und DNS-Anfragen aufzeichnen soll, wirft erhebliche verfassungsrechtliche Fragen auf. Ihre Umsetzung belastet den Dienstleister nicht nur durch erheblichen organisatorischen, technischen und personellen Aufwand. Sie birgt zudem die Gefahr eines irreparablen Reputationsverlusts, wenn sich die Maßnahme nachträglich als verfassungswidrig herausstellt.

(Leitsätze der *Verf.*)

GG Art. 2 Abs 1, 10 Abs. 1, 12 Abs. 1, 14 Abs. 1
StPO §§ 100a, 100e, 101 Abs. 4
BVerfGG § 32

*RiOLG Prof. Dr. Janique Brüning, Wiss. Mitarbeiter Paul Benk, Kiel**

I. Einführung in die Problematik

Die Strafverfolgung im digitalen Raum ist seit Jahren von einer bemerkenswerten Ermittlungsdynamik geprägt. Wo neue technische Zugriffsmöglichkeiten auf digitale Infrastrukturen entstehen, wächst regelmäßig auch das Strafverfolgungsinteresse, diese für datengetriebene Ermittlungszwecke nutzbar zu machen. Dabei entsteht nicht selten der Eindruck, dass die Strafverfolgungsbehörden in zunehmendem Maße nicht von den gesetzlich normierten Ermittlungsbefugnissen her denken, sondern von der kriminalistischen Erwartung, möglichst alle verfügbaren Daten(ströme) auswerten zu können. Die jüngere Diskussion um die zwangsweise biometrische Entsperrung von Mobiltelefonen[2] hat bereits gezeigt, wie rasch sich ein „rechtlicher Innovationsdruck" entfalten kann, wenn digitale Beweismittel für die Ermittlungen attraktiv erscheinen. Mit Hilfe des Begriffs der Technologieoffenheit werden Ermittlungspraktiken in den bestehenden Rechtsrahmen hineininterpretiert, auch wenn dies mit Wortlaut und Telos nur schwer zu vereinbaren ist.

* Die Verf. Prof. *Dr. Janique Brüning* ist Inhaberin der Professur für Strafrecht, Strafprozessrecht, Wirtschaftsstrafrecht und Sanktionenrecht an der Christian-Albrechts-Universität zu Kiel und Richterin am Schleswig-Holsteinischen Oberlandesgericht. Der Verf. *Paul Benk* ist Wiss. Mitarbeiter an der genannten Professur.

[1] Die Entscheidung ist veröffentlicht u.a. in BeckRS 2025, 33604 und NVwZ 2026, 317.

[2] Die zwangsweise biometrische Entsperrung von Mobiltelefonen ist deshalb rechtlich nicht ganz unproblematisch, weil sie die Grenze zwischen bloßer Duldung körperlicher Identifizierungsmaßnahmen und erzwungener Mitwirkung an der Erschließung eines hochpersönlichen digitalen Datenbestands verwischt und damit die Tragfähigkeit von § 81b Abs. 1 StPO als Ermächtigungsgrundlage in Frage stellt. Dies gilt insbesondere, wenn man bedenkt, dass auf diese Weise mit der vergleichsweisen niederschwelligen erkennungsdienstlichen Vorschrift des § 81b StPO der Zugang auf das gesamte digitale Leben des Beschuldigten ermöglicht wird. Dazu BGH, Beschl. v. 13.3.2025 – 2 StR 232/24 = NJW 2025, 2265; zur berechtigten Kritik vgl. die Anmerkungen von *Eckstein*, ZfIStw 6/2025, 712 ff.; *Cornelius*, NJW 2025, 2265 (2270 f.); *Satzger/Sarfraz*, NStZ 2025, 560 (566); *El-Ghazi*, NJW 2025, 847 (850); dazu auch in dieser Ausgabe die Besprechung von *Jansen*, ZJS 2026, 479.

Bereits mit den Trojaner-I-[3] und Trojaner-II[4]-Entscheidungen des BVerfG ist die Tendenz zu beobachten, dass die digitale Strafverfolgung nicht durch funktionale Ausdehnung vorhandener Eingriffsnormen, sondern nur auf der Grundlage hinreichend bestimmter, eingriffsspezifischer Ermächtigungen erfolgen darf.

Dass dies inzwischen auch gesetzgebungspolitisch anerkannt ist, zeigt der Referentenentwurf zur Änderung der Strafprozessordnung betreffend digitale Ermittlungsmaßnahmen[5], der selbst von einem Fehlen ausdrücklicher Ermächtigungsgrundlagen für neue digitale Analyse- und Abgleichmaßnahmen ausgeht.

Vor diesem Hintergrund betrifft die hier zu besprechende Entscheidung des BVerfG einen weiteren Grenzfall digitaler Strafverfolgung. Das AG Oldenburg verpflichtete – gestützt auf §§ 100a, 100e StPO – einen großen Telekommunikationsdiensteanbieter (Vodafone), sämtliche DNS-Anfragen seiner etwa 40 Millionen Kundinnen und Kunden zu einem mutmaßlich inkriminierten Server zu überwachen, aufzuzeichnen und nebst Bestandsdaten an die Ermittlungsbehörden weiterzuleiten. Nach Angaben der Beschwerdeführerin betraf dies etwa 12,96 Billionen DNS-Anfragen pro Monat. Das BVerfG musste im einstweiligen Rechtsschutzverfahren prüfen, ob der Vollzug der Maßnahme bis zur Entscheidung in der Hauptsache vorläufig auszusetzen ist.

Um die hierzugrundeliegende Problematik besser nachvollziehen zu können, wird ein kurzer Überblick zum Eilverfahren nach § 32 BVerfGG gegeben (1.). Daran schließt sich die Erläuterung über die Funktionsweise einer DNS-Abfrage (2.) sowie ein kurzer Überblick über die strafprozessualen Ermittlungsmaßnahmen, die im Zusammenhang mit der Telekommunikationsüberwachung stehen (3.).

1. Das Eilverfahren gem. § 32 BVerfGG

Das Bundesverfassungsgericht kann durch eine einstweilige Anordnung nach § 32 BVerfGG einen Zustand vorläufig regeln, wenn dies zur Abwendung schwerer Nachteile zur Verhinderung drohender Gewalt oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist. Regelmäßig entscheidet das BVerfG aufgrund eines Antrags, es kann aber auch eine Anordnung von Amts wegen treffen, wenn bereits ein Hauptsacheverfahren anhängig ist.[6] Im Falle der Verfassungsbeschwerde entscheidet im Eilverfahren nicht der Senat, sondern eine Kammer in einer Besetzung von drei Richter*innen, vgl. § 94d Abs. 2 BVerfGG, § 15a Abs. 1 S. 1, 2 BVerfGG.

Es ergibt sich folgender Prüfungsaufbau für eine Anordnung nach § 32 BVerfGG:

I. Zulässigkeit
   1. Zuständigkeit des BVerfG
   2. Antrag
   3. Antragsfähigkeit
   4. Keine Unzulässigkeit des Hauptsacheverfahrens
   5. Keine offensichtliche Unbegründetheit des Hauptsacheverfahrens
   6. Keine Vorwegnahme der Hauptsache
   7. Form, § 23 BVerfGG

[3] BVerfG BeckRS 2025, 19412.

[4] BVerfG BeckRS 2025, 19413.

[5] Abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Digitale_Ermittlungsmaßnahmen.pdf?__blob=publicationFile&v=2 (19.3.2026).

[6] *Sodan/Ziekow*, Grundkurs Öffentliches Recht, 10. Aufl. 2023, § 57 Rn. 4.

II. Begründetheit
1. Besondere Eilbedürftigkeit
2. Folgenabwägung
a) Folgen bei unterbliebener Anordnung und Erfolg der Hauptsache
b) Folgen bei Erlass der Anordnung und Erfolglosigkeit der Hauptsache
c) Abwägung

a) Zulässigkeit

Die Zulässigkeit dieses Antrags richtet sich im Wesentlichen nach den Zulässigkeitsanforderungen des Hauptsacheverfahrens. Im Falle einer Verfassungsbeschwerde gem. Art. 94 Abs. 1 Nr. 4a GG muss also das BVerfG in der Hauptsache das zuständige Gericht sein, vgl. § 13 Nr. 8a BVerfGG. Die Antragsberechtigung richtet sich nach der Beteiligtenfähigkeit am Verfahren in der Hauptsache (im Falle der Verfassungsbeschwerde: „jedermann", Art. 94 Abs. 1 Nr. 4a GG, § 13 Nr. 8a BVerfGG, § 90 Abs. 1 BVerfGG). Weitere Zulässigkeitsvoraussetzungen sind, dass das Verfahren in der Hauptsache nicht unzulässig oder offensichtlich unbegründet ist und dass durch die Anordnung das Verfahren in der Hauptsache nicht vorweggenommen wird.[7] Der Antrag muss schriftlich gestellt und begründet werden, vgl. § 23 Abs. 1 BVerfGG.

b) Begründetheit

Die Begründetheit des Antrags setzt zunächst eine besondere Eilbedürftigkeit voraus.[8] § 32 Abs. 1 BVerfGG spricht von der Abwehr schwerer Nachteile, der Verhinderung von Gewalt oder anderen wichtigen Gründen.

Im Übrigen haben bei „[…] der Entscheidung über die einstweilige Anordnung […] die Gründe, die für die Verfassungswidrigkeit der mit der Verfassungsbeschwerde angegriffenen Maßnahmen vorgetragen werden, grundsätzlich außer Betracht zu bleiben […]"[9]. Das heißt, dass anders als z.B. beim einstweiligen Rechtsschutz gem. § 80 Abs. 5 VwGO keine (summarische) Prüfung der Erfolgsaussichten in der Hauptsache erfolgt.[10] Stattdessen richtet sich die Begründetheit nach einer bloßen Folgenabwägung in Form der sog. Doppel-Hypothese.[11] Das BVerfG nimmt also zwei hypothetische Folgenabwägungen vor: In einem ersten Schritt prüft es die Folgen, die eintreten würden, wenn die einstweilige Anordnung nicht erginge, das Verfahren in der Hauptsache aber Erfolg hätte.[12] Im zweiten Schritt prüft es die Folgen die sich ergäben, wenn die Anordnung erlassen würde, das Verfahren in der Hauptsache aber keinen Erfolg hätte.[13] In einem dritten Schritt werden diese hypothetischen Folgen miteinander abgewogen. Überwiegen die Nachteile für den Antragssteller bei dieser Abwägung ist der Antrag begründet und die Anordnung wird erlassen.[14]

---

[7] *Sodan/Ziekow*, Grundkurs Öffentliches Recht, 10. Aufl. 2023, § 57 Rn. 7 ff.
[8] *Sodan/Ziekow*, Grundkurs Öffentliches Recht, 10. Aufl. 2023, § 57 Rn. 13.
[9] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 10.
[10] *Walter*, in: BeckOK BVerfGG, Stand: 1.12.2025, § 32 Rn. 49.
[11] *Walter*, in: BeckOK BVerfGG, Stand: 1.12.2025, § 32 Rn. 48.
[12] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 16.
[13] Vgl. BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 17.
[14] Vgl. BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.

2. Was ist das Domain-Name-System (DNS) und wie funktioniert es?

a) Verbindungherstellung im Internet

Möchte eine Person auf Inhalte aus dem Internet, also beispielsweise auf eine Website zugreifen, so tippt man dafür regelmäßig die Adresse der Website, die Domain, in seinen Browser ein. Gibt jemand „www.uni-kiel.de“ im Browser seiner Wahl ein, dann kann der Computer damit grundsätzlich nichts anfangen, denn Computer im Internet kommunizieren über Internet-Protocol-Adressen (IP-Adressen), die ausschließlich aus Zahlenkombinationen bestehen (z.B. 192.168.1.38). Um zu diesem Server eine Verbindung herstellen und dessen Inhalte abrufen zu können, brauchen Computer also zwingend die IP-Adresse des Servers, auf den zugegriffen werden soll. Domainnamen sind nur für Menschen lesbare Bezeichnungen, die zunächst in eine IP-Adresse übersetzt werden müssen, bevor eine Verbindung aufgebaut werden kann. Domains sind dabei immer hierarchisch aufgebaut:

Eine Domain besteht am rechten Ende immer aus einem Top-Level, welches den (von links nach rechts gelesen) letzten Teil der Domain nach dem Punkt beschreibt, also „de“, „com“, u.s.w. Die Vergabe von Top-Level-Domains ist zentral organisiert; neue Top-Level-Domains können nicht beliebig durch Einzelne geschaffen werden.

Liest man eine Internetadresse von rechts nach links, folgt nach dem Top-Level zunächst das Second-Level – in unserem Beispiel „uni-kiel“. Es können sich noch beliebig viele weitere Sub-Level anschließen. Diese Level sind durch einen Punkt getrennt.

Menschen kennen aber nur Domain-Namen, aber nicht die dazugehörigen IP-Adressen. Das bedeutet, dass die Domain in die dazugehörige IP-Adresse übersetzt werden muss, sonst funktioniert „das Internet“, so wie wir es heute kennen, nicht.

b) Die Rolle des DNS

aa) Grundsätzliches[15]

Das Domain-Name-System (DNS) wurde entwickelt, um eine Domain automatisch in die zugehörige IP-Adresse zu übersetzen, ohne dass der Mensch sich lange Zahlenfolgen merken muss. Das DNS funktioniert gewissermaßen wie ein Telefonbuch: man kennt den Namen einer Person, aber nicht die dazugehörige Telefonnummer.[16]

Diese Übersetzung funktioniert mithilfe eines sog. DNS-Resolvers. Das ist ein Server, der meistens von dem jeweiligen Internetanbieter zur Verfügung gestellt wird und der in der Lage ist, Anfragen an andere Server zu stellen, die ein Verzeichnis über Domainnamen und dazugehörige IP-Adressen führen.

Der Resolver-Server kommuniziert also in zwei Richtungen: erstens erhält er vom Computer, der die IP-Adresse für eine Domain anfragt, die besagte Anfrage und soll diese beantworten. Hierfür kommuniziert er zweitens mit einem Netzwerk von Servern, deren alleinige Aufgabe es ist, Informationen darüber bereit zu stellen, welche IP-Adresse welchem Domainnamen zugeordnet ist.

Dieses Netzwerk von Servern ist hierarchisch aufgebaut, weshalb die Kommunikation zwischen Resolver und DNS-Servern immer nach dem gleichen Schema abläuft: die ersten Server in der Hierarchie helfen dem Resolver nur dabei, den zuständigen autoritativen Nameserver ausfindig zu machen, der die gesuchte IP-Adresse kennt. Die Hierarchie der Server spiegelt dabei den Aufbau der Domain wider. An der Spitze steht ein Root-Server, der die IP-Adressen aller sog. Top-Level-Domain-Server

[15] Eine ausführliche Darstellung findet sich auch bei *Heine*, in: MüKo-BGB, Bd. 1, 10. Aufl. 2025, § 12 Rn. 232 ff.
[16] Vgl. BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 15.

(TLD-Server) kennt. Diese wiederum kennen dann die entsprechenden autoritativen Nameserver, oder – falls die Domain weitere Sub-Level enthält – die den Sub-Leveln entsprechenden Server.

Die Root-Server werden von verschiedenen international tätigen Organisationen an unterschiedlichen Orten weltweit betrieben. Entsprechendes gilt für die Nameserver der Top-Level-Domains. Die autoritativen Nameserver einzelner Domains werden hingegen regelmäßig von den Domaininhabern selbst oder von diesen beauftragten technischen Dienstleistern (z.B. Cloudflare) betrieben. Die DNS-Resolver werden typischerweise von Internetzugangsanbietern oder spezialisierten Drittunternehmen betrieben. Bei den meisten Internetnutzer*innen sind diese Resolver voreingestellt und werden vom jeweiligen Internetanbieter bereitgestellt.

DNS-Anfragen enthalten den vollständigen Domainnamen sowie die IP-Adresse des anfragenden Geräts. Werden sie protokolliert, entstehen zusätzlich Zeitstempel. DNS-Daten erlauben also Rückschlüsse darauf, welche konkreten Domains oder Subdomains kontaktiert wurden. Subdomains wie „www.cloud.uni-kiel.de“ sind vollständig sichtbar, weil das DNS stets den konkret angefragten vollständigen Domainnamen auflöst. Wird etwa „www.cloud.uni-kiel.de“ angefragt, so ist genau diese Subdomain in der DNS-Anfrage sichtbar. Nicht erfasst werden dagegen Unterseiten. Ob eine Person nur „www.uni-kiel.de“oder nur „www.uni-kiel.de/studium/bewerbung“ aufruft, ist aus der DNS-Anfrage nicht ersichtlich, da dieser Zugriff auf Unterseiten erst nach erfolgter Domainauflösung über HTTP bzw. HTTPS stattfindet.

Wie oben bereits angedeutet, wäre die Internetnutzung in ihrer heutigen Form ohne DNS nicht möglich. Nicht nur der Zugriff auf Websites funktioniert durch das DNS, sondern u.a. auch das Versenden von E-Mails.

In seinem Beschluss verdeutlicht das BVerfG die Dimension der bei einer DNS-Abfrage anfallenden Daten. Das Gericht geht davon aus, dass allein die Kundinnen und Kunden der Beschwerdeführerin innerhalb eines Monats ca. 12,96 Billionen Anfragen an den DNS-Resolver von Vodafone senden.[17] Würden diese Anfragen alle aufgezeichnet, ließe sich nicht nur nachvollziehen für welche Domains wie viele Anfragen innerhalb eines bestimmten Zeitraums eingegangen sind. Da auch die IP-Adresse des anfragenden Anschlusses oder des Geräts gespeichert wird, wäre es sogar möglich aus den Aufzeichnungen abzuleiten, welcher Anschluss bzw. welches Gerät zu welchem Zeitpunkt welche Websites besucht hat.

bb) Ablauf einer DNS-Abfrage

Den Ablauf einer DNS-Abfrage muss man sich nun wie folgt vorstellen:[18]

Schritt 1:[19] Der*die Nutzer*in gibt die Domain „www.uni-kiel.de“ in seinen Browser ein. Der Computer sendet daraufhin eine DNS-Anfrage an einen vorkonfigurierten rekursiven DNS-Resolver, der meistens vom Internetprovider zur Verfügung gestellt wird. Der Router leitet diese lediglich weiter. Der Computer beauftragt durch diese DNS-Anfrage den Resolver sinngemäß, die zugehörige IP-Adresse herauszufinden (sinngemäß: „Hallo Resolver! Wie lautet die IP-Adresse für die Domain www.uni-kiel.de?“). Diese Anfrage ist rekursiv, das heißt der Computer erwartet eine vollständige Antwort auf die Frage nach der IP-Adresse. Dazu durchsucht der Resolver zunächst seinen Cache

[17] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 15.

[18] Die nachfolgende Darstellung ist technisch vereinfacht und beschränkt sich auf die für das Verständnis der Entscheidung wesentlichen technischen Prozesse. Insbesondere die Fragen und Antworten der Server in der Schritt-für-Schritt Darstellung dienen ausschließlich der Illustration des Ablaufs der DNS-Auflösung.

[19] Bitte vgl. Sie zum besseren Verständnis der einzelnen Schritte die jeweiligen Nrn. des im Anhang befindlichen Schaubilds.

(also den Zwischenspeicher), um festzustellen, ob die zur Domain gehörige IP-Adresse aufgrund einer früheren Anfrage noch gespeichert ist. Ist dies nicht der Fall, folgt *Schritt 2*.

Schritt 2: Ist die IP-Adresse nicht im Cache gespeichert, so kommuniziert der Resolver schrittweise mit den nachgelagerten DNS-Servern der oben beschriebenen Hierarchie. Dabei liefert jeder angefragte Server keine vollständige Antwort, sondern verweist lediglich auf den nächsten zuständigen Server. Das bedeutet, die Anfrage wird von Server zu Server weitergereicht, bis die gesuchte IP-Adresse gefunden ist. Dieser Ablauf gestaltet sich wie folgt:

Schritt 3: Der erste angefragte Server ist der sog. Root-Server. Er kennt zwar keine IP-Adressen von Websites, wohl aber die IP-Adressen der Server, die für die jeweiligen Top-Level-Domains zuständig sind. Der Resolver fragt den Root-Server sinngemäß: „Wie lautet die IP-Adresse für www.uni-kiel.de?“

Schritt 4: Hierauf teilt der Root-Server dem anfragenden DNS-Resolver mit, welcher Server für die Top-Level-Domain „de“ zuständig ist, und übermittelt dessen IP-Adresse. Der Root-Server antwortet also sinngemäß: „Ich kenne die IP-Adresse nicht. Frag mal beim de-Server nach, der kann dir weiterhelfen!“

Schritt 5: Da der DNS-Resolver nun weiß, welcher Server für „de“ zuständig ist, fragt er diesen Server, welcher autoritative Nameserver für das Second-Level „uni-kiel“ zuständig ist. Der Resolver fragt den TLD-Server sinngemäß: „Wie lautet die IP-Adresse für www.uni-kiel.de?“

Schritt 6: Dieser Top-Level-Domain-Server schickt dem Resolver eine Antwort in Form der IP-Adresse des autoritativen Nameservers für die konkrete Domain „uni-kiel.de“. Der TLD-Server antwortet also sinngemäß: „Ich kenne die IP-Adresse nicht. Frag mal beim uni-kiel-Server nach, der kann dir weiterhelfen!“

Schritt 7: Nun fragt der Resolver bei diesem autoritativen Nameserver der Domain „uni-kiel.de“ die IP-Adresse für die Domain an. Der Resolver fragt den Root-Server sinngemäß: „Wie lautet die IP-Adresse für www.uni-kiel.de?“

Schritt 8: Bei diesem Server schließlich erhält der Resolver als Antwort keine weitere Zuständigkeitsantwort, sondern eine IP-Adresse für die Domain „www.uni-kiel.de“. Die iterative Anfrage ist damit beendet. Der autoritative Nameserver antwortet also sinngemäß: „Ich kenne die IP-Adresse. Sie lautet 123.456.7.89!“

Schritt 9: Der Resolver kann die nun bekannte IP-Adresse für die Domain über den Router an den Computer weiterleiten und damit die rekursive Anfrage beantworten. Er antwortet dem Computer auf dessen Frage in Schritt 1 sinngemäß: „Hallo Computer! Ich habe die IP-Adresse für www.uni-kiel.de herausgefunden – sie lautet 123.456.7.89!“

Schritt 10: Erst mit der erhaltenen IP-Adresse kann der Computer über den Router eine Verbindung zum hostenden Server aufbauen – regelmäßig verschlüsselt über HTTPS – und dessen Inhalte abrufen. Der Server sendet die entsprechenden Datenpakete, die der Computer zusammensetzt und anzeigt. Ein behördlicher Zugriff auf diese Datenübertragung ist nach vom BVerfG bestätigter Rechtsprechung an § 100a Abs. 1 S. 1 StPO zu messen.[20]

c) Wie wäre die DNS-Überwachung technisch umzusetzen?

Nachdem die Ermittler einen Server ausfindig gemacht haben, auf welchem mutmaßlich regelmäßig strafrechtsrelevante Inhalte veröffentlicht und abgerufen werden, soll die übliche Ermittlungsrichtung umgedreht werden: anstatt vom Inhalt auf die Person zu schließen, soll überwacht werden, wer zu welchem Zeitpunkt auf die Website zugegriffen hat, und zwar, indem die DNS-Daten durch die

[20] BVerfG NJW 2016, 3508 (3510); *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 126. Zur nicht ganz unberechtigten Kritik *Heinrich*, ZIS 2020, 421 ff.

Beschwerdeführerin ausgeleitet werden. Die den DNS-Server betreibende Beschwerdeführerin soll alle an diesen DNS-Resolver gerichteten DNS-Anfragen der Kund*innen überwachen und diejenigen samt Zeitstempel und IP-Adresse herausfiltern, die sich auf die Domain mit den mutmaßlich inkriminierten Inhalten beziehen. Diese Daten soll die Beschwerdeführerin sodann samt den Bestandsdaten an die Ermittlungsbehörden herausgeben, sodass diese erkennen können, welche Person bzw. über welchen Anschluss zu welchem Zeitpunkt auf die Website zugegriffen hat. Müsste die Beschwerdeführerin den Beschluss des AG Oldenburg, der mit der Verfassungsbeschwerde angegriffen wurde, umsetzen, so ist denkbar, dass alle Anfragen aller Nutzer*innen, die den DNS-Resolver der Beschwerdeführerin nutzen, geloggt, also zwischengespeichert und ausgewertet werden. Andererseits könnte auch eine laufende Analyse der Anfragen ohne Zwischenspeicherung erfolgen – hierfür müssen ebenfalls sämtliche Anfragen analysiert werden, allerdings werden nur diejenige mit den relevanten Daten gespeichert, die eine DNS-Anfrage für die inkriminierte Website enthalten.

An der Geeignetheit der Maßnahme könnten allerdings leise Zweifel angemeldet werde. So ist es durch den Einsatz von VPN oder Tor[21] möglich, dass Nutzer*innen keine Anfrage mehr an den Resolver des Internetanbieters stellen, und sich auf diese Weise der Überwachung durch die Beschwerdeführerin entziehen. Denkbar ist auch die Nutzung eines anderen Resolvers als dem des Internetanbieters. In allen diesen Fällen laufen DNS-Anfragen nicht mehr über den Resolver des Internetanbieters, sodass er die Anfragen auch nicht auswerten kann. Es ist wohl davon auszugehen, dass zumindest ein Großteil, die auf die inkriminierte Website zugreifen wollen, solche Vorsichtsmaßnahmen treffen werden.[22]

3. Ermittlungsmaßnahmen im Zusammenhang mit der Telekommunikation – ein skizzenhafter Überblick

Ermittlungsmaßnahmen, die auf Telekommunikation, digitale Dienste oder informationstechnische Systeme zugreifen, greifen in besonders geschützte Freiheitsräume ein. Dazu bedürfen sie einer gesetzlichen Ermächtigungsgrundlage. Die StPO enthält in §§ 100a, 100b, 100g, 100i, 100j und 100k ein abgestuftes System telekommunikationsbezogener Ermittlungsmaßnahmen. Welche Ermächtigungsgrundlage einschlägig ist, richtet sich vor allem danach, ob auf Inhalts-, Bestands-, Verkehrs- oder Nutzungsdaten zugegriffen wird und ob die Maßnahme laufende Kommunikation, bloße Kommunikationsumstände oder den Zugriff auf ein informationstechnisches System betrifft. Verfassungsrechtlich ist dabei zu unterscheiden: Die Überwachung laufender Telekommunikation ist in erster Linie am Fernmeldegeheimnis des Art. 10 Abs. 1 GG zu messen. Der Zugriff auf gespeicherte Daten oder die Infiltration eines Endgeräts berührt demgegenüber vor allem das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme (sog. IT-System-Grundrecht[23]) aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[24] Das Bundesverfassungsgericht geht dabei nicht mehr von einem strikten Entweder–Oder aus, sondern hält eine gleichzeitige Betroffenheit beider Grundrechte für möglich.[25] Werden die erhobenen Daten anschließend automatisiert analysiert oder ausgewertet, ist darüber hinaus auch das Recht auf informationelle Selbstbestimmung betroffen, weil die automatisierte Weiterverarbeitung einen eigenständigen zusätzlichen Grundrechtseingriff begründet.[26]

---

[21] Das Tor-Netzwerk anonymisiert die Nutzer*innen des Netzwerks durch Verschlüsselung und Verschleierung, vgl. die Erklärung bei *Krause*, NJW 2018, 678.

[22] Hierbei handelt es sich um eine persönliche Einschätzung der *Verf*.

[23] Die bisher gängige Abkürzung „IT-Grundrecht" wurde nun zum „IT-System-Grundrecht", so bereits *Rückert,* Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 5.

[24] *Ostendorf/Brüning*, Strafprozessrecht, 5. Aufl. 2024, § 11 Rn. 53.

[25] BVerfG BeckRS 2025, 19413 Rn. 174, 241 (Trojaner II).

[26] BVerfGE 165, 363 (388).

a) § 100a Abs. 1 S. 1 StPO

Den Ausgangspunkt der TKÜ-Maßnahmen bildet § 100a StPO. Die Vorschrift erlaubt vor allem die Überwachung und Aufzeichnung laufender Telekommunikationsinhalte und greift damit in Art. 10 Abs. 1 GG ein. Erfasst sind insbesondere Telefonate, E-Mails, Messenger-Kommunikation und Internettelefonie, aber auch Begleitumstände der konkret überwachten Kommunikation wie etwa die beteiligten Anschlüsse, Zeitpunkt und Dauer. Die Eingriffsschwelle ist hoch: Erforderlich sind bestimmte Tatsachen, die den Verdacht einer in § 100a Abs. 2 StPO abschließend aufgeführten schweren Katalogtat begründen. Außerdem muss die Aufklärung oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein. Hinzu treten Richtervorbehalt, Befristung und qualifizierte Begründungsanforderungen. § 100a StPO ist damit auf die Überwachung eines bereits konkretisierten Kommunikationsvorgangs zugeschnitten.

b) § 100a Abs. 1 S. 2, 3 StPO

Von der klassischen Telekommunikationsüberwachung ist die Quellen-TKÜ nach § 100a Abs. 1 S. 2 und 3 StPO zu unterscheiden. Auch sie knüpft an Telekommunikation an, setzt technisch aber einen heimlichen Zugriff auf das Endgerät voraus. Gerade deshalb geht das BVerfG für die Quellen-TKÜ bei Zugriff auf ein eigengenutztes IT-System nicht mehr von einem bloßen Entweder–Oder zwischen Art. 10 Abs. 1 GG und dem IT-System-Grundrecht aus. Vielmehr könnten beide Grundrechte gleichzeitig betroffen sein. Insoweit ist zwischen § 100a Abs. 1 S. 2 und 3 StPO zu unterscheiden. § 100a Abs. 1 S. 2 StPO betrifft die Überwachung laufender Telekommunikation an der Quelle und greife – so das BVerfG in der sog. Trojaner-II-Entscheidung – sowohl in das Fernmeldegeheimnis als auch in das IT-System-Grundrecht ein.[27] § 100a Abs. 1 S. 3 StPO erlaube demgegenüber den Zugriff auf bereits auf dem Gerät gespeicherte Kommunikationsinhalte und -umstände, die ab Anordnung auch während des laufenden Übertragungsvorgangs hätten erhoben werden können. Maßgeblich sei insoweit vor allem das IT-System-Grundrecht.[28] Wegen des erheblichen Eingriffsgewichts hat das BVerfG beide Vorschriften für teilweise verfassungswidrig erklärt, soweit sie auch an Straftaten des einfachen Kriminalitätsbereichs anknüpfen.[29]

c) § 100b StPO

Noch weiter reicht § 100b StPO. Die Vorschrift erlaubt die Online-Durchsuchung, also den verdeckten Zugriff auf ein informationstechnisches System insgesamt. Anders als § 100a StPO beschränkt sie sich nicht auf die laufende Kommunikation, sondern eröffnet den Zugriff auf gespeicherte Datenbestände und auf das IT-System in seiner ganzen Breite. Maßgeblicher verfassungsrechtlicher Bezugspunkt ist deshalb vor allem das IT-System-Grundrecht.[30] Das BVerfG hat jedoch auch hier festgestellt, dass daneben auch Art. 10 Abs. 1 GG betroffen sein könne, wenn die Online-Durchsuchung auch die laufende Telekommunikation erfasse.[31] § 100b Abs. 1 StPO sei deshalb wegen Verstoßes gegen das Zitiergebot des Art. 19 Abs. 1 S. 2 GG formell verfassungswidrig, wirke aber bis zu einer Neuregelung fort.[32]

---

[27] BVerfG BeckRS 2025, 19413 Rn. 172 (Trojaner II).

[28] BVerfG BeckRS 2025, 19413 Rn. 220 ff. (Trojaner II) – zwar sei auch das Recht auf informationelle Selbstbestimmung betroffen, dieses trete aber hinter dem IT-System-Grundrecht zurück, Rn. 222, 225.

[29] BVerfG BeckRS 2025, 19413 Rn. 270 (Trojaner II).

[30] Vgl. BVerfG BeckRS 2025, 19413 Rn. 242 (Trojaner II).

[31] BVerfG BeckRS 2025, 19413 Rn. 243 (Trojaner II).

[32] BVerfG BeckRS 2025, 19413 Rn. 271, 275 (Trojaner II).

d) § 100g StPO

Neben diesen Befugnissen kennt die StPO Ermächtigungen, die ausschließlich den Zugriff auf Kommunikationsumstände erlauben. Zentrale Vorschrift ist § 100g StPO. Sie betrifft Verkehrsdaten, also die äußeren Umstände der Kommunikation, etwa Zeitpunkt, Dauer, beteiligte Anschlüsse, IP-Bezüge oder Standortdaten. Die Norm erlaubt damit nicht die Einsicht in Kommunikationsinhalte, wohl aber die Rekonstruktion von Kommunikationsbeziehungen und Bewegungsbildern. Auch insoweit ist der Schutzbereich des Art. 10 Abs. 1 GG betroffen.[33]

§ 100g Abs. 1 StPO bildet den Grundfall des gezielten Zugriffs auf Verkehrsdaten eines bestimmten Anschlusses. Zulässig ist die Maßnahme, wenn bestimmte Tatsachen den Verdacht einer Straftat von erheblicher Bedeutung begründen oder wenn eine Straftat mittels Telekommunikation begangen wurde. Demgegenüber betrifft § 100g Abs. 2 StPO besonders eingriffsintensive, rückwirkend auswertbare Verkehrsdaten, vor allem solche, aus denen sich aussagekräftige Bewegungs- und Kontaktprofile erstellen lassen. Deshalb verlangt Abs. 2 den Verdacht einer besonders schweren Straftat aus einem gesetzlichen Katalog. Praktisch läuft Abs. 2 derzeit allerdings weitgehend leer, soweit er an Daten anknüpft, die nur aufgrund einer allgemeinen – für rechtswidrig erklärten – Vorratsdatenspeicherung verfügbar wären.[34] § 100g Abs. 3 StPO regelt die Funkzellenabfrage. Bei ihr werden für einen bestimmten Ort und Zeitraum sämtliche Mobiltelefone erfasst, die in einer Funkzelle eingeloggt waren. Die Maßnahme streut daher besonders weit und betrifft typischerweise auch eine Vielzahl unbeteiligter Dritter. Der BGH verlangt daher auch für die Funkzellenabfrage den Verdacht einer Katalogtat i.S.d. § 100g Abs. 2 StPO.[35]

e) §§ 100k, 100j, 100i StPO

Mit § 100k StPO hat der Gesetzgeber die Struktur des § 100g StPO auf digitale Dienste erweitert. Die Vorschrift betrifft Nutzungsdaten digitaler Dienste, also etwa Daten über die Nutzung sozialer Netzwerke, Suchmaschinen oder Internetforen.

Davon zu unterscheiden ist die Bestandsdatenauskunft nach § 100j StPO. Sie dient vor allem der Identifizierung, etwa der Zuordnung eines Anschlusses oder einer IP-Adresse zu einer bestimmten Person. Anders als § 100g StPO oder § 100k StPO zielt § 100j StPO nicht auf die Rekonstruktion eines Kommunikations- oder Nutzungsverhaltens, sondern auf die Feststellung, wer hinter einem Anschluss oder Nutzer*innenkonto steht.

Noch einmal anders gelagert ist schließlich § 100i StPO. Die Norm erlaubt insbesondere den Einsatz eines IMSI-Catchers zur Ermittlung von Geräte- und Kartennummern sowie zur Standortbestimmung. Inhaltlich geht es damit weder um Kommunikationsinhalte noch um einen den Nutzer*innen bewusst veranlassten Informationsaustausch, sondern um die technische Identifizierung eines Mobilfunkendgeräts und die Erfassung seiner Einbuchung in das Mobilfunknetz.

f) Das Doppel-Tür-Modell und das Eigengewicht der automatisierten Datenanalyse

Zu beachten ist ferner, dass sowohl die Speicherung der Daten durch das Telekommunikationsunternehmen als auch der Abruf der Daten durch die Strafverfolgungsbehörden jeweils einer hinrei-

[33] BVerfGE 130, 151 (179).

[34] Zur Vorratsdatenspeicherung: BVerwG NJW 2024, 98; EuGH NJW 2024, 2099.

[35] BGH NJW 2024, 2336; zustimmend *Singelnstein*, NJW 2024, 2336 (2339 f.); a.A. LG Hamburg MMR 2025, 154; *Kienle*, NZWiSt 2024, 261 (266 f.); *Nettersheim*, NStZ 2024, 557 (560 ff.).

chend bestimmten gesetzlichen Grundlage bedürfen (sog. Doppel-Tür-Modell).[36] Und schließlich ist auch darauf zu achten, dass neben der Datenerhebung die anschließende automatisierte Auswertung ebenfalls als eigenständiger Grundrechtseingriff zu begreifen ist, der gesondert gesetzlich zu regeln ist. Insoweit ist darauf hinzuweisen, dass das BVerfG 2023 zur automatisierten Datenanalyse hervorgehoben hat, dass die Weiterverarbeitung bereits erhobener Daten ein „Eigengewicht“ [37] besitzt, weil sie zusätzliche Belastungseffekte erzeugen und je nach Datenbestand und Analysemethode ein gegenüber der bloßen Erhebung gesteigertes Eingriffsgewicht entfalten kann und einen Eingriff in die informationelle Selbstbestimmung darstellt (siehe oben).

g) Rechtsschutz gegen telekommunikationsbezogene Ermittlungsmaßnahmen

Auch der Rechtsschutz gegen telekommunikationsbezogene Ermittlungsmaßnahmen ist durch deren Heimlichkeit strukturell erschwert. Dabei ist zwischen den Rechtsschutzmöglichkeiten der Betroffenen und denen der in Anspruch genommenen Anbieter zu unterscheiden.

Aufgrund der Heimlichkeit der Maßnahme ist vorbeugender Rechtsschutz durch die von der Maßnahme betroffenen Personen ausgeschlossen. Nachträglicher Rechtsschutz kommt zwar grundsätzlich über die Beschwerde nach § 304 StPO in Betracht, setzt aber voraus, dass die Betroffenen überhaupt Kenntnis von der Maßnahme erlangen. Daran fehlt es häufig. Zwar sieht § 101 Abs. 1 StPO eine Benachrichtigung vor. Diese kann jedoch nach § 101 Abs. 4 S. 1 Nr. 3, S. 4 und 5 StPO zurückgestellt werden oder unterbleiben. Bei Maßnahmen mit einer großen Anzahl von Betroffenen – etwa einer DNS-Server-Überwachung – dürfte eine individuelle Benachrichtigung praktisch ausgeschlossen sein, sodass der Rechtsschutz faktisch von der Medienberichterstattung abhinge.[38]

Dem in Anspruch genommenen Telekommunikationsanbieter steht grundsätzlich die Beschwerde nach § 304 StPO zu, jedoch nur zur Wahrung eigener Rechte. Er kann nicht das Fernmeldegeheimnis der betroffenen Nutzer*innen prozessual geltend machen, sondern lediglich Eingriffe in die eigene Rechtssphäre rügen, insbesondere in seine Berufsausübungsfreiheit aus Art. 12 Abs. 1 GG. Dementsprechend ist er darauf beschränkt, die fehlenden gesetzlichen Voraussetzungen seiner Inanspruchnahme geltend zu machen, etwa nach § 100a Abs. 4 StPO, § 2 G 10 oder § 170 TKG. Eine inhaltliche Überprüfung der Überwachungsanordnung im Interesse der Betroffenen ist ihm hingegen mit Hilfe der strafprozessualen Rechtschutzmöglichkeiten verwehrt.

II. Die Entscheidung des BVerfG

1. Vorgeschichte

Der Antrag auf Erlass der einstweiligen Anordnung wurde von der Beschwerdeführerin[39] vor folgendem Hintergrund gestellt:

„Die Beschwerdeführerinnen sind Konzernunternehmen eines Telekommunikationsdiensteanbieters. Das Amtsgericht hat gegenüber den Beschwerdeführerinnen, die Überwachung und Aufzeichnung

[36] BVerfGE 130, 151 (184); *Ostendorf/Brüning*, Strafprozessrecht, 5. Aufl. 2024, § 11 Rn. 62; ausführlich zum Doppel-Tür-Modell *Wäger*, MMR 2026, 15.

[37] BVerfGE 165, 363 (398).

[38] *Huber*, NVwZ 2026, 319 (320).

[39] Tatsächlich handelt es sich um mehrere Beschwerdeführerinnen, der Einfachheit halber haben die *Verf.* auf Singular reduziert.

der inländischen Domain-Name-System-Anfragen über die von [den Beschwerdeführerinnen] bereitgestellten Netzwerkinfrastrukturen zu dem Serversystem mit dem Namen […] mit der […] nebst Übermittlung der zur Identifizierung der Anschlussinhaber erforderlichen Kundendaten für die Dauer von etwas mehr als einem Monat angeordnet."[40]

Diese Anordnung hatte das Amtsgericht Oldenburg auf Grundlage der §§ 100a Abs. 1, 100e StPO erlassen.[41]

Das heißt, dass die Beschwerdeführerin alle DNS-Anfragen zu einer bestimmten, mutmaßlich inkriminierten Website erfassen und diese samt Informationen über die anfragenden Personen (IP-Adresse und Zuordnung zu Anschlüssen/Mobilgeräten) an die Ermittlungsbehörden weiterleiten sollte. Die Beschwerde der Beschwerdeführerin gem. § 304 Abs. 1 StPO gegen diese Anordnung des AG hatte das LG als unzulässig verworfen.[42] Daraufhin hat die Beschwerdeführerin Verfassungsbeschwerde eingelegt und einen Antrag auf Erlass einer einstweilige Anordnung nach § 32 BVerfGG gestellt, mit der sie die Überwachungsanordnung des AG Oldenburg auszusetzen wünscht.[43] Im Hauptsacheverfahren macht die Beschwerdeführerin insbesondere geltend, für die vom AG angeordnete Maßnahme existiere keine Ermächtigungsgrundlage.[44]

2. Entscheidungsgründe

Der Antrag auf einstweilige Anordnung hatte Erfolg. Das BVerfG entschied, dass die Vollstreckung der Anordnung des AG Oldenburg bis zur Entscheidung über die Verfassungsbeschwerde in der Hauptsache (längstens aber für die Dauer von sechs Monaten) ausgesetzt wird und verbot dem AG Oldenburg, inhaltsgleiche Anordnungen auf Grundlage von § 100a StPO gegen die Beschwerdeführerin zu treffen. Über die Begründetheit der Verfassungsbeschwerde in der Hauptsache hat das BVerfG also explizit noch nicht entschieden.

Der Ausgang des Hauptsacheverfahrens sei „mindestens offen"[45], daher sei der Antrag zulässig gewesen. Das BVerfG konzentrierte sich in der Begründung der Entscheidung ausschließlich auf die Folgenabwägung im Rahmen der Begründetheit:

a) Folgen bei unterbliebener Anordnung und Erfolg der Verfassungsbeschwerde in der Hauptsache

Das BVerfG führte zunächst zu den Folgen aus, die eintreten würden, wenn der Erlass der einstweiligen Anordnung nach § 32 BVerfGG unterbliebe, die Verfassungsbeschwerde in der Hauptsache aber Erfolg hätte. Dabei ging das BVerfG nicht nur auf die Folgen für Grundrechte der Beschwerdeführerin (vor allem Art. 12 GG) ein, sondern auch auf die Folgen für die Grundrechte der Anschlussinhaber, deren DNS-Anfragen infolge der Anordnung überwacht werden würden. Insbesondere sei aufgrund der Menge der DNS-Anfragen an die Beschwerdeführerin, das BVerfG geht von monatlich 12,96 Billionen Anfragen aus, der organisatorische Aufwand für die Beschwerdeführerin erheblich. Eine Ausleitung von DNS-Anfragen für eine bestimmte Website sei nur möglich, wenn die Beschwerdeführerin

[40] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 2.
[41] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 2.
[42] Vgl. BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 3.
[43] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 6.
[44] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 5.
[45] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 13.

alle DNS-Anfragen ihrer 40 Millionen Kundinnen und Kunden auswerte.[46] Neben diesem erheblichen organisatorischen Aufwand sei auch ein Reputationsverlust der Beschwerdeführerin zu erwarten, wenn die Anordnung nicht erginge, die Maßnahme sich aber später als verfassungswidrig herausstelle.[47] Zudem wären durch die Maßnahme massenhafte Eingriffe in das Fernmeldegeheimnis, Art. 10 GG, der Kundinnen und Kunden zu befürchten.[48] Aus diesen Umständen ergibt sich für das BVerfG wohl auch die besondere Eilbedürftigkeit, die Voraussetzung der Anordnung ist.

b) Folgen bei Ergehen der Anordnung und Abweisung der Verfassungsbeschwerde in der Hauptsache

Erginge die Anordnung und die Verfassungsbeschwerde hätte keinen Erfolg, dann könnten die Ermittlungsbehörden ihre Ermittlungen nicht auf die DNS-Daten der Beschwerdeführerin stützen und wären auf andere Ermittlungsmöglichkeiten beschränkt.[49]

c) Abwägung

Die Folgenabwägung fällt zugunsten der Beschwerdeführerin aus. Einerseits sei weder aus den Ermittlungsakten ersichtlich, dass die mit der DNS-Überwachung verfolgten Delikte besonders schwer wögen, noch sei erkennbar, warum andere Ermittlungsmaßnahmen nicht ebenso erfolgsversprechend sein sollten wie die DNS-Überwachung.[50] Andererseits sei der organisatorische Aufwand der Umsetzung der Anordnung für die Beschwerdeführerin ganz erheblich.[51] Darüber hinaus wögen aber die „massenhaften und irreversiblen“[52] Eingriffe in das Fernmeldegeheimnis der Kundinnen und Kunden der Beschwerdeführerin besonders schwer, da zum einen alle DNS-Anfragen aller Kundinnen und Kunden der Beschwerdeführerin überwacht werden müssten und dies zum anderen auch noch heimlich geschehen müsste und aufgrund der großen Anzahl der DNS-Anfragen auch eine nachgelagerte Information über die Überwachung nicht möglich sei.[53]

III. Bewertung der Entscheidung

Der Beschluss vermag zu überzeugen. Zwar hat das BVerfG nur eine Folgenabwägung vorgenommen und die Erfolgsaussichten der Verfassungsbeschwerde im Hauptsacheverfahren nur als „mindestens offen“[54] bezeichnet. Gleichwohl lässt sich erkennen, dass die Kammer erhebliche verfassungsrechtliche Bedenken hatte. Sie setzte nicht nur die Vollziehung des Beschlusses des AG Oldenburg bis zur Entscheidung über die Verfassungsbeschwerde aus, sondern untersagte dem AG Oldenburg auch, inhaltsgleiche Anordnungen gegen Vodafone auf Grundlage von § 100a StPO bis zur Entscheidung über die Verfassungsbeschwerde zu wiederholen.[55]

---

[46] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 15.
[47] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 16.
[48] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 16.
[49] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 17.
[50] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.
[51] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.
[52] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.
[53] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.
[54] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 13.
[55] *Huber*, NVwZ 2026, 319 (320).

Das BVerfG hat im Rahmen der Folgenabwägung entscheidend darauf abgestellt, dass ohne den Erlass der einstweiligen Anordnung die drohenden massenhaften und irreversiblen Eingriffe in das Fernmeldegeheimnis der Kund*innen aus Art. 10 Abs. 1 GG drohten, ohne dass diese entsprechende Verdachtsmomente geliefert hätten.[56] Für die Hauptsache muss gleichwohl unterschieden werden: Im Rahmen der Zulässigkeit kann die Beschwerdeführerin nur die Verletzung eigener Grundrechte rügen. Damit wäre eine Verfassungsbeschwerde insoweit unzulässig, als die Beschwerdeführerin eine Verletzung von Art. 10 Abs. 1 GG ihrer Kund*innen geltend macht.[57] Im Rahmen der Begründetheit der Verfassungsbeschwerde prüft das BVerfG den angegriffenen Hoheitsakt, also die Anordnung durch das AG (in ihrer letztinstanzlichen Ausprägung), jedoch am Maßstab des gesamten Verfassungsrechts.[58] In Betracht kommt daher, dass bei der Anwendung und Auslegung des § 100a StPO Bedeutung und Tragweite der Grundrechte verkannt wurden, da § 100a StPO gerade keine Ermächtigung für die DNS-Überwachung, also massenhafte Eingriffe in Art. 10 Abs. 1 GG der Kund*innen enthält. Somit erlangt der Eingriff in Art. 10 Abs. 1 GG dennoch Bedeutung für die Begründetheitsprüfung. Denn die Ermittlungsbehörde ist nicht befugt, einen privaten Dritten zur Durchführung von Maßnahmen zu verpflichten, die diese selbst mangels einer ausreichenden Ermächtigungsgrundlage nicht durchführen dürfte. Insoweit ist zu prüfen, ob § 100a StPO eine ausreichende Ermächtigungsgrundlage für die Eingriffe in Art. 12 Abs. 1 GG und Art. 10 Abs. 1 GG im Einzelfall bildet.

Dies macht auch das BVerfG deutlich, in dem es feststellt:

> „Für den Erlass einer einstweiligen Anordnung sprechen insbesondere die drohenden massenhaften und irreversiblen Eingriffe in das Fernmeldegeheimnis der Kundinnen und Kunden, die einer Kenntnisnahme ihrer privaten oder beruflichen Kontakte ausgesetzt wären, ohne entsprechende Verdachtsmomente geliefert zu haben.“[59]

Ein solcher „irreversibler Eingriff“ in Art. 10 GG läge jedenfalls dann vor, wenn die Anordnung des AG Oldenburg nicht auf einer ausreichenden Ermächtigungsgrundlage beruht. Das wäre der Fall, wenn die Maßnahme auf § 100a StPO gestützt worden wäre, obwohl diese Vorschrift auf die Überwachung laufender Kommunikationsinhalte zugeschnitten ist. Gerade daran fehlt es hier. Gegen die Heranziehung von § 100a StPO sprechen im Kern drei Aspekte: die Einordnung der DNS-Abfrage als Kommunikationsumstand, die Umkehr der Ermittlungsrichtung sowie der mehrstufige Charakter des Grundrechtseingriffs.

1. DNS-Abfrage als Kommunikationsumstand

Ausgangspunkt jeder rechtlichen Einordnung ist die technische Funktion der DNS-Abfrage. Welche der Eingriffsnormen der §§ 100a ff. StPO anwendbar ist, entscheidet sich vor allem danach, ob auf laufende Kommunikation oder auf gespeicherte Kommunikationsumstände zugegriffen wird.

Das DNS dient der vorgelagerten „Adressauflösung“, das heißt ein Endgerät fragt rekursiv beim DNS-Resolver an, der die Anfrage iterativ über Root-, TLD- und autoritative Nameserver auflöst, bis schließlich eine IP-Adresse zurückgeliefert wird. In diesem Stadium findet noch keine inhaltliche Interaktion zwischen Nutzer*innen und der aufgerufenen Website und damit keine laufende Kommunika-

[56] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.
[57] Vgl. *Voßkuhle*, in: Huber/Voßkuhle, Grundgesetz, Kommentar, 8. Aufl. 2024, Art. 93 Rn. 183.
[58] *Walter*, in: Dürig/Herzog/Scholz, Grundgesetz, Kommentar, 108. Lfg., Stand: August 2025, Art. 94 Rn. 226.
[59] BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 18.

tion statt. Es handelt sich lediglich um eine maschinelle Infrastrukturkommunikation. Das DNS übermittelt keinen Inhalt einer Kommunikation, sondern löst lediglich einen Domainnamen in eine IP-Adresse auf, damit eine spätere Verbindung zum Zielserver überhaupt erst aufgebaut werden kann, die erst eine inhaltliche laufende Kommunikation ermöglicht. Bildlich gesprochen geht es eher um das Ermitteln einer Telefonnummer vor dem Anruf als um das eigentliche Gespräch selbst. Die DNS-Abfrage betrifft damit einen gespeicherter Kommunikationsumstand im Sinne der Systematik der §§ 100g, 100k StPO, nicht „Inhalt" einer laufenden Kommunikation i.S.d. § 100a StPO, sodass die Norm systematisch nicht passt. Auch eine Anwendung von § 100a Abs. 1 S. 2 und 3 StPO scheidet aus. Die Ermittlungsbehörden wollen die Daten gerade nicht an der Quelle, also auf dem informationstechnischen System des Betroffenen, erheben, sondern vielmehr beim Eingang der DNS-Anfrage am Resolver.

2. Umkehr der Ermittlungsrichtung

Hinzu kommt, dass die angeordnete Maßnahme die Ermittlungsrichtung umkehrt. Sie zielt nicht auf die Überwachung der Kommunikation einer bereits individualisierten Person, gegen die ein Anfangsverdacht wegen einer Katalogtat nach § 100a Abs. 2 StPO besteht. Vielmehr soll die Maßnahme überhaupt erst aufdecken, welche Nutzer*innen über welche Anschlüsse mit der fraglichen Domain in Verbindung standen. Der Ermittlungsansatz verläuft damit nicht von einem individualisierten Tatverdächtigen zu dessen Kommunikationsbeziehungen, sondern von massenhaft erhobenen technischen Umständen zu bislang unbekannten und auch unverdächtigen Nutzer*innen. Systematisch weist die Maßnahme deshalb eine deutlich größere Nähe zur Funkzellenabfrage nach § 100g Abs. 3 StPO auf als zur Telekommunikationsüberwachung nach § 100a Abs. 1 StPO.

Unabhängig davon ist zudem nicht erkennbar, ob überhaupt ein Verdacht hinsichtlich einer der in § 100a StPO genannten Katalogtaten bestand.[60]

Auch weist die Umkehrung der Ermittlungsrichtung eine gewisse Nähe der Maßnahme zur Vorratsdatenspeicherung und Rasterfahndung auf. Erfasst werden nicht die Daten eines bereits individualisierten Beschuldigten, sondern die DNS-Anfragen eines großen, im Voraus unbestimmten Nutzer*innenkreises. Auf diese Weise wird zunächst ein breiter Datenbestand geschaffen, aus dem erst nachträglich verdächtige Verbindungen herausgefiltert werden sollen. Der Umstand, dass die Maßnahme an einen konkreten Ermittlungsanlass anknüpft, zeitlich begrenzt ist und sich auf einen bestimmten Zielserver bezieht, ändert nichts daran, dass bereits auf der Erhebungsebene eine Vielzahl unverdächtiger Nutzer*innen in die Maßnahme einbezogen wird. Ob eine solche Vorratsdatenspeicherung „durch die Hintertür" verfassungs- und europarechtskonform wäre, kann mindestens bezweifelt werden. Insbesondere der EuGH hat für die Vorratsdatenspeicherung strenge Maßstäbe aufgestellt und diese lediglich für die Speicherung von IP-Adressen gelockert.[61] Da die massenhafte Speicherung von DNS-Daten aber eine Profilerstellung von Internetnutzer*innen möglich macht, die detaillierte Rückschlüsse auf das Privatleben zulässt, erscheint es sicher, dass selbst eine beschränkte DNS-Überwachung verfassungs- und unionsrechtswidrig wäre.[62] Jedenfalls aber ist § 100a StPO keine hierfür geeignete Rechtsgrundlage.

---

[60] Nach den Entscheidungsgründen hat die Anordnung des AG Oldenburg den Tatverdacht abstrakt wiedergegeben und darüber hinaus den Beschluss nicht begründet, BVerfG, Beschl. v. 25.11.2025 – 1 BvR 2317/25 = BeckRS 2025, 33604 Rn. 2.

[61] EuGH NJW 2024, 2099; vgl. auch die Anmerkungen von *Hartl/Vogel*, NJW 2024, 2099 (2106 f.), und *Roßnagel*, EuZW 2024, 657 (664 ff.).

[62] Vgl. zum Unionsrecht schon den ersten Spiegelstrich des Leitsatzes von EuGH NJW 2024, 2099.

Eine inhaltliche Nähe besteht schließlich aufgrund der Umkehr der Ermittlungsrichtung auch zur digitalen Rasterfahndung im G-10-Gesetz. Zu dieser hatte das BVerfG zumindest angedeutet, dass eine Umkehr der Ermittlungsrichtung ohne einen vor der Aufnahme der Ermittlung bestehenden Tatverdacht verfassungsrechtlich unzulässig sein könnte.[63]

3. Mehrstufiger Grundrechtseingriff

Darüber hinaus ist zu beachten, dass sich die vom AG Oldenburg angeordnete Maßnahme nicht in einem einheitlichen Grundrechtseingriff erschöpft. Vielmehr sind drei eigenständige Grundrechtseingriffe auseinander zu halten.

Erstens muss die betroffene Providerin den laufenden DNS-Datenstrom sämtlicher Kund*innen über einen Monat hinweg erfassen, gegebenenfalls kurzfristig vorhalten und technisch vollständig durchmustern. Dieser Zugriff auf die äußeren Umstände der Kommunikation von ca. 40 Millionen Anschlüssen stellt einen Eingriff in Art. 10 Abs. 1 GG der Nutzer*innen dar.

Zweitens setzt die Umsetzung der Anordnung voraus, dass eine technische Anpassung der Resolver-Systeme und der Überwachungsinfrastruktur erfolgt. Soweit damit ein strukturierter Eingriff in die Netzinfrastruktur selbst verbunden ist, ist auf der Grundlage der neuen „Trojaner-Rechtsprechung“ davon auszugehen, dass zusätzlich das IT-System-Grundrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG berührt ist. Systematisch handelt es sich bei der zweiten Stufe um die zweite Tür des oben beschriebenen Doppel-Tür-Modells.

Drittens müssen die massenhaft erfassten Datensätze automatisiert nach Treffern durchsucht und mit Bestandsdaten verknüpft werden. Das BVerfG hat insoweit betont, dass die algorithmische Weiterverarbeitung bereits erhobener Daten kein bloßer Annex der Erhebung ist, sondern einen eigenständigen Grundrechtseingriff in das Recht auf informationelle Selbstbestimmung mit spezifischem Belastungspotential darstellt, für die der Gesetzgeber nun voraussichtlich mit der anstehenden Reform der StPO die erforderliche Rechtsgrundlage schaffen wird.

§ 100a StPO jedenfalls bietet für keine dieser drei Ebenen eine tragfähige Ermächtigungsgrundlage. Die amtsgerichtliche Konstruktion, § 100a StPO gleichsam als „Alles-aus-einer-Hand-Norm“ zu verwenden, ist damit systemwidrig, verstößt gegen den Vorbehalt des Gesetzes und ist somit verfassungswidrig.

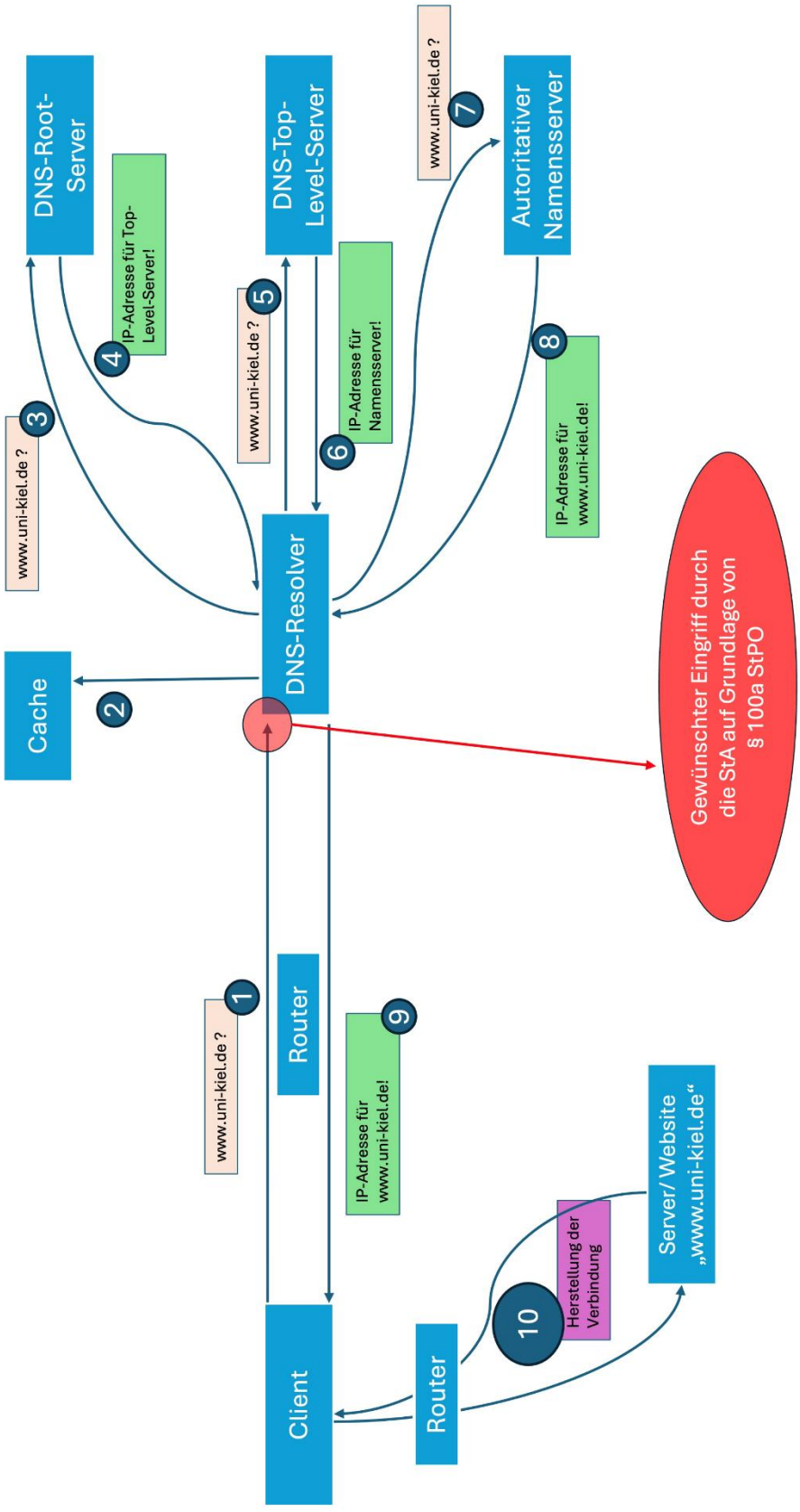
IV. Fazit

Das BVerfG setzt damit dem Versuch, eine technisch neuartige und massenhaft streuende Ermittlungsmaßnahme funktional unter eine bestehende Eingriffsnorm zu ziehen, zu Recht vorläufig eine Grenze und knüpft damit – ohne sich freilich in der Sache zu verhalten – an die Linie der sog. Trojaner-Entscheidungen an, wonach digitale Ermittlungsmaßnahmen nicht durch bloße Ausdehnung vorhandener Vorschriften legitimiert werden dürfen, sondern einer eingriffsspezifischen und hinreichend bestimmten gesetzlichen Grundlage bedürfen.

Der Referentenentwurf zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen bestätigt diesen Befund, indem er für neue digitale Analyse- und Abgleichmaßnahmen mit §§ 98d, 98e StPO-E eigenständige Ermächtigungsgrundlagen normiert. Gesetzesvorbehalte dürfen nicht unter dem Deckmantel der Technologieoffenheit umgangen werden.

[63] BVerfGE 93, 181 (191 f.).

V. Schaubild


DNS-Root-Server
IP-Adresse für Top-Level-Server!
DNS-Top-Level-Server
www.uni-kiel.de ?
IP-Adresse für Namensserver!
Autoritativer Namensserver
www.uni-kiel.de ?
IP-Adresse für www.uni-kiel.de!
www.uni-kiel.de ?
DNS-Resolver
Cache
Gewünschter Eingriff durch die StA auf Grundlage von § 100a StPO
www.uni-kiel.de ?
Router
IP-Adresse für www.uni-kiel.de!
Server/ Website „www.uni-kiel.de“
Herstellung der Verbindung
Client
Router