Hessisches Ministerium der Justiz
und für den Rechtsstaat

HESSEN

Fakten zur IP-Adressdatenspeicherung

Wiesbaden, den 19. April 2023

- **Was sind IP-Adressen?**

IP-Adressen sind – vereinfacht gesagt – die „**Telefonnummer eines Computers**.“ IP-Adressen werden von den Internetzugangsanbietern den an das Internet angebundenen Geräten ihrer Kunden zugewiesen. Bei dem Aufrufen von Webseiten, dem Download einer Datei oder dem Einloggen in ein E-Mail-Postfach wird jeweils diese IP-Adresse übertragen, um einen Datenaustausch mit diesem Gerät zu ermöglichen.
Während eine statische IP-Adresse einem bestimmten Anschlussinhaber dauerhaft fest zugewiesen wird, wird im Fall der dynamischen Adressierung dem Anschlussinhaber **täglich eine neue IP-Adresse zugewiesen** (die absolute Regel für Privatkunden). Die „Telefonnummer des Computers“ ändert sich also täglich.

- **Wie werden IP-Adressen von Strafverfolgungsbehörden genutzt?**

Cyber-Kriminelle agieren im Netz oft anonym. Die Strafverfolgungsbehörden wissen dann nur, welche IP-Adresse ein Täter wann genutzt hat, um beispielsweise eine erpresserische E-Mail zu verschicken oder ein Hassposting zu verbreiten. Mit der IP-Adresse lässt sich **ermitteln, von welchem Festnetz- oder Mobilfunkanschluss der Täter seine Internetverbindung aufgebaut hat**. Da hinter einem solchen Anschluss eine Person oder Firma steht, kann die IP-Adresse so zum Täter führen.

Pressesprecher und Leiter Presse- und Öffentlichkeitsarbeit:
Sebastian Zwiebel
Luisenstraße 13
65185 Wiesbaden
Telefon: 0611 32 142615
Telefax: 0611 32 7142763

DIGITALER SERVICE POINT
DER HESSISCHEN JUSTIZ
0800 96 32 147

pressestelle@hmdj.hessen.de
http://www.justizministerium.hessen.de

- **Ist eine Mindestspeicherung von IP-Adressen aus Sicht der Praxis notwendig?**

Ja. Während die Straftaten der Polizeilichen Kriminalstatistik (PKS) zwischen 2015 bis 2022 **insgesamt um über 11% zurückgegangen** sind, sind „digitale“ Straftaten **gegen den allgemeinen Trend stark gestiegen.**
Bei im Internet begangenen Straftaten kann die IP-Adresse der zur Tatbegehung genutzten Internetverbindung der **einzige vorliegende Ermittlungsansatz** zur Identifizierung des unbekannten Täters sein. Wenn diese IP-Adresse mangels Speicherung keinem Anschlussinhaber zugeordnet werden kann, kann die Tat nicht aufgeklärt werden – die Spur ist kalt. Ohne Regelung einer Mindestspeicherfrist sind Ermittlungserfolge vom Zufall abhängig, ob und wie lange Internetzugangsdienste die Zuordnung der vergebenen IP-Adressen zu den Kunden speichern.
Aber auch wenn weitere Ermittlungsansätze zur Identifizierung eines unbekannten Cyber-Kriminellen vorliegen, ist die Abfrage der IP-Adressen **der effektivste Ermittlungsansatz**. Dies beruht darauf, dass E-Mail-Adressen oder Profile in sozialen Netzwerken kostenlos und ohne Identitätskontrolle durch die Verwendung frei erfundener Personalien registriert werden können. Diese Personendaten sind daher oftmals nicht werthaltig. Die Internetzugangsdienste erheben dagegen verifizierte Personalien ihrer Kunden, um die Bezahlung der Dienstleitung sicherzustellen. Die hinter IP-Adressen stehenden Personendaten sind für die Strafverfolgungsbehörden daher wesentlich werthaltiger zum Zwecke der Identifizierung unbekannter Tatverdächtiger.

- **Wie lange werden IP-Adressen bei Internetzugangsdiensten gespeichert?**

Internetzugangsanbieter können aus Datenschutzgründen nicht frei entscheiden, ob und wie lange Verkehrsdaten zu geschäftlichen Zwecken vorgehalten werden. Zu **Abrechnungszwecken** werden bei Internetzugangsdiensten **keine IP-Adressen** gespeichert. Bei den im Bereich der Festnetzanschlüsse zum Regelfall gewordenen Tarifen mit einer „Flatrate“ besteht keine Notwendigkeit, IP-Adressen zu Abrechnungszwecken zu speichern. Aber auch bei volumenbegrenzten Verträgen werden aus Datenschutzgründen nur Datenvolumen und Benutzerkennung gespeichert. Zum Zwecke der **Erkennung, Eingrenzung und Beseitigung von Störungen** dürfen Internetzugangsdienste IP-Adressen und Benutzerkennung für einen kurzen Zeitraum (wenige Tage) speichern. Danach sind diese Daten unverzüglich zu löschen. Eine solche unternehmensinterne Speicherung wird von einigen Anbietern bei Festnetzanschlüssen für **maximal sieben Tage** durchgeführt; andere Anbieter speichern mangels Speicherverpflichtung kürzer oder gar nicht. Insbesondere im Bereich des mobilen Internetzugangs, bei dem einzelne IP-Adressen mehreren Kunden gleichzeitig zugewiesen werden können, erfolgt derzeit bei keinem Anbieter eine entsprechende Speicherung.

- **Gilt die Notwendigkeit auch für die Verfolgung von Darknet-Kriminalität?**

Ja. Eine anlasslose Speicherung von IP-Adressen wäre auch geeignet, die Strafverfolgung im Darknet zu verbessern. Die Zuordnung von IP-Adressen zu Anschlussinhabern ist ein **wichtiger Ermittlungsansatz**. Etwa im Ermittlungsverfahren der ZIT gegen die Betreiber der kinderpornografischen **Darknet-Plattform „BoysTown "** sind Betreiber nur deswegen identifiziert und verurteilt worden, weil die IP-Adresse, mit der sie sich auf Servern der Tätergruppierung angemeldet hatten, im Rahmen einer Server-Überwachung festgestellt und beim Internetdienstanbieter einem Anschlussinhaber zugeordnet werden konnten. Bei Nutzung anderer Internetdienstanbieter seitens der Beschuldigten wäre eine **Identifizierung mangels Speicherung nicht möglich** gewesen. Die Identifizierung ist insofern von der Zufälligkeit abhängig, welchen Internetdienstanbieter die Täter verwenden. Dieser Fall zeigt, dass die gegenwärtige Rechtslage unbedingt geändert werden muss, um es nicht dem Zufall zu überlassen, ob sexueller Missbrauch von Kindern aufgeklärt werden kann. Möglicherweise bleiben derzeit andere Kindesmissbraucher nur deshalb unentdeckt, weil sie einen Internetdienstanbieter verwenden, der die IP-Adressen nicht speichert.

- **Was hat der Europäische Gerichtshof (EuGH) entschieden?**

Nachdem die in Deutschland ab Januar 2009 geltende Pflicht zur anlasslosen Speicherung aller Verkehrsdaten bei Telefonaten und Internet-Nutzung für sechs Monate durch das Bundesverfassungsgericht im März 2010 für verfassungswidrig erklärt worden ist, sollte **ab Juli 2017** eine beschränkte **Pflicht zur anlasslosen Speicherung von Telefon-Verbindungsdaten und IP-Adressen für zehn Wochen sowie Standortdaten der Funkzellen für vier Wochen** bestehen. Daten zur E-Mail-Nutzung waren ausdrücklich ausgeschlossen. Die Umsetzung war jedoch aufgrund von Gerichtsentscheidungen und einer Entscheidung der Bundesnetzagentur wegen europarechtlicher Bedenken von Beginn an ausgesetzt. Im **September 2022** hat der **EuGH festgestellt, dass diese deutschen Regelungen nicht mit geltendem EU-Recht vereinbar** sind. Infolge dieses Urteils haben Bundesverfassungsgericht (BVerfG) und Bundesverwaltungsgericht (BVerwG) festgestellt, dass die nationalen Regelungen zur Vorratsdatenspeicherung unionsrechtswidrig sind und wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden dürfen.

- **Wie sind die Vorgaben des EuGH für eine Vorratsdatenspeicherung?**

Nach der Rechtsprechung des EuGH ist eine anlasslose Speicherung von Verkehrs- und Standortdaten nur zum **Schutz der nationalen Sicherheit** vor einer aktuell oder vorhersehbar einzustufenden ernsten Bedrohung möglich.
Für die **Verfolgung schwerer Kriminalität** oder die Verhinderung schwerer Bedrohungen der öffentlichen Sicherheit ist eine anlasslose Speicherung von Verkehrsdaten und Standortdaten nicht zulässig. Möglich sind nur weniger eingriffsintensive Maßnahmen, von denen der EuGH drei Ausgestaltungen ausdrücklich genannt hat:

- eine anlasslose **gezielte Vorratsdatenspeicherung** anhand von objektiven oder geografischen Kriterien, z.B. an Flughäfen oder Bahnhöfen
- eine anlassbezogene Speicherung von Verkehrsdaten und Standortdaten aufgrund einer behördlichen Anordnung bei einem konkreten Verdacht („**Quick Freeze**“)
- eine anlasslose **Speicherung von IP-Adressen** in einem auf das absolut Notwendige begrenzten Zeitraum, da IP-Adressen in bestimmten Bereichen der einzige Anhaltspunkt sein können, um den genutzten Anschluss zu identifizieren.

- **Was sieht der hessische Gesetzentwurf vor?**

Mit dem hessischen Gesetzentwurf soll die vom EuGH ermöglichte anlasslose Speicherung von IP-Adressen umgesetzt werden, weil dies für die **Strafrechtspraxis und insbesondere die Bekämpfung des sexuellen Missbrauchs von Kindern und der Kinderpornografie** besonders wichtig ist. Auch für die **Gefahrenabwehrbehörden** ist es wichtig, zur **Identifizierung von Gefährdern** auf vorratsgespeicherte IP-Adressen zugreifen zu können, um **extremistische und terroristische Bedrohungen wirksam abwehren** zu können. Auch dies sieht hessische Gesetzentwurf vor.
Daneben soll es – ebenfalls unter Berücksichtigung der genannten Rechtsprechung – **zur Verfolgung allgemeiner Kriminalität und zum Schutz der öffentlichen Sicherheit** auch weiterhin möglich sein, dass Internetzugangsdienste mindestgespeicherte IP-Adressen für eine **Bestandsdatenauskunft anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse** verwenden dürfen, um den **Strafverfolgungs- und Gefahrenabwehrbehörden die Identitätsdaten** des relevanten Anschlussinhabers zu übermitteln. Für den Abruf der mindestgespeicherten IP-Adressen durch die Strafverfolgungsbehörden sieht die Strafprozessordnung (StPO) schon jetzt in § 100g Abs. 2 StPO einen **Katalog entsprechender Straftaten der schweren Kriminalität** vor. Dieser **kann bestehen bleiben**. Darunter fallen etwa Straftaten des sexuellen Missbrauchs von Kindern und der Vergewaltigung sowie die Verbreitung, der Erwerb und Besitz kinderpornografsicher Inhalte.

- **Wie kommt der Speicherzeitraum von einem Monat zustande?**

Der Speicherzeitraum von einem Monat ist Ergebnis einer **Gesamtabwägung** unter Berücksichtigung der **Vorgaben des EuGH** zur Eingriffstiefe der Speicherung von IP-Adressen sowie den berechtigten Speicherzwecken als Rechtfertigung des Eingriffs. Zur Ausfüllung dieser Vorgaben sind die **fachlichen Erfordernisse der Strafverfolgungspraxis** in Deutschland berücksichtigt worden, wie etwa die hohen Gesamtzahlen schwerer internetbezogener Kriminalität und das durch Studien abschätzbare Dunkelfeld nicht angezeigter Straftaten. Entscheidend ist die nur kurze und unvollständige Speicherung der Internetzugangsdienste auf freiwilliger Basis sowie die darauf beruhende niedrige Aufklärungsrate von tatrelevanten IP-Adressen.
Angesichts dessen überschreitet dieser Speicherzeitraum nicht das im Hinblick auf das Ziel der Bekämpfung schwerer internetbezogener Kriminalität absolut Notwendige.

- **Was sieht der Gesetzentwurf für minderschwere Kriminalität vor?**

Die anlasslose Erhebung der IP-Adressen hat zwar den Zweck, bei schwerer Kriminalität die gespeicherten IP-Adressen zu einer tatrelevanten Benutzerkennung in Gänze an die Strafverfolgungsbehörden auszuliefern. Da dieser **Abruf der gesamten mindestgespeicherten IP-Adressen** durch die Strafverfolgungsbehörden **nur bei Straftaten der schweren Kriminalität** möglich ist, kann dies nicht bei allgemeiner Internetkriminalität wie Hasspostings, Volksverhetzungen oder bei Cyberangriffen erfolgen.
Erforderlich für eine effektive Aufklärung und **Verfolgung allgemeiner Internetkriminalität** ist aber regelmäßig nur, dass eine den Strafverfolgungsbehörden **bereits bekannte IP-Adresse durch die Internetzugangsanbieter dem jeweiligen Anschlussinhaber zugeordnet** werden kann. Bei einer entsprechenden Anfrage der Strafverfolgungsbehörden sind die Internetzugangsdienste derzeit verpflichtet, intern auch auf den anlasslos gespeicherten Gesamtdatenbestand von IP-Adressen zuzugreifen, so den zu der mitgeteilten IP-Adresse verknüpften Abschlussinhaber zu identifizieren und anschließend ausschließlich die entsprechenden Personendaten an die Strafverfolgungsbehörden herauszugeben. Diese Unterscheidung zwischen **Herausgabe aller gespeicherter IP-Adressen** einerseits und lediglich **punktuellem internem Zugriff der Internetzugangsdienste** andererseits hat auch das (BVerfG) anerkannt und ausdrücklich festgehalten, dass bei einer Zuordnung von IP-Adressen durch anlasslos gespeicherte Verkehrsdaten verfassungsrechtlich nicht die für die unmittelbare Verwendung der Gesamtheit der vorsorglich gespeicherten Verkehrsdaten geltenden besonders strengen Voraussetzungen gegeben sein müssen.
Da auch allgemeine Kriminalität Menschen aus der Mitte der Gesellschaft treffen, sollen die mindestgespeicherten IP-Adressen auch weiterhin durch Internetzugangsdienste zur Beauskunftung von Anschlussinhabern genutzt werden können.

- **Wäre „Quick Freeze“ eine Alternative zur Speicherung von IP-Adressen?**

Nein. Ziel von „Quick Freeze“ ist es, eine anlasslose Speicherung von Verkehrsdaten zu verhindern und stattdessen nur eine **anlassbezogene Speicherung** in einem konkreten Einzelfall beschränkt auf relevante Kennungen zu ermöglichen. Dazu sollen mittels einer **behördlichen Anordnung** die bei den Dienstanbietern vorliegenden Verkehrsdaten zu Festnetz- oder Mobilrufnummern bzw. IP-Adressen „eingefroren“ werden, um eine Löschung zu verhindern.
Ein behördlich angeordnetes „Einfrieren“ von Verkehrsdaten ist aber nur dann möglich, wenn diese bei dem jeweiligen Dienstanbieter überhaupt vorhanden sind. Im Bereich der **Internetnutzung** werden IP-Adressen den Anschlussinhabern ständig dynamisch neu zugewiesen. Für ein „Einfrieren“ der noch gespeicherten Daten muss daher zunächst der tatrelevante Anschluss der Betroffenen über eine Zuordnung der IP-Adresse zu einem Kunden identifiziert werden. Ist diese Zuordnung jedoch nicht oder nicht mehr gespeichert, können auch keine Verkehrsdaten zu dem jeweiligen Tatverdächtigen „eingefroren“ werden.

„Quick Freeze“ kann daher eine **anlasslose Speicherung von IP-Adressen nicht ersetzen**, um unbekannte Internetnutzer zu identifizieren. Vor diesem Hintergrund hatte das Bundesjustizministerium bereits im Jahr 2011 in einem Referentenentwurf zur Ermöglichung von „Quick Freeze“ eine begrenzte anlasslose Speicherung von IP-Adressen für sieben Tage als zwingend notwendig erachtet, um Bestandsdatenauskünfte zum Zwecke der Identifizierung unbekannter Internetnutzer zu ermöglichen.

- **Ist nicht bereits heute in über 90% eine Aufklärung über die IP-Adresse möglich?**

Nein. In diesem Zusammenhang wird häufig auf eine Mitteilung der Bundesregierung im Januar 2022 abgestellt, wonach in den Jahren 2017 bis 2021 von über 300.000 Hinweisen der U.S.-amerikanischen NGO „NCMEC“ zu Kinderpornographie im Internet etwa 19.000 Fälle nicht aufgeklärt werden konnten, weil die IP-Adresse mangels Speicherung nicht mehr abfragbar war. Der Umkehrschluss, dass in über 90% aller Fälle eine Aufklärung über die IP-Adresse möglich war, ist zwar naheliegend, aber nicht zutreffend. Denn diese Statistik bezieht sich einerseits ausschließlich auf nicht abfragbare IP-Adressen und nicht etwa auch auf Fälle, in denen eine IP-Adresse erfolglos abgefragt worden ist. Andererseits sind in der Statistik nur solche Fälle erfasst worden, in denen **als einziger Identifizierungsansatz ausschließlich eine IP-Adresse** vorlag und nicht etwa weitere Ermittlungsansätze wie E-Mail-Adressen, bei denen eine Abklärung der IP-Adressen ebenfalls zur Aufklärung hätte führen können.
Das BKA hat vielmehr klargestellt, dass in dem genannten NCMEC-Prozess trotz tagesaktueller Abfrage der mitgeteilten IP-Adressen **nur 41%** einem Nutzeranschluss zugeordnet werden konnten. Etwa 34% der angelieferten IP-Adressen waren bei den Internetzugangsdiensten trotzdem bereits nicht mehr gespeichert und weitere 24% aus anderen Gründen nicht beauskunftbar. Durch weitere und wesentlich aufwändigere Ermittlungen erreichte das BKA zwar eine **Erfolgsquote von insgesamt etwa 75%** – die übrigen 25% der Meldungen mussten aber mangels Ermittlungsansätzen durch die **ZIT eingestellt** werden.

- **Wie viele Verdachtsfälle von Kinderpornografie bleiben unaufgeklärt?**

Alleine in dem beschriebenen NCMEC-Prozess müssen etwa **25 % der Meldungen zu Kinder- und Jugendpornografie** bei unbekannten deutschen Internetnutzern mangels Ermittlungsansätzen durch die ZIT eingestellt werden. Dies waren im Jahr 2022 knapp 20.000 Fälle. **Nimmt man das Urteil des Europäischen Gerichtshofs (EuGH) als Stichtag**, mussten seit Oktober 2022 insgesamt knapp **29.500 entsprechende Vorgänge ohne Identifizierung der Tatverdächtigen eingestellt** werden, insbesondere weil die angelieferten IP-Adressen mangels Speicherung keinem Anschlussinhaber zugeordnet werden konnten. Bei den übrigen strafrechtlich relevanten Hinweisen, die nicht aufgeklärt werden konnten, erhielt das BKA neben einer IP-Adresse weitere Ermittlungsansätze, die dennoch nicht zum Erfolg führten. Auch in diesen Fällen hätten die IP-Adressen zum Ermittlungserfolg führen können.

- **Wären diese Fälle mit einer Mindestspeicherfrist für IP-Adressen aufklärbar?**

Zur Beantwortung der Frage, welche Erfolgsquoten im NCMEC-Prozess erreicht werden könnten, wenn eine einheitliche Speicherverpflichtung für IP-Adressen umgesetzt würde, hat das BKA eine **technische Auswertung von etwa 66.000 strafrechtlich relevanten NCMEC-Vorgängen aus dem Jahr 2022** durchgeführt. Dabei wurde festgestellt, dass die Erfolgsquote durch eine einheitliche gesetzliche Speicherverpflichtung erheblich gesteigert werden könnte, wobei der Effekt in den ersten Wochen besonders signifikant wäre. So würde bei einer einmonatigen Speicherpflicht die **Aufklärungsrate der IP-Adressen in dem NCMEC-Prozess auf über 90%** steigen. Dies ist insbesondere deswegen wichtig, weil im Rahmen des NCMEC-Prozesses von BKA und ZIT regelmäßig auch **reale Missbrauchsfälle aufgedeckt** werden, auch in Hessen. So beruht etwa das Urteil des LG Fulda gegen einen ehemaligen Schulleiter von Anfang Juni 2023 auf einem NCMEC-Hinweis. Das LG sah es als erwiesen an, dass der Angeklagte in einem Zeitraum von über 20 Jahren in über 90 Fällen über 30 Kinder und Jugendliche sexuelle missbraucht haben soll und verurteilte ihn deswegen zu einer Gesamtfreiheitsstrafe von 7 Jahren und ordnete die anschließende Sicherungsverwahrung an. Das Urteil ist noch nicht rechtskräftig.

- **Können zukünftig Persönlichkeitsprofile der Internetnutzer erstellt werden?**

Nein. Bewegungs- oder Persönlichkeitsprofile können auch zukünftig nicht erstellt werden. Der Entwurf sieht nur eine Speicherung derjenigen IP-Adressen vor, die der Quelle einer Verbindung bei dem Internetzugangsdienst zugewiesen sind. Mit diesen Quell-IP-Adressen kann jedoch **nicht automatisch nachvollzogen werden, welche Internetseiten aufgerufen oder welche Begriffe bei Suchmaschinen eingegeben** wurden. Nur wenn den Strafverfolgungsbehörden der eigentliche Telekommunikationsvorgang bereits genau bekannt ist, kann ermittelt werden, welcher Kunde Teilnehmer an der betreffenden Internetnutzung ist. Es ist jedoch bei geltender Verpflichtung zur Vorratsdatenspeicherung **nicht möglich, die komplette Internetnutzung einer Person nachzuvollziehen**, weil die Provider nicht speichern müssen, welche Internetseiten ein Kunde aufgerufen hatte. Da im Rahmen der Vorratsdatenspeicherung **keine Inhaltsdaten** aufgezeichnet werden, können durch die Strafverfolgungsbehörden lediglich die näheren Umstände der Telekommunikation ermittelt werden.

- **In welchen Fällen werden alle IP-Adressen eines Nutzers benötigt?**

In Fällen schwerer Kriminalität sind solche Abfragen denkbar, wenn durch die Ermittlungen auch entsprechende Vergleichsdaten von IP-Adressen erhoben worden sind, etwa durch Sicherstellung eines Servers oder durch Herausgabe entsprechender Informationen durch einen Internetdienstes. In einem fiktiven Beispielsfall der Ermittlun-

gen wegen Verbreitung bislang unbekannter Abbildungen des sexuellen Kindesmissbrauchs über ein Profil in sozialen Netzwerken könnten zunächst die Login-IP-Adressen des betreffenden Nutzerprofils bei dem sozialen Netzwerk für den letzten Monat erhoben und anschließend nach einer Abfrage aller mindestgespeicherter IP-Adressen in Bezug auf einen Anschlussinhaber verglichen werden, ob dieser oder andere Anschlussinhaber sich in das Profil eingeloggt hatten.

- **Wie kann die Vorratsdatenspeicherung nach dem hessischen Gesetzentwurf bei der Gefahrenabwehr, z.B. der Verhinderung terroristischer Anschläge, helfen?**

Nach dem hessischen Entwurf besteht für die Gefahrenabwehrbehörden zukünftig die Möglichkeit, z.B. auf Grundlage der Polizeigesetze 30 Tage lang auf vorratsgespeicherte IP-Adressen zur Identifizierung von potenziellen Gefährdern zuzugreifen. Wenn die Behörden z.B. Informationen erhalten, dass eine unbekannte Person in sozialen Medien Drohungen gepostet oder auf einer Darknet-Seite eine Anleitung zum Bombenbau heruntergeladen hat, kann diese Person zukünftig über die Zuordnung der genutzten IP-Adresse 30 Tage rückwirkend identifiziert und Folgemaßnahmen eingeleitet werden.