

Die vorsorgliche Speicherung von IP-Adressen

– Häufig gestellte Fragen zum Gesetzentwurf des BMJV –

Auf einen Blick

Das Problem

Straftaten im digitalen Raum nehmen erheblich zu. Vor allem die digitale Verbreitung von Kinderpornographie ist in den letzten Jahren drastisch gestiegen. Stark zugenommen haben auch Online-Betrug und Hasskriminalität im Netz. Derzeit kommen viele Täter ungestraft davon. Ihre Identität lässt sich in vielen Fällen nicht ermitteln.

Unser Ziel

Wir wollen beim Kampf gegen Kriminalität im Netz vorankommen. Unser Ziel ist eine höhere Aufklärungsquote bei internetbezogener Kriminalität. Dazu wollen wir Internetzugangsanbieter in die Pflicht nehmen – und den Ermittlungsbehörden neue Instrumente an die Hand geben. Dabei ist für uns klar: Es geht uns um eine Stärkung der Ermittlungsbehörden – unter strikter Wahrung verfassungs- und europarechtlicher Vorgaben. Grundrechte gelten auch im digitalen Raum; rechtsstaatliche Prinzipien sind nicht verhandelbar.

Unsere Lösung

Anbieter von Internetzugangsdiensten sollen verpflichtet werden, IP-Adressen ihrer Kunden für drei Monate vorsorglich zu speichern (dazu unten I). IP-Adressen sind oft der einzige Anhaltspunkt, um Täter bei internetbezogener Kriminalität zu identifizieren. Ihre verpflichtende Speicherung ist kein tiefer Grundrechtseingriff: Denn mit diesen Daten lassen sich keine Rückschlüsse auf die Inhalte von Kommunikation ziehen. Die Bildung von digitalen Bewegungs- oder Persönlichkeitsprofilen ist ausgeschlossen. Darüber hinaus wollen wir das neue Instrument der Sicherungsanordnung für sonstige Verkehrsdaten einführen (dazu unten II) und wir wollen die Funkzellenabfrage neu regeln (dazu unten III).

I. Die vorsorgliche Speicherung von IP-Adressen

1. Was sind IP-Adressen?

IP-Adressen sind quasi „Autokennzeichen des Internets“. Jedes Mal, wenn sich ein internetfähiges Gerät (z. B. Smartphone, PC oder Tablet) mit dem Internet verbindet, weist der betreffende Internetzugangsdiensteanbieter (z. B. Telekom, Vodafone, o2 etc.) dem Anschluss, von dem aus das Gerät aktiv ist, eine IP-Adresse zu. Die IP-Adresse (Internetprotokoll-Adresse; Internet Protocol Address) besteht aus einer Kette aus Zahlen und Buchstaben. Ihr Zweck ist es, den betreffenden Anschluss im Netz eindeutig zu identifizieren und so die Kommunikation

zwischen den Geräten zu ermöglichen. Eine IP-Adresse wird üblicherweise dynamisch vergeben. Das heißt, anders als beispielsweise eine Telefonnummer, ändert sie sich ständig. Eine bestimmte IP-Adresse ist einem bestimmten Anschluss also nur für eine gewisse Zeit zugewiesen.

2. Weshalb sind IP-Adressen für die Strafverfolgung wichtig?

Wenn Straftaten im Internet begangen werden, sind IP-Adressen oft die einzige Spur, die ein Täter hinterlässt. Das Gerät, mit dem der Täter im Netz unterwegs ist, kommuniziert mit anderen Geräten. Dabei hinterlässt das Gerät regelmäßig die seinem Anschluss zugewiesene IP-Adresse.

Beispiel: Die Strafverfolgungsbehörden beschlagnahmen einen Server, auf dem kinderpornographisches Material gespeichert ist. Aus dem Verbindungsprotokoll des Servers ergibt sich, von welchen IP-Adressen auf das Material zugegriffen wurde. Die IP-Adresse liefert im besten Fall den Hinweis auf einen bestimmten Internetanschluss; dieser Internetanschluss läuft unter dem Namen einer natürlichen Person, die mit dem Internetzugangsanbieter einen Vertrag über den Internetanschluss abgeschlossen hat.

Allerdings: IP-Adressen werden dynamisch (also nur vorübergehend) vergeben. Deshalb reicht die IP-Adresse allein noch nicht aus, um einen Internetanschluss und dessen Inhaber zu identifizieren. Die Ermittlungsbehörden müssen in Erfahrung bringen, welchem Anschluss die fragliche IP-Adresse zur Tatzeit zugeordnet war. Über diese Information verfügen grundsätzlich die Internetzugangsdiensteanbieter.

3. Warum ist eine vorsorgliche Speicherung von IP-Adressen durch Internetzugangsdiensteanbieter für die Strafverfolgung wichtig?

Nur die Internetzugangsdiensteanbieter können Auskunft darüber geben, welchem Anschluss eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Gegenwärtig sind die Anbieter nicht verpflichtet, diese Informationen zu speichern; viele löschen die fraglichen Informationen schon nach wenigen Tagen. Damit läuft der Ermittlungsansatz ins Leere, den die IP-Adresse liefert. Das bereits bestehende Abfragerecht der Ermittlungsbehörden geht daher aktuell oft ins Leere.

4. Bei der Aufklärung welcher Straftaten kann eine vorsorgliche Speicherung von IP-Adressen helfen?

Eine vorsorgliche Speicherung von IP-Adressen kann grundsätzlich bei allen internetbezogenen Straftaten einen Beitrag zur Aufklärung leisten. Besonders relevant sind IP-Adressen für

die Aufklärung der Verbreitung von Kinderpornographie im Netz. Wichtig sind sie auch für die Aufklärung von Cyber-Betrug und Hasskriminalität im Netz.

5. Welche Daten sollen Internetzugangsdiensteanbieter nach dem Gesetzentwurf vorsorglich speichern? Und wie lange sollen die Daten gespeichert werden?

Die Anbieter sollen verpflichtet werden, vorsorglich die Information darüber zu speichern, welchem Internetanschluss eine IP-Adresse zu einem fraglichen Zeitpunkt zugeordnet war. Diese Daten sollen für drei Monate gespeichert werden. Die Pflicht soll sich auf weitere Daten wie die Portnummern erstrecken, sofern dies für die eindeutige Zuordnung der IP-Adresse zu einem Anschlussinhaber erforderlich ist. Sogenannte Ziel-IP-Adressen (also Informationen über angesurfte Websites und Online-Dienste) sollen hingegen nicht gespeichert werden: Es geht allein um die Sicherung von IP-Adressen an der Quelle.

Andere Informationen sollen nicht vorsorglich gespeichert werden müssen. Insbesondere werden die Anbieter nicht zur vorsorglichen Speicherung von Standortdaten (d. h. Informationen über den geographischen Standort eines internetfähigen Geräts zu einem bestimmten Zeitpunkt) verpflichtet. Gleiches gilt für sonstige Verkehrsdaten: also zum Beispiel Informationen darüber, mit wem oder wann oder wie lange von einem bestimmten Anschluss aus kommuniziert worden ist. Auch diese Daten sind nicht von der Speicherpflicht umfasst.

6. Welche staatlichen Stellen sollen von den Internetzugangsdiensteanbietern Auskunft über gespeicherte Daten verlangen können?

Der Gesetzentwurf sieht insoweit keine Neuerungen im Vergleich zur geltenden Rechtslage vor. Schon heute können Strafverfolgungsbehörden bei Internetzugangsdiensten Auskunft darüber verlangen, welchem Anschluss eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war und welche Person (insbesondere: Name und Adresse) Inhaber des betreffenden Anschlusses ist. Gleiches wird künftig unverändert möglich sein. Auch Polizeibehörden und Nachrichtendienste sollen – wie bislang – Auskunft über die gespeicherten Daten verlangen können. Neu ist nur die Verpflichtung der Anbieter die IP-Adressen, die den Anschlussinhabern zu einem bestimmten Zeitpunkt zugeordnet waren, zu speichern. Zukünftig werden damit die Auskunftsverlangen der staatlichen Behörden nicht mehr ins Leere laufen, weil die Anbieter die fraglichen Daten bereits gelöscht haben.

7. Unter welchen Voraussetzungen sollen Strafverfolgungsbehörden die gespeicherten Daten bei den Internetzugangsdiensteanbietern abfragen können?

Der Gesetzentwurf sieht insoweit keine Neuerung vor: Die Strafverfolgungsbehörden sollen – wie bislang – Auskunft über die Bestandsdaten eines Anschlussinhabers verlangen können,

sofern dies erforderlich ist, um den Sachverhalt zu erforschen oder den Aufenthaltsort eines Beschuldigten zu ermitteln. Notwendig ist also der Anfangsverdacht einer bestimmten Straftat und die Erforderlichkeit der Abfrage. Eine Beschränkung der Abfragemöglichkeit auf bestimmte Straftaten ist – wie bisher – nicht vorgesehen.

8. Ist die vom Gesetzentwurf vorgeschlagene vorsorgliche Speicherung von IP-Adressen mit der Freiheit im Netz vereinbar?

Ja. Mit den gespeicherten IP-Adressen lassen sich keine Persönlichkeits- oder Bewegungsprofile erstellen. Auch die Vertraulichkeit von Kommunikationsinhalten bleibt selbstverständlich gewahrt: Inhaltsdaten sind nicht Gegenstand der vorsorglichen Speicherpflicht. Auch Daten über angesurfte Webseiten und Online-Dienste (Ziel-IP-Adressen) sind nicht von der Speicherpflicht umfasst. Es geht allein um die Speicherung der Daten, die notwendig sind, um nachträglich eine bestimmte IP-Adresse einem bestimmten Internetanschluss zuordnen zu können. Strafverfolgungsbehörden dürfen auf die zu einer gespeicherten Adresse vorhandenen Bestandsdaten (Informationen über die Identität des Anschlussinhabers) im Übrigen nur dann zugreifen, wenn dies erforderlich ist, um eine Straftat aufzuklären. Die zugewiesene IP-Adresse selbst wird nicht an die Behörden herausgegeben werden. Die Möglichkeit zur Abfrage der zu einer IP-Adresse gespeicherten Daten lässt sich am ehesten mit der Möglichkeit zur Halterabfrage bei Kfz-Kennzeichen vergleichen: Das ist auch keine übermäßige Einschränkung bürgerlicher Freiheit (genauso wenig, wie es die Pflicht zur Kfz-Kennzeichnung ist).

9. In der Vergangenheit wurden gesetzliche Regelungen über eine vorsorgliche Datenspeicherungspflicht wiederholt von Gerichten als grundrechtswidrig verworfen. Ist die jetzt vorgeschlagene vorsorgliche Speicherung von IP-Adressen mit Grundrechten vereinbar?

Ja. Der Europäische Gerichtshof hat zuletzt mehrfach ausdrücklich klargestellt, dass eine vorsorgliche Speicherung von IP-Adressen mit europäischen Grundrechten vereinbar ist. Der Entwurf bewegt sich im Rahmen der grundrechtlichen Vorgaben. Die gesetzlichen Regelungen, die in der Vergangenheit für grundrechtswidrig erklärt wurden, waren andere als die jetzt vorgeschlagenen Regeln. Sie hätten insbesondere die Erstellung von Persönlichkeits- und Bewegungsprofil ermöglicht.

10. In der letzten Legislaturperiode hat das BMJV keine vorsorgliche Speicherung von IP-Adressen vorgeschlagen. Stattdessen wurde vorgeschlagen, eine anlassbezogene Speicherung (ein „Einfrieren“) von Verkehrsdaten (sog. Quick-Freeze-Verfahren) zu ermöglichen. Warum verfolgt das BMJV jetzt einen anderen Ansatz?

Die Rückmeldungen von Ermittlerinnen und Ermittlern zum Quick-Freeze-Vorschlag des BMJV aus der letzten Wahlperiode waren eindeutig: Das Quick-Freeze-Verfahren allein ist mit Blick auf das Ziel einer effektiven Strafverfolgung nicht ausreichend effektiv. Es kann in bestimmten Fällen eine sinnvolle Ergänzung sein zu einer vorsorglichen IP-Adressenspeicherung. Aber es kann die vorsorgliche IP-Adressenspeicherung nicht ersetzen. Denn IP-Adressen, deren Zuordnung nicht mehr bei den Anbietern gespeichert ist, können bei einem konkreten Anlass auch nicht „eingefroren“ werden: Wenn die Anbieter die Information gar nicht oder nur kurz speichern, welche IP-Adresse welchem Internetzugang zu einem bestimmten Zeitpunkt zugeordnet ist, dann läuft das anlassbezogene Quick-Freeze-Verfahren leer (Argument des „leeren Kühlschranks“). Eine vorsorgliche IP-Adressenspeicherung lässt sich grundrechtskonform ausgestalten; sie greift in der konkret vorgeschlagenen Form nicht unverhältnismäßig in Grundrechte ein.

II. Die Sicherungsanordnung

1. Was ist der Zweck der Sicherungsanordnung? Wie unterscheidet sich diese Regelung von der vorsorglichen IP-Adressenspeicherung?

Die europarechtlich gebotene Regelung über die Sicherungsanordnung soll ebenfalls bei der Verfolgung von internetbezogener Kriminalität helfen. Sie soll die Regelung über die vorsorgliche IP-Adressenspeicherung ergänzen. Die Sicherungsanordnung zu anderen Daten soll, anders als die vorsorgliche IP-Adressenspeicherung, einen konkreten Anlass voraussetzen.

2. Welche Daten sollen Ermittlungsbehörden mit einer Sicherungsanordnung sichern können?

Mit einer Sicherungsanordnung sollen Ermittlungsbehörden Verkehrsdaten sichern lassen können: also Daten darüber, wer wann mit wem kommuniziert hat. Inhaltsdaten – Informationen über Kommunikationsinhalte – werden nicht Gegenstand einer Sicherungsanordnung sein können. IP-Adressen sollen Internetzugangsdiensteanbieter künftig ohnehin vorsorglich sichern müssen, um über die Identität von Anschlussinhabern Auskunft erteilen zu können (siehe dazu I). Es geht bei der Sicherungsanordnung also um andere Verkehrsdaten – zum Beispiel um Informationen, an welche andere E-Mail-Adresse von einem bestimmten Account wann eine E-Mail verschickt wurde. Die Staatsanwaltschaft soll bei konkretem Anlass

alle gespeicherten Verkehrsdaten zu einem Anschluss sichern lassen können, die bei Telekommunikationsanbietern (das sind Internetzugangsdiensteanbieter und Anbieter von sogenannten Over-The-Top-1-Diensten wie E-Mail- und Messengeranbieter) noch vorhanden sind.

3. Gegen wen soll sich eine Sicherungsanordnung richten? Was ist Gegenstand der Anordnung?

Eine Sicherungsanordnung soll sich gegen die Telekommunikationsanbieter richten, bei denen die fraglichen Verkehrsdaten vorhanden sind. Den Anbietern soll durch die Anordnung aufgegeben werden, bestimmte bei Ihnen vorhandene Daten zu speichern – damit sie ggf. später zum Zwecke der Strafverfolgung verwendet werden können.

4. Unter welchen Voraussetzungen soll die Sicherungsanordnung erfolgen können?

Die Anordnung der Sicherung von Verkehrsdaten soll durch die Staatsanwaltschaft erfolgen können. Im Eilfall sollen auch die Ermittlungspersonen, vor allem die Polizei, die Anordnung erlassen können. Eine Sicherungsanordnung soll voraussetzen, dass es um die Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung geht oder um Straftaten, die mittels Telekommunikation begangen wurden. Mit der Sicherungsanordnung sollen auch Daten von Personen gesichert werden können, von denen zunächst unklar ist, ob sie in ein Tatgeschehen involviert sind. Auch das Bundeskriminalamt soll die Möglichkeit erhalten, zur Erfüllung seiner Aufgaben unter bestimmten Voraussetzungen zu Zwecken der Strafverfolgung und Gefahrenabwehr eine Sicherungsanordnung zu erlassen.

5. Wie lange sollen TK-Anbieter durch eine Sicherungsanordnung verpflichtet werden können, Verkehrsdaten zu sichern?

Die Daten sollen bis zu drei Monate gesichert werden, eine einmalige Verlängerung um bis zu drei Monate soll möglich sein. Für die Verlängerung soll eine richterliche Anordnung erforderlich sein.

6. Unter welchen Voraussetzungen sollen gesicherte Daten abgefragt werden können?

Die Erhebung der Daten im Rahmen eines Strafverfahrens soll nur unter den gleichen Voraussetzungen wie bisher erfolgen können. Eine Abfrage wird also nur möglich sein, wenn dies für die Erforschung des Sachverhalts erforderlich ist und in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Erforderlich ist auch, dass der Verdacht besteht, dass eine Straftat entweder auch im Einzelfall erhebliche Bedeutung hat oder mittels

Telekommunikation begangen wurde. Für die Erhebung der Daten ist außerdem im Regelfall eine richterliche Anordnung nötig.

7. Was ist der Mehrwert der Sicherungsanordnung gegenüber der geltenden Rechtslage?

Schon nach geltendem Recht können Strafverfolgungsbehörden – unter bestimmten rechtlichen Voraussetzungen – auf Verkehrsdaten zugreifen, die bei Telekommunikationsanbietern noch vorhanden sind. Oft laufen diese Zugriffsmöglichkeiten jedoch ins Leere, weil die fraglichen Daten gar nicht mehr vorhanden sind zu dem Zeitpunkt, in dem die rechtlichen Voraussetzungen für den Zugriff vorliegen. Die Sicherungsanordnung soll den Strafverfolgungsbehörden mehr Zeit verschaffen, um die Voraussetzungen für eine Erhebung zu erfüllen, und sicherstellen, dass die Daten noch vorhanden sind. Die rechtlichen Voraussetzungen für einen Zugriff werden nicht abgesenkt; es soll lediglich sichergestellt werden, dass die Daten erst einmal erhalten bleiben.

III. Funkzellenabfrage

Welche Anpassungen sind vorgesehen?

Die Strafverfolgungsbehörden sollen durch eine Anpassung an die Rechtsprechung wieder bei allen Straftaten von auch im Einzelfall erheblicher Bedeutung eine Funkzellenabfrage durchführen können. Dies betrifft beispielsweise den gewerbsmäßigen Betrug. Der Bundesgerichtshof hatte im Januar 2024 entschieden, dass die Funkzellenabfrage nach bisher geltendem Recht nur bei besonders schweren Straftaten wie Mord oder Totschlag zulässig sei.