Gesetzentwurf zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten

- Fragen- und Antwortenpapier -

Zur Speicherpflicht:

1. Welche Daten müssen gespeichert werden?

Gespeichert werden müssen im TKG genau bezeichnete Verkehrsdaten, die bei der Telekommunikation anfallen. Das sind insbesondere die Rufnummern der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, bei Mobilfunk auch die Standortdaten, sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse.

Nicht gespeichert werden dürfen:

- Inhalt der Kommunikation,
- aufgerufene Internetseiten und
- Daten von Diensten der elektronischen Post

2. Wie lange müssen die Daten gespeichert werden?

Hinsichtlich der Speicherdauer wird differenziert zwischen den Standortdaten und den weiteren Verkehrsdaten. Für die Standortdaten wird eine Speicherfrist von vier Wochen, im Übrigen eine Speicherfrist von zehn Wochen bestimmt.

3. Ist die vorgeschlagene Einführung einer Höchstspeicherfrist für Verkehrsdaten mit den Vorgaben des Bundesverfassungsgerichts und des Europäischen Gerichtshofs vereinbar?

Die Vorgaben des Bundesverfassungsgerichts und des Europäischen Gerichtshofs werden eingehalten. Die Regelungen sind deutlich enger als die alte EU-Richtlinie zur Vorratsdatenspeicherung. Es werden weniger Daten für einen deutlich kürzeren Zeitraum gespeichert. Es sollen bei weitem nicht alle Daten gespeichert werden. Die Daten von Diensten der elektronischen Post sind komplett ausgenommen. Hinsichtlich der Speicherfrist wird – ausgehend von der Sensibilität der Daten für den Bürger – nach Datenarten differenziert: Die Höchst-

speicherfrist für Standortdaten beträgt vier Wochen, für die übrigen Verkehrsdaten zehn Wochen.

Auch für den Zugriff auf die Daten werden mit dem strikten Richtervorbehalt, dem sehr engen Straftatenkatalog und Substantiierungsanforderungen hohe Hürden aufgestellt. Auf Standortdaten darf nur einzeln zugegriffen werden, um die Erstellung von Bewegungsprofilen zu vermeiden. Grundrechtseingriffe werden auf das absolut Notwendige beschränkt. Darüber wird für die Bürgerinnen und Bürger Datensicherheit, Transparenz und effektiver Rechtsschutz gewährleistet. Berufsgeheimnisträger werden besonders geschützt.

4. Warum dürfen Standortdaten nur für kurze Zeit gespeichert werden?
Standortdaten sind besonders sensible Daten, weil sie Auskunft darüber geben, in welcher Funkzelle sich ein Mobiltelefon bei einem Kommunikationsvorgang befindet.

Wenn viele Standortdaten über einen längeren Zeitraum ausgewertet werden, lassen sich Regelmäßigkeiten in den Bewegungen einer Person feststellen. Auch Rückschlüsse von den Bewegungen einer Person auf ihre Persönlichkeit werden dann möglich. Diese Gefahr wird noch größer, wenn Standortdaten in Kombination mit anderen Daten, wie zum Beispiel Kreditkartendaten, ausgewertet werden. Die Erstellung solcher Bewegungs- und Persönlichkeitsprofile soll durch die verkürzte Speicherfrist und hohe Hürden für den Abruf solcher Daten verhindert werden.

5. Wie soll die Erstellung solcher Bewegungs- und Persönlichkeitsprofile verhindert werden?
Wir führen enge Grenzen für den Abruf von Standortdaten ein. Zu geschäftlichen Zwecken gespeicherte Standortdaten dürfen nicht mehr abgerufen werden. Abgerufen werden dürfen nur noch die verpflichtend gespeicherten Standortdaten. Hier erreichen wir eine Verbesserung des Datenschutzes im Vergleich zum geltenden Recht, indem wir die Höchstspeicherfrist auf lediglich vier Wochen festsetzen und so den Zeitraum beschränken, für den gespeicherte Standortdaten zur Verfügung stehen. Zudem ist der Abruf nur unter den strengen Voraussetzungen möglich, die für den Abruf aller verpflichtend zu speichernden Verkehrsdaten gelten. Schließlich werden hohe Anforderungen an die Verhältnismäßigkeit der

Standortdatenerhebung gestellt. Um die Erstellung von Bewegungsprofilen zu verhindern, sollen Standortdaten nur einzeln abgerufen werden. Lediglich im Ausnahmefall, z.B. wenn es für die Aufklärung einer Serientat unerlässlich ist, dürfen mehrere Standortdaten abgerufen werden.

6. Wer ist berechtigt, die gespeicherten Daten abzurufen?

Die Strafverfolgungsbehörden dürfen die gespeicherten Daten zu eng definierten Strafverfolgungszwecken abrufen. Den Ländern wird ermöglicht, einen Abruf der Verkehrsdaten in ihren Polizeigesetzen zu regeln, wenn tatsächliche Anhaltspunkte für bestimmte konkrete schwerste Gefahren vorliegen.

Nachrichtendienste wie der BND sind nicht Gegenstand des Gesetzentwurfs und erhalten keinen Zugriff auf die Daten.

7. Wie werden Berufsgeheimnisträger geschützt?

Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, sind grundsätzlich von der Speicherpflicht ausgenommen.

Darüber hinaus dürfen Verkehrsdaten in Bezug auf alle nach § 53 StPO zeugnisverweigerungsberechtigten Personen (insbesondere Geistliche, Rechtsanwälte, Ärzte, Apotheker, Beratungsstellen für Betäubungsmittelabhängigkeit und Schwangerschaftskonflikte, Abgeordnete, Presse) nicht abgerufen werden. Zufallsfunde unterliegen einem Verwertungsverbot.

8. Warum kann im TKG keine Möglichkeit vorgesehen werden, alle Berufsgeheimnisträger bereits von der Speicherpflicht auszunehmen?

Unter Datenschutzgesichtspunkten ist es nicht vertretbar, eine Art Datenbank mit Berufsgeheimnisträgern und ihren Rufnummern anzulegen und bei allen TK-Anbietern zu hinterlegen. Es gibt in Deutschland ca. 1000 TK-Anbieter; die Erstellung, Übermittlung und Aktualisierung

einer solchen Liste von Berufsgeheimnisträgern würde ein erhebliches Missbrauchsrisiko bergen. Der Eingriff in deren Berufsfreiheit und ihr Recht auf informationelle Selbstbestimmung wäre größer als der Nutzen, der in der Ausnahme von der Speicherung liegt. Der Ausschluss der Verwendung der Verkehrsdaten von Berufsgeheimnisträgern bietet daher größeren Schutz. Erhebungs- und Verwertungsverbote haben sich auch in anderen Regelungen der StPO bewährt.

Bei dynamischen IP-Adressen ist eine Ausnahme von der Speicherung technisch nicht möglich. So hat zum Beispiel eine Anwaltskanzlei in der Regel keine nur ihr zugewiesene IP-Adresse, vergleichbar einer Telefonnummer, sondern bekommt wie die meisten Internet-Nutzer vorübergehend eine Adresse zugewiesen, die nach Abschluss der Nutzung dem nächsten Kunden zugewiesen wird.

9. In Bezug auf welche Straftaten ist der Abruf der Daten zulässig?

Der Abruf der nach § 113b TKG-E gespeicherten Daten ist im Bereich der Strafverfolgung nur zur Verfolgung von katalogmäßig aufgeführten besonders schweren Straftaten zulässig, die auch im Einzelfall besonders schwer wiegen müssen. Dabei ist der Katalog im Vergleich zu dem Katalog, der nach der vorhergehenden, vom BVerfG verworfenen Regelung maßgeblich war, deutlich reduziert und lehnt sich an den Katalog zur Wohnraumüberwachung an. Erfasst werden insbesondere terroristische Straftaten und Straftaten gegen höchstpersönliche Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung.

Im Bereich der Gefahrenabwehr ist der Abruf durch die Länder zulässig, wenn diese sie zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes benötigen und eine entsprechende landesgesetzliche Erlaubnisregelung vorhanden ist.

10. Können Verbindungs- und Standortdaten auch dann abgerufen werden, wenn der enge Straftatenkatalog nicht erfüllt ist, sondern beim bloßen Verdacht auf "mittels Telekommunikation begangene" Straftaten?

Nein, die aufgrund der neu eingeführten Speicherpflicht gespeicherten Verbindungs- und Standortdaten können nicht beim bloßen Verdacht auf „mittels Telekommunikation began-

gene“ Straftaten abgerufen werden. Erforderlich ist hier stets das Bestehen eines Verdachts in Bezug auf eine Katalogtat.

Aus geschäftlichen Gründen gespeicherte Verbindungsdaten im Sinne des § 96 TKG können bereits nach geltendem Recht abgerufen werden, wenn der Verdacht besteht, dass eine Straftat mittels Telekommunikation begangen worden ist (§ 100g Absatz 1 Satz 1 Nr. 2 StPO). Dies wird auch künftig so bleiben.

Anders als nach dem geltenden Recht können Standortdaten jedoch nicht mehr abgerufen werden, wenn der Verdacht besteht, dass eine Straftat mittels Telekommunikation begangen worden ist. Es darf nur noch auf die verpflichtend zu speichernden Standortdaten zugegriffen werden und dies nur unter den engen Voraussetzungen des neuen § 100g Absatz 2 StPO-E, d.h. bei Vorliegen einer Katalogtat.

11. Ist ein Richtervorbehalt vorgesehen?

Ja, die Leitlinien sehen einen umfassenden Richtervorbehalt für den Abruf der nach § 113b TKG-E gespeicherten Daten durch die Strafverfolgungsbehörden vor. Eine Eilkompetenz der Staatsanwaltschaft besteht – wie bei der Wohnraumüberwachung nach §§ 100c, 100d StPO – für den Abruf dieser Daten nicht. Die Verkehrsdatenerhebung nach § 100g Absatz 1 StPO, die nicht auf die nach § 113b TKG-E gespeicherten Daten zugreift, ist wie zuvor mit einem Richtervorbehalt mit Eilkompetenz der Staatsanwaltschaft ausgestattet.

12. Dürfen die auf Vorrat gespeicherten Daten zur Verfolgung von Ordnungswidrigkeiten verwendet werden?

Nein, die nach § 113b TKG-E gespeicherten Daten dürfen nicht zur Verfolgung von Ordnungswidrigkeiten übermittelt werden.

Sie dürfen auch nicht im Rahmen von Bestandsdatenauskünften zur Zuordnung dynamischer IP-Adressen verwendet werden, wenn es um die Verfolgung von Ordnungswidrigkeiten geht. Da die Zuordnung dynamischer IP-Adressen nach dem Urteil des BVerfG einen Eingriff in das Fernmeldegeheimnis nach Artikel 10 GG darstellt, ist der Rückgriff auf die nach § 113b TKG-E gespeicherten Daten zur Zuordnung von dynamischen IP-Adressen im Rahmen einer Be-

standsdatenauskunft für die Verfolgung von Ordnungswidrigkeiten nicht zulässig. Das ergibt sich aus § 46 Absatz 3 Satz 1 OWiG.

13. Erfahren die Betroffenen von dem Abruf der Daten?

Der Abruf der Daten ist keine verdeckte Maßnahme. Deshalb wurden die Worte „auch ohne Wissen des Betroffenen“ in § 100g StPO gestrichen. Die betroffenen Personen sind grundsätzlich vor der Erhebung der Daten zu benachrichtigen. Eine Verwendung der Daten ohne Wissen des Betroffenen ist nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist (BVerfGE 125, 260 <335 f.>).

Ist eine heimliche Verwendung nach gerichtlicher Prüfung ausnahmsweise zulässig, bedarf es grundsätzlich einer nachträglichen Benachrichtigung.

14. Ist die Sicherheit der gespeicherten Daten gewährleistet?

Die nach dem Stand der Technik höchstmögliche Sicherheit der Daten sowohl bei der Aufbewahrung als auch bei der Übermittlung wird gewährleistet. Die Anbieter müssen die Daten gegen unbefugte Kenntnisnahme und Verwendung schützen. Die Speicherung hat im Inland zu erfolgen. Konkret vorgesehen sind insbesondere der Einsatz eines besonders sicheren Verschlüsselungsverfahrens, die Speicherung in gesonderten Speichereinrichtungen mit einem hohen Schutz vor Zugriffen aus dem Internet, die revisionssichere Protokollierung des Zugriffs sowie die Gewährleistung des Vier-Augen-Prinzips für den Zugriff auf die Daten.

Zudem sind effektive Sicherungen zur Gewährleistung der Löschung der Daten sowohl für die TK-Anbieter als auch für die Strafverfolgungsbehörden vorgesehen. Verfassungsrechtlich geboten ist auch das Sanktionssystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst.

Generell wird ein hoher Standard der Datensicherheit gewahrt, der sich an dem Stand der Technik orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Dies wird durch die Bundesnetzagentur kontrolliert.

15. Was geschieht mit den Daten nach Ablauf der Höchstspeicherfrist?

§ 113b Absatz 8 TKG-E bestimmt, dass die Verkehrsdaten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfrist zu löschen sind oder deren Löschung sicherzustellen ist. Das Löschen der Daten hat nach dem Stand der Technik zu erfolgen, zu dem der Anforderungskatalog nach § 113f TKG-E Orientierung gibt. Die Löschung der Daten ist nach § 113e Absatz 1 TKG-E zu protokollieren.

16. Gibt es eine Sanktionierung, wenn die TK-Anbieter der Löschverpflichtung oder anderen Pflichten zur Datensicherheit nicht nachkommen?

Ja, Verstöße gegen die Bestimmungen zur Sicherung und zum Schutz der Daten werden als Ordnungswidrigkeiten geahndet. Das gilt u.a. für den Fall, dass die TK-Anbieter die gespeicherten Daten nicht rechtzeitig löschen, für andere als die vorgesehenen Zwecke verwenden oder die Sicherheit der gespeicherten Daten nicht hinreichend gewährleisten. Diese Ordnungswidrigkeiten werden nach § 149 Abs. 2 TKG-E mit Geldbußen zwischen 100.000 und 500.000 EUR geahndet.

17. Wer trägt die Kosten?

Für Kosten, die durch die Übermittlung der abgerufenen Daten entstehen, wird im Justizvergütungs- und -entschädigungsgesetz eine gesonderte Entschädigungsregelung vorgesehen.

Die Kosten, die den TK-Anbietern durch die Speicherpflicht nach § 113b TKG-E und die damit verbundenen Regelungen zur Gewährleistung der Datensicherheit nach den §§ 113d bis 113g TKG-E entstehen, tragen die TK-Anbieter hingegen grundsätzlich selbst.
Wenn für die TK-Anbieter durch die Speicherung eine unverhältnismäßige Kostenlast entsteht, die in solcher Weise erdrosselnde Wirkung hat, dass das Übermaßverbot verletzt ist, können sie für die Umsetzung der Speicherverpflichtung entschädigt werden. Über diese Anträge auf Entschädigung entscheidet die Bundesnetzagentur.

18. Ist eine Evaluierung des Gesetzes vorgesehen?

101b StPO-E sieht die Erstellung einer Statistik über den Abruf von Verkehrsdaten auf der Grundlage von § 100g StPO-E vor. Auf diese Weise bleibt eine spätere Evaluierung des Gesetzes möglich.

19. Wie ist der weitere Zeitplan? Ab wann wird das neue Gesetz angewandt?
Nach dem Kabinettsbeschluss wird der Gesetzentwurf in das parlamentarische Verfahren eingebracht. Der weitere Zeitplan liegt dann in den Händen des Deutschen Bundestages.

Nach Verabschiedung des Gesetzes durch den Bundestag wird den TK-Unternehmen ein Zeitraum von 18 Monaten eingeräumt, um die erforderlichen Maßnahmen (insbesondere technischer Art) zu ergreifen. Dabei geht es um die Sicherstellung der Zugriffsberechtigung, der besonderen Sicherheitsvorkehrungen beim Speichern und der Löschverpflichtungen.

<u>Zur Datenhehlerei:</u>

1. Wieso wird mit dem Referentenentwurf auch eine Vorschrift zur Strafbarkeit der Datenhehlerei eingeführt?
Dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, steht die Notwendigkeit gegenüber, den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen ausreichend zu gewährleisten.

Die geltenden strafrechtlichen Regelungen gegen den Handel mit illegal erlangten Daten sind unzureichend und weisen Schutzlücken auf, die durch die Einführung eines neuen Straftatbestands der Datenhehlerei geschlossen werden.

Dem Berechtigten wird mit der Vortat die ihm zustehende Entscheidung, wem seine Daten zugänglich sein sollen, aus der Hand genommen. Durch die Datenhehlerei wird dieses Unrecht aufrechterhalten und vertieft.

2. Machen Journalisten sich strafbar, wenn sie illegal beschaffte Daten eines Whistleblowers erwerben und für ihre Berichterstattung verwenden?
Nein, denn journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung sind vom Tatbestand der Datenhehlerei ausgeschlossen. § 202d StGB-E sieht in Absatz 3 einen

Tatbestandsausschluss für Handlungen vor, die ausschließlich zu dem Zwecke der Erfüllung rechtmäßiger beruflicher Pflichten dienen.

Dazu gehören insbesondere solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen. Darunter fällt, wer bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirkt oder mitgewirkt hat.

Für die beruflichen Pflichten kommt es nicht darauf an, ob diese von dritter Seite auferlegt wurden, so dass auch die freie Entscheidung des Journalisten im Rahmen seiner beruflichen Tätigkeit erfasst wird.