

AKTUELL

EINFÜHRUNG EINER SPEICHERPFLICHT UND HÖCHSTSPEICHERPFLICHT FÜR VERKEHRSDATEN

Die SPD hat auf dem Bundesparteitag 2011 beschlossen, dass es in Deutschland nur unter extrem restriktiven Bedingungen eine Speicherung von Telekommunikationsverbindungsdaten geben darf. Eine Verwendung der Daten, bspw. wer mit wem wann telefoniert hat, darf es nur zur Bekämpfung von schweren Verbrechen geben. Die Vorgaben des Bundesverfassungsgerichts haben wir in unserem Beschluss noch einmal verschärft.

Am 27. Mai hat das Bundeskabinett einen Gesetzentwurf „zur Einführung einer Speicherpflicht und Höchstspeicherpflicht für Verkehrsdaten“ beschlossen. Auch um europäischem Recht zu entsprechen, ist dieser Entwurf noch einmal restriktiver gefasst als der Beschluss, den wir 2011 gefasst haben. Geregelt ist in dem Gesetzentwurf abschließend, welche Daten wie lange gespeichert werden dürfen. Hierzu zählen die Rufnummern, der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, bei Mobilfunk auch die Standortdaten. Zudem wird die sogenannte IP-Adresse gespeichert, also quasi das Nummernschild, mit dem ein Internetnutzer zu einem bestimmten Zeitpunkt auf der Datenautobahn unterwegs ist.

- **Nicht gespeichert werden dürfen:**
 - jedweder Inhalt von Kommunikation;
 - Verbindungsdaten im Zusammenhang mit verschickten Emails;
 - die von einem Nutzer aufgerufenen Internetseiten.
- Darüber hinaus dürfen auch **keine Persönlichkeits- und Bewegungsprofile** aufgrund der gespeicherten Daten erstellt werden.
- Die bei Mobiltelefonaten anfallenden **Standortdaten dürfen höchstens vier Wochen alle anderen Daten höchstens zehn Wochen gespeichert** werden. Alle Daten müssen **unmittelbar nach Ablauf der Fristen gelöscht** werden.
- Die Erlaubnis, die gespeicherten Daten bei einem Unternehmen (Telekom, Vodafone, E-Plus etc.) abrufen zu dürfen, darf **nur von einem Richter erteilt** werden und nur bei einem **Verdacht, dass ein einer ihrer Kunden eine schwere Straftat begangen hat. Kunden, deren Daten gespeichert und verwendet werden**, bekommen grundsätzlich hierüber eine **Benachrichtigung**.
- Die **Daten von allen Berufsgeheimnisträgern dürfen ausdrücklich nicht abgerufen** werden. Tabu sind damit die Daten von Seelsorgerinnen und Seelsorgern, Rechtsanwältinnen und -anwälten, Ärztinnen und Ärzten, Apothekerinnen und Apothekern, Abgeordneten, Journalistinnen und Journalisten, Beratungsstellen für Betäubungsmittelabhängigkeit und Schwangerschaftskonflikte sowie weitere kirchliche und soziale Beratungsstellen für seelische und soziale Notlagen.
- Die Telekommunikationsunternehmen, die die Daten kurzfristig speichern, müssen **Maßnahmen zur höchstmöglichen Sicherung der Daten vor unbefugtem Zugriff** garantieren.

Warum unterstützt die SPD die Speicherung von Kommunikationsdaten?

Ohne Zweifel ist die Verpflichtung der Telekommunikationsunternehmen, die Verbindungsdaten ihrer Kunden für einen kurzen Zeitraum zu speichern, ein Eingriff in deren Grundrechte. Die Urteile des Bundesverfassungsgerichts von 2010 und des Europäischen Gerichtshofes von 2014 haben diesen Eingriffen zu recht enge Grenzen gesetzt. Gleichzeitig kann niemand bestreiten, dass Telekommunikationsdaten für die Strafverfolgung von schwerstverbrechern von erheblicher Bedeutung sind. Dabei geht es um „schwerste Straftaten gegen Leib, Leben oder sexuelle Selbstbestimmung“ (so der Beschluss des SPD-Bundesparteitags 2011).

Die Digitalisierung unserer Gesellschaft geht weiter rasant voran. Sie ist ein enorm wichtiger Motor für Innovations- und Zukunftsfähigkeit Deutschlands. Aber allen muss klar sein, dass auch Kriminelle und Schwerstkriminelle die Möglichkeiten digitaler Techniken nutzen.

Für die SPD gilt der Grundsatz: Wer die Möglichkeiten der Digitalisierung als Tatwerkzeug für Verbrechen missbraucht, dem müssen Ermittlungsbehörden ein rechtsstaatlich einwandfreies Instrument zur Strafverfolgung entgehen können.

Im Bundesparteitagsbeschluss von 2011 ist sehr klar formuliert worden, welche restriktiven Voraussetzungen für die Vorratsdatenspeicherung erfüllt sein müssten:

- Nur eine kurze Speicherung der Daten bei den Providern.
- Höchste Datenschutzstandards müssen gewahrt sein.
- Abruf der Daten bei den Providern nur bei Verdacht auf schwerste Straftaten und mit qualifiziertem Richtervorbehalt (3 Richter, wie bei Anordnung von Wohnungsdurchsuchungen).
- Das Verbot Bewegungsprofile von Kunden anzulegen.
- Daten von Berufsgeheimnisträgern und -trägerinnen dürfen nicht abgefragt werden.

Beispiele für den sinnvollen Einsatz gespeicherter Daten

- **Mit „Handydaten“ können Mörder überführt werden.** In einigen Fällen konnte ein Mordversuch mittels noch zufällig vorhandener Information, dass sich das Handy eines Tatverdächtigen in einer bestimmten Funkzelle befand, aufgeklärt werden. Der öffentlich bekannt gewordene „Flensburger Bahnhofs-

mord“ wäre ohne ebenfalls nur zufällig vorhandener Mobil- daten nie aufgeklärt worden, sondern wäre als Suizid zu den Akten gelegt worden. Mit dem neuen Gesetz überlassen wir es nicht mehr dem Zufall, dass Daten zur Aufklärung vollendet oder geplanter Verbrechen führen, sondern sorgen dafür, dass die Daten über einen kurzen Zeitraum zur Verfügung stehen und zur Aufklärung eingesetzt werden können?

■ **Mit der Zuordnung einer IP-Adresse kann / könnte man Täter, Käufer, Besitzer von Kinderpornografie überführen.**

Vor allem bei Verbrechen, die aus und im Internet begangen werden ist die Speicherung der Verbindungsdaten oft der einzige Weg, Verbrecher zu überführen. Die IP-Adresse ist quasi das „Nummernschild“, mit dem wir im Internet unterwegs sind. Die Ziffernfolge wird bei jedem Internetzugriff neu vom Provider vergeben (dynamische IP).

Bei 90 Prozent der Anfragen der Ermittler geht es laut Bundeskriminalamt um die IP-Adresse. In den meisten Fällen geht es dabei um brutalen Missbrauch von Kindern und Kinderpornografie. Ein Beispiel, das die Dramatik der fehlenden Zuordnungsmöglichkeit der IP-Adresse verdeutlicht (BKA, Fall nach Wegfall der VDS durch BVerfGE von 2010): *In einem Forum wurde ein Hinweis eingestellt, in dem eine Mutter mitteilt, dass ihr Sohn vom Stiefvater missbraucht und in Teilen zu diesem Zweck sogar mit Medikamenten ruhig gestellt werde. Ausschließlich die IP-Adresse war sichtbar. Das Auskunftersuchen beim Provider wurde noch am gleichen Tag gestellt, jedoch nicht beauskunftet. Eine Überprüfung am gleichen Tag ergab, dass keine Anhaltspunkte für einen weiteren zuzuordnenden Login vorlagen. Aus dem Inhalt des Textes ergaben sich ebenfalls keine Hinweise auf die Identität des Users. Dem konkreten Verdacht eines schweren Kindesmissbrauch konnten die Ermittler mangels Auskunft über Inhaber der IP-Adresse nicht nachgehen.*

Bundesjustizminister Heiko Maas:

„Wir haben klare und transparente Regeln zu Höchstspeicherfristen von Verkehrsdaten beschlossen. Damit wahren wir die Balance zwischen Freiheit und Sicherheit in der Digitalen Welt. Den Sicherheitsbehörden geben wir bei schweren Straftaten ein zusätzliches Instrument. Die Privatsphäre schützen wir: Eine Speicherung darf nur in äußerst engen Grenzen erfolgen. Inhalte werden nicht gespeichert. Das Recht auf unbeobachtete Kommunikation erhalten wir. Bewegungsprofile dürfen nicht erstellt werden. Emails werden nicht erfasst. Die Speicherfristen sind weit kürzer, der Zugriff auf die Daten deutlich schwerer als zuvor.“