

# Medieninformation

Sächsisches Staatsministerium des Innern

**Ihr Ansprechpartner**  
Martin Strunden

**Durchwahl**  
Telefon +49 351 564 30400  
Telefax +49 351 564 30409

presse@smi.sachsen.de\*

08.04.2014

## Entscheidung des Europäischen Gerichtshofes über Vorratsdatenspeicherung

**Ulbig: „Jetzt sollte es zügig einen Gesetzentwurf geben“**

Der Europäische Gerichtshof hat die europäische Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt, weil die Beeinträchtigung der Grundrechte nicht auf das notwendige Maß beschränkt und damit der Grundsatz der Verhältnismäßigkeit nicht eingehalten wird. Konkret kritisiert der Gerichtshof fehlende Konturen bei der Regelung der betroffenen Personen, Kommunikationsmittel und Verkehrsdaten. Auch seien hinreichende Garantien dafür erforderlich, dass die Daten für die Dauer der Vorratsdatenspeicherung vor Missbrauch geschützt sind. Der Europäische Gerichtshof hat darüber hinaus die fehlende Präzisierung bei der Dauer der Speicherung bemängelt.

Innenminister Markus Ulbig: „Der Bundesgesetzgeber hat jetzt Hinweise, an denen sich eine Regelung zur Vorratsdatenspeicherung orientieren sollte. Jetzt sollte es zügig einen Gesetzentwurf geben. Ich halte die Vorratsdatenspeicherung unter engen Voraussetzungen für ein wichtiges Mittel, um schwere Straftaten schnell aufzuklären.“

Zur Vorratsdatenspeicherung:

Mit der Zunahme der Telekommunikation nimmt auch die Bedeutung der Vorratsdatenspeicherung zu. Damit können Telekommunikationsdaten überhaupt hinreichend ausgewertet und Beweise für mögliche Ermittlungsverfahren beschafft werden. Immer häufiger ist die Beweiskette nur dadurch zu schließen. Besonders bei schwerwiegender Kriminalität ist das wichtig. Strafverfolgungsbehörden sollen dabei mit richterlicher Anordnung auf länger zurückliegende Verbindungsdaten zurückgreifen können, um Terrorismus, international organisierte Kriminalität und Sexualstraftaten, wie beispielsweise sexuellen Missbrauch und Kinderpornographie zu bekämpfen. Der Zugriff auf die von

**Hausanschrift:**  
**Sächsisches Staatsministerium  
des Innern**  
Wilhelm-Buck-Straße 2  
01097 Dresden

[www.smi.sachsen.de](http://www.smi.sachsen.de)

Zu erreichen mit den  
Straßenbahnlinien 3,6,7,8,9, 11  
und 13. Haltestelle Carolaplatz.

\* Kein Zugang für verschlüsselte elektronische Dokumente. Zugang für qualifiziert elektronisch signierte Dokumente nur unter den auf [www.lsf.sachsen.de/eSignatur.html](http://www.lsf.sachsen.de/eSignatur.html) vermerkten Voraussetzungen.

Telekommunikationsanbietern gespeicherten Vorratsdaten ist keinesfalls im Bereich der Massen- und Kleinkriminalität zulässig.

Bei den folgenden vier Fallbeispielen aus Sachsen ist auf Grundlage der bis 2010 in der Bundesrepublik Deutschland geltenden Vorratsdatenspeicherung ein Ermittlungserfolg gelungen:

#### 1. Tötungsdelikt

Im August 2009 wurde in einem Steinbruchsee eine drei Tage alte Frauenleiche gefunden. Der später zu lebenslanger Freiheitsstrafe verurteilte Hauptangeklagte konnte schon einen Tag später festgenommen werden. Die vorläufige Festnahme des später wegen Strafvereitelung verurteilten Mitangeklagten erfolgte Ende Oktober 2009. Mittels der eine Woche bzw. einen Monat nach der Tat erhobenen Telekommunikationsdaten konnte das Tatgeschehen und das gemeinschaftliche Handeln beider Personen beim Verbringen des Fahrzeuges der Geschädigten nachgewiesen werden. Nach aktueller Rechtslage wären bereits eine Woche nach der Tat keine Daten mehr vorhanden gewesen.

#### 2. Tötungsdelikt

Im September 2009 wurde eine Person tot in seiner Wohnung aufgefunden. Sie wies erhebliche Verletzungen auf. In dem Ermittlungsverfahren wurde ein Bezug in das Rotlichtmilieu aufgedeckt. Die Täter konnten mit an Sicherheit grenzender Wahrscheinlichkeit nur mit Hilfe der aufwändig geführten Auswertungen retrograder Verbindungsdaten sowie einer Funkzellenanalyse ermittelt werden. Zudem trug die Aufarbeitung dieser Daten, speziell der Funkzellenanalyse, maßgeblich zur Verurteilung der vier Täter bei. Gegen alle Beteiligten wurden Haftstrafen verhängt. Die beiden Haupttäter wurden zu lebenslangen Haftstrafen verurteilt. Bei geltender Rechtslage wäre die Aufklärung über einen für Ermittlungsarbeit mindestens notwendigen Zeitraum nicht sichergestellt gewesen.

#### 3. Computersabotage

Im Oktober 2009 wurden mehrere sogenannte Ping-Attacken auf einen Server der geschädigten Computerfirma festgestellt. Der Angriff richtete sich auf eine für die Bundeswehr wesentliche Datenverbindung für die in Afghanistan eingesetzten Truppen. In einem darauf geführten Ermittlungsverfahren wegen des Verdachts der Computersabotage konnte als Absender der Attacken eine IP-Adresse ausgemacht werden. Aufgrund der Vorratsdatenspeicherung konnte der zuständige Provider den Anschlussinhaber sowie späteren Beschuldigten feststellen und weitere beweissichernde Maßnahmen einleiten, wie die Sicherstellung des Tatmittels. Bei geltender Rechtslage wäre die Aufklärung über einen für Ermittlungsarbeit mindestens notwendigen Zeitraum nicht sichergestellt gewesen.

#### 4. Computerbetrug

Durch die in banden- und gewerbsmäßigen Strukturen arbeitenden Täter wird mittels Kartenlesegerät sowie Aufsatztastatur ein Geldautomat einer Filiale der Deutschen Bank AG in Chemnitz manipuliert, um so die Daten von Zahlungskarten sowie der zugehörigen PIN rechtswidrig zu erlangen. Gleichzeitig fand in Dresden eine gleichartige Manipulation

des gleichen Automatentyps statt. Nach Ermittlung der Tatverdächtigen führten die Funkzellenanalyse und die Erhebung der Verkehrsdaten nicht nur zur vollumfänglichen Aufklärung der Tathandlung sondern auch zur Identifizierung weiterer Tatorte. Bei geltender Rechtslage wäre die Aufklärung über einen für Ermittlungsarbeit mindestens notwendigen Zeitraum nicht sichergestellt gewesen.