Speicherpflichten von und Auskunftserteilung über Verkehrsdaten der Telekommunikation

Vortragsreihe des CCCS e.V.

Bibliothek am Mailänder Platz • 13.07.2017

Thomas Hochstein

Themenübersicht

- ⇒ Einführung und Grundlagen
  - Arten von Daten und abgestufter Grundrechtsschutz
  - Bedürfnis zur Abfrage und Speicherung von Verkehrsdaten
  - Überblick über die verfassungs- und europarechtliche Rechtsprechung
- ⇒ Speicherpflicht und Auskunftserteilung
  - Speicherung von Verkehrsdaten
  - Rechtsgrundlagen für die Auskunftserteilung, insbesondere im Bereich der Strafverfolgung
  - Benachrichtigungs- und Löschungspflichten
- ⇒ Speicherpflichten: Aktueller Umsetzungsstand
- ⇒ Fragen und Diskussion

Einführung und Grundlagen

Bildnachweis: Justitia © Freelancer0111 / Pixelio

Arten von Daten

Telekommunikationsgeheimnis

informationelle Selbstbestimmung

Inhaltsdaten — *§ 100a StPO*

Standortdaten

Verkehrsdaten — §§ 96 Abs. 1, 113b TKG; *§ 100g Abs. 1–3 StPO*

Nutzungsdaten — §§ 15 Abs. 5 S. 4, 14 Abs. 2 TMG; *§§ 161, 163 StPO*

IP-Adressnutzer — § 113 Abs. 1 S. 3 TKG; *§ 100j Abs. 2, Abs. 1 S. 1 StPO*

Zugangsdaten — § 113 Abs. 1 S. 2 TKG; *§ 100j Abs. 1 S. 2 StPO*

Bestandsdaten — §§ 112–113 TKG; § 14 TMG; *§ 100j Abs. 1 S. 1 StPO*

Abfrage von Verkehrsdaten

⇒ Verkehrsdaten werden – für Zwecke der Strafverfolgung – immer dann benötigt, wenn

- Täter zu identifizieren sind
- ein Tatnachweis zu führen (oder ein mutmaßlicher Täter auszuschließen) ist
- der Aufenthalt eines Täters festzustellen ist

⇒ Das kann betreffen

- die Feststellung von Rufnummern bzw. Anschlusskennungen von Kommunikationsteilnehmern
- die Identifizierung von Nutzern einer Kennung
- die Feststellung von Kennungen von Personen in einem bestimmten räumlichen Bereich
- die Feststellung des Aufenthalts von Nutzern

Warum Speicherpflichten?

⇒ Eine Speicherung von Verkehrsdaten für eigene Zwecke der Provider erfolgt zunehmend selten.

- Flatrates u.ä. Abrechnungsmodelle
- größeres Bewusstsein für Datenschutz und entsprechende gesetzliche Regelungen

⇒ In der Folge werden Verkehrsdaten

- teilweise gar nicht mehr
- oder nur noch kurz,
- jedenfalls aber – je nach Provider – für stark unterschiedliche, teilweise wechselnde Zeiträume

gespeichert und stehen daher für Zwecke der Strafverfolgung nicht mehr zur Verfügung.

Bisherige Regelungen

⇒ Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten vom 13.04.2006

- mindestens sechs, höchstens 24 Monate
- Telefonie, Internetzugang, E-Mail-Verkehr
- Umsetzungsfrist: 15.07.2007 (15.03.2009)

⇒ Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007

- Speicherpflicht für sechs Monate
- Telefonie, Internetzugang, E-Mail-Verkehr
- Speicherpflichten auch für die Umschreibung von Daten (Caches, Proxys)

Rechtsprechung I

⇒ BVerfG, Urteil vom 02.03. 2010 – 1 BvR 256/08

- sechsmonatige Vorratsdatenspeicherung ist verfassungsrechtlich zulässig
- Ausgestaltung muss die Eingriffstiefe berücksichtigen:
  - gesetzlich geregelter hoher Datensicherheitsstandard
  - Verwendung nur für bestimmte schwere Straftaten
  - unverzügliche Auswertung und ggf. Löschung
  - ggf. Einschränkung nach Umfang und Art der Daten
  - Transparenz: grundsätzliche Offenheit, Benachrichtigung
- Ablehnung einer befristeten Weitergeltungsanordnung mit denkbar knappen Stimmenverhältnis (4:4)
- Aufhebung der entsprechenden Vorschriften als mit dem Grundgesetz unvereinbar und nichtig

Rechtsprechung II

⇒ EuGH, Urteil vom 08.04. 2014 – C-293/12 u.a.

- Richtlinie zur Vorratsdatenspeicherung ist ungültig
- Die grundsätzlich zulässige Vorratsdatenspeicherung muss auf das absolut Notwendige beschränkt bleiben.
- Dies ist nicht gegeben, wenn sie
  - uneingeschränkt alle Kommunikationsmittel und Verkehrsdaten erfasst,
  - auch Personen ohne auch nur entfernten Zusammenhang mit schweren Straftaten erfasst,
  - auch Berufsgeheimnisträger erfasst,
  - keinen Zusammenhang zwischen den Daten und einer Gefahr für die öffentliche Sicherheit verlangt,
  - keine Anforderungen an den Datenzugriff stellt und
  - uneingeschränkt eine Mindestfrist von 6 Monaten vorgibt.
- Außerdem fehlen Vorschriften zum Datenschutz.

Rechtsprechung III

⇒ EuGH, Urteil vom 21.04. 2016 – C-203/15 u.a.

- Vorabentscheidungsersuchen (Schweden und UK)
- Nationale Regelungen zur Vorratsdatenspeicherung müssen
  - die Umstände und Voraussetzungen für eine Vorratsdatenspeicherung regeln, um deren Beschränkung auf das absolut Notwendige zu sichern,
  - objektive Kriterien für einen Zusammenhang zwischen den Daten und der Bekämpfung schwerer Straftaten enthalten, um den Umfang der Speicherung und die betroffenen Personenkreise wirksam zu begrenzen und
  - durch objektive Anknüpfungspunkte nur solche Personenkreise erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, bspw. durch die Beschränkung auf bestimmte geographische Bereiche.

Historie der Auskunftspflichten

⇒ **1928**: § 12 FAG (Fernmeldeanlagengesetz)
- „Bedeutung für die Ermittlungen“

⇒ 01.01.**2002**: §§ 100g, 100h StPO
- Definition von Verbindungsdaten
- keine ausdrückliche Regelung der Funkzellenabfrage

⇒ 01.01.**2008**: § 100g StPO
- Verweisung auf das TKG
- Regelung der Funkzellenabfrage

⇒ 18.12.**2015**: § 100g StPO (§§ 101a, 101b StPO)
- getrennte Regelung für Speicherpflicht-Daten
- getrennte Regelung für Standortdaten
- (wieder) Sonderregelungen unter Abänderung der allgemeinen Regelungen für verdeckte Maßnahmen

SPEICHERUNG VON VERKEHRSDATEN

Verkehrsdaten

⇒ § 96 TKG regelt grundsätzlich die Erhebung und Speicherung von Verkehrsdaten für Zwecke der Telekommunikationsanbieter.

- (Ruf-)Nummer / Anschlusskennung u.ä.
- Standortdaten
- Beginn / Ende der Verbindung, Datenvolumen (bei Entgeltrelevanz)
- genutzter Telekommunikationsdienst
- sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation oder zur Abrechnung erforderliche Daten

⇒ Speicherung / Verwendung nur zulässig, soweit gesetzlich ausdrücklich erlaubt

Speicherrechte

⇒ Entgeltermittlung und –abrechnung (§ 97 TKG)
- Ermittlung der zur Abrechnung erforderlichen Daten
- Speicherung bis zu 6 Monate nach Rechnungsversand
- Löschung der nicht erforderlichen Daten

⇒ Erstellung eines Einzelverbindungsnachweises (EVN, § 99 TKG)

⇒ Nutzung von Standortdaten für „location based services“ (§ 98 TKG)

⇒ Störungsbeseitigung und Missbrauchsbekämpfung (§ 100 TKG)
- Dies umfasst die generelle Protokollierung dynamischer IP-Adressen für bis zu sieben Tage (BGH, Urteil vom 03.07.2014 – III ZR 391/13)

Speicherpflichten

⇒ Verpflichtet zur Speicherung sind Erbringer
- in der Regel gegen Entgelt erbrachter
- öffentlich zugänglicher Telekommunikationsdienste
- für Endnutzer

⇒ Wer nicht alle erforderlichen Daten selbst erzeugt oder verarbeitet, muss dafür sorgen, dass die Daten anderweitig gespeichert werden.

⇒ Der Verpflichtete muss die gespeicherten Daten technisch und organisatorisch besonders sichern (§§ 113d–113g TKG).

⇒ Einzelheiten regelt die BNetzA.
(Anforderungskatalog nach § 113f TKG vom 16.11.2016)

Zu speichernde Daten

⇒ Gespeichert werden müssen
- **Verkehrsdaten** für **10 Wochen** (70 Tage)
- **Standortdaten** für **4 Wochen** (28 Tage)

⇒ Telefonieanbieter:
- Rufnummer / Kennung beider Teilnehmer, bei Mobiltelefonie auch IMSI/IMEI
- Datum / Uhrzeit von Beginn / Ende der Verbindung
- genutzter Telekommunikationsdienst
- bei VoIP zusätzlich IP-Adressen / Nutzerkennungen

⇒ Internetzugangsanbieter:
- IP-Adresse / Anschlusskennung / Nutzerkennung
- Datum / Uhrzeit von Beginn / Ende der Verbindung

⇒ Standortdaten: nur die Funkzelle (Beginn)

Auskunftspflichten

⇒ Für zu eigenen Zwecken gespeicherte Daten:

- § 96 Abs. 1 S. 2 TKG (i.V.m. § 100g StPO)

⇒ Für aufgrund von Speicherpflichten gespeicherte Daten (§ 113c TKG):

- Übermittlung an Strafverfolgungsbehörden, wenn ein Gesetz Datenerhebung für schwere Straftaten gestattet
- Übermittlung an Gefahrenabwehrbehörden (der Länder), wenn ein Gesetz Datenerhebung zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes gestattet
- Erteilung einer Nutzerauskunft (§ 113 Abs. 1 S. 3 TKG)

⇒ Einzelheiten sind in TKÜV / TR TKÜV geregelt.

AUSKUNFTSERTEILUNG ÜBER VERKEHRSDATEN

Bildnachweis: Justitia © Freelancer0111 / Pixelio

Auskunftsberechtigte

⇒ Auskünfte über (nicht aufgrund von Speicherpflichten gespeichert) Verkehrsdaten können u.a. verlangen

- Polizeibehörden des Bundes und der Länder
  - § 20m BKAG *(zur Terrorismusbekämpfung)*
  - § 23a PolG BW
- Nachrichtendienste des Bundes und der Länder
  - §8a Abs. 2 Nr. 4 BVerfSchG
  - § 3 BNDG, § 4a MADG
  - § 5b LVSG
- Private bei Urheberrechtsverletzungen (§ 101 UrhG)

⇒ In der Folge soll es um Auskünfte für Zwecke der Strafverfolgung gehen.

Auskünfte zur Strafverfolgung

- ⇒ § 100g Abs. 1 StPO:
  Auskunft über vorhandene Verkehrsdaten
- ⇒ § 100g Abs. 2 StPO:
  Auskunft über nach § 113b TKG
  gespeicherte Verkehrsdaten
- ⇒ § 100g Abs. 3 StPO: Funkzellenabfrage
- ⇒ Das Gesetz unterscheidet nunmehr zwischen „normalen“ Verkehrs- und den Standortdaten.
- ⇒ § 100g StPO betrifft nicht die Erhebung beim Teilnehmer.
- ⇒ §§ 100g Abs. 4, 101a StPO regeln das Verfahren zur Verkehrsdatenerhebung gesondert.

Auskünfte nach § 100g StPO

⇒ Straftat von erheblicher Bedeutung (Abs. 1 Nr. 1)
- auch im Einzelfall:
  - mittl. Kriminalität, insb. Katalog des § 100a Abs. 2 StPO
  - empfindliche Störung des Rechtsfriedens
- auch Versuch oder strafbare Vorbereitungshandlung
- Erhebung von **zukünftigen** Standortdaten zulässig
- Funkzellenabfrage zulässig (ultima-ratio-Klausel)

⇒ Straftat mittels Telekommunikation begangen (Abs. 1 Nr. 2)
- ultima-ratio-Klausel
- keine Erhebung von Standortdaten
- keine Funkzellenabfrage

⇒ Sonderregelung für Daten nach § 113b TKG

Allgemeine Voraussetzungen

⇒ Zulässige Betroffene (§ 100a Abs. 3 StPO):
- Beschuldigte
- Anschlussinhaber vom Beschuldigten genutzter Anschlüsse
- Nachrichtenmittler

⇒ „bestimmte Tatsachen“

⇒ Richtervorbehalt mit Eilkompetenz der StA

⇒ Befristung auf drei Monate in die Zukunft

⇒ Schriftliche Anordnung:
- Name und Anschrift des Betroffenen
- Rufnummer / Anschlusskennung
- Art, Umfang und Dauer der Maßnahme
- einzelfallbezogene Begründung

Daten nach § 113b TKG

- ⇒ Sonderregelung in § 100g Abs. 2 StPO
- ⇒ Straftatenkatalog
  - kein Verweis auf § 100a StPO oder § 100c StPO; eigener Katalog (vergleichbar § 100c StPO)
  - Tat muss auch im Einzelfall besonders schwer wiegen
- ⇒ ultima-ratio-Klausel
- ⇒ keine Eilkompetenz der Staatsanwaltschaft
- ⇒ Erhebung retrograder Standortdaten nur noch aufgrund dieser Vorschrift
- ⇒ Provider müssen Daten nach § 113b TKG bei Übermittlung kennzeichnen
- ⇒ Umwidmung nur unter selben Voraussetzungen

Funkzellenabfrage

⇒ Sonderregelung in § 100g Abs. 3 StPO

⇒ Ziel darf nur die Ermittlung Beschuldigter (nicht: Zeugen) sein.

⇒ nur bei Straftaten von erheblicher Bedeutung

⇒ ultima-ratio-Klausel

⇒ besondere Verhältnismäßigkeitsprüfung

- konkrete Anhaltspunkte für Telekommunikation
- Abwägung von Ort, Zeit und Dauer der Maßnahme

⇒ räumlich und zeitlich hinreichend bestimmt

⇒ Vor Abfrage erfolgt regelmäßig eine Vermessung der Funkzellen.

⇒ Zugriff auf Daten nach § 113b TKG möglich

Benachrichtigungspflichten

⇒ § 100g StPO ist nunmehr als grundsätzlich offene Maßnahme unter Benachrichtigung der Betroffenen ausgestaltet.

⇒ Zurückstellung der Benachrichtigung muss gerichtlich angeordnet werden.

⇒ Zu benachrichtigen sind alle Beteiligten der jeweils betroffenen Telekommunikation.

- Identifizierungen von Beteiligten nur zur Benachrichtigung unterbleiben in der Regel.
- Benachrichtigungen können unterbleiben, wenn Beteiligte von der Maßnahme nur unerheblich betroffen sind und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung haben.

Weitere Nebenregelungen

⇒ § 100g Abs. 4 StPO (§ 160a StPO)

- Keine gezielten Verkehrsdatenerhebungen gegen Zeugnisverweigerungsberechtigte
- Verwertungsverbot für erhobene Verkehrsdaten, die Zeugnisverweigerungsberechtigte betreffen

⇒ Kennzeichnungspflichten
(§ 101a Abs. 3 StPO / § 101 Abs. 3 StPO)

⇒ Umwidmungsregelungen
(§ 101a Abs. 4-5 StPO /
§§ 161 Abs. 2,477 Abs. 2 StPO)

⇒ Löschungspflichten
(§ 101a Abs. 3 StPO / § 101 Abs. 8 StPO)

Aktueller Umsetzungsstand

Übergangsfristen

⇒ § 150 Abs. 13 TKG:
Die Speicherverpflichtung und die damit verbundenen Verpflichtungen […] sind spätestens ab dem 1. Juli 2017 zu erfüllen.

⇒ § 12 Abs. 1 EGStPO:
Nach § 96 [TKG] gespeicherte Standortdaten dürfen erhoben werden bis zum 29. Juli 2017 auf der Grundlage des § 100g Abs. 1 [StPO a.F.].

⇒ Ab dem 30.07.2017 dürfen retrograde Standortdaten dann nur nach § 100g Abs. 2 StPO erhoben werden, was mit der vierwöchigen Speicherfrist (§ 113b Abs. 1 TKG) gleichläuft.

Aussetzung der Speicherpflicht?

⇒ OVG Münster, Beschluss vom 22.06.2017 – 13 B 238/17

- Die derzeitige Regelung zur Speicherpflicht verstößt gegen europäisches Recht.
- Im Wege des Eilrechtschutzes wird festgestellt, dass die Antragstellerin derzeit nicht speichern muss.
- Die Entscheidung gilt nur für die SpaceNet AG.

⇒ BNetzA, Mitteilung vom 28.06.2017

- Aufgrund dieser Entscheidung sieht die BNetzA bis zum rechtskräftigen Abschluss des Verfahrens von Anordnungen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab. Bis dahin werden auch keine Bußgeldverfahren eingeleitet.

Fragen / Diskussion

Bildnachweis: Justitia © Freelancer0111 / Pixelio

Danke!

Danke für Ihre Aufmerksamkeit!

Thomas Hochstein
http://thomas-hochstein.de/