Das Urteil zur Vorratsdatenspeicherung aus Sicht der Speicherungspflichtigen

20. März 2010

Valerian Jenny

Bird & Bird LLP Frankfurt

BIRD & BIRD

Inhaltsüberblick

1. Prolog
2. Unmittelbare Auswirkungen der Entscheidung
3. Die Speicherpflichtigen als „Datenhüter“
4. Wer soll das bezahlen?
5. Wie sicher muss es zukünftig sein?






Prolog

- Aufbau einer einstweilen nutzlosen Speicherinfrastruktur:

  300 MEUR

- Auskunft über gespeicherte Verkehrsdaten: für jede Kennung, die der Auskunftserteilung zugrunde liegt

  30,00 EUR

- Löschung von 44 Terabyte Vorratsdaten:

  Unbezahlbar!

ABER:

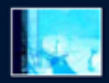
- Vorratsdatenspeicherung hat den Segen aus Karlsruhe!






Unmittelbare Auswirkungen

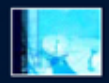
- „Die […] von Anbietern öffentlich zugänglicher Telekommunkationsdienste […] erhobenen […] Telekommunikationsverkehrsdaten sind unverzüglich zu löschen." (BVerfG Urt. v. 02.03.2010, Tenor zu 3.)
- 1&1 Internet AG hat angeblich 25 Terabyte an Daten gelöscht, Deutsche Telekom AG 19 Terabyte (1 TB = 10^{12} Byte)
- Zum Vergleich: 1 DVD-ROM (single layer) hat 4,7 GB (1 GB = 10^{9} Byte)
- Von 1&1 sowie DTAG gelöschte Datenmenge entspricht 9.361 DVD-ROM (44 / 4,7 x 1.000)



Unmittelbare Auswirkungen (2)

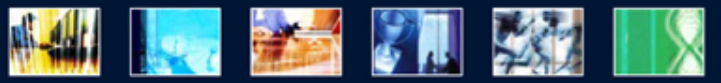
- Nach Angaben des Bitkom hat die Speicherinfrastruktur Carrier und Internet-Unternehmen EUR 300 Mio. gekostet.
- BVerfG sieht Art. 12 GG durch diese Belastung nicht als verletzt.
- Was wird aus diesem nunmehr womöglich nutzlosen Anlagevermögen?
- Wohl keine Staatshaftung für legislatives Unrecht (Ausnahme: Nichtumsetzung von EU-Richtlinien!)



Die Speicherungspflichtigen als „Datenhüter“

- „Maßgeblich ist hierfür (scil. Zulässigkeit der Vorrats-DS) zunächst, dass die vorgesehene Speicherung der Telekommunikations-verkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht wird. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen und stehen dem Staat unmittelbar als Gesamtheit nicht zur Verfügung (Rn. 214). […] Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, […] (Rn. 218).“
- Im Klartext: Die Vorrats-DS ist hinnehmbar, weil der Staat die Daten nicht selbst speichert.



Die Speicherungspflichtigen als „Datenhüter“ (2)

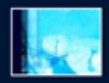
- „Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden also nicht ein Direktzugriff auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden (Rn. 250).“
- Die Speicherungspflichtigen sollen also bei der Bearbeitung von Auskunftsersuchen die Daten „filtern“ und damit den Eingriff in Art. 10 im Einzelfall auf das erforderliche Maß beschränken.

Zur Diskussion:

- Ist die Grundannahme realistisch, dass Carrier und Internetunternehmen die Strafverfolgungsbehörden oder gar Geheimdienste kontrollieren können?
- Trauen wir ihnen dies zu?
- Wollen die Unternehmen diese Verantwortung überhaupt?

Wer soll das bezahlen?

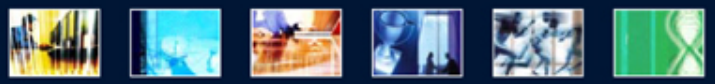
- Das Gericht lehnt einen unverhältnismäßigen Eingriff in Art. 12 durch die Kostenlast ab.
- Die speicherpflichtigen Unternehmen verursachen die Gefahr mit.
- Das Gericht erwartet, dass die Kosten über den Markt refinanziert werden können.
- Ist die Annahme realistisch, dass die Kosten einer erneuten Vorrats-DS im Wettbewerb über den Marktpreis einspielen lassen?
- Die Aussagen des Gerichts enthalten nur eine rechtliche Bewertung, keine politische. Die Speicherungspflichtigen sollten sich also nicht entmutigen lassen, bei einer etwaigen Neueinführung der Vorrats-DS eine angemessene Kostenerstattung zu erreichen.



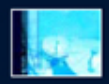
Wer soll das bezahlen (2)

- Immerhin: Auskünfte sind nicht unentgeltlich: § 23 Abs. 1 Justizvergütungs- und entschädigungsgesetz (JVEG) iVm Anlage 3 zum Gesetz
- Danach kosten zB
  - Umsetzung einer Anordnung zur Überwachung der Telekommunikation, unabhängig von der Zahl der dem Anschluss zugeordneten Kennungen: je Anschluss **100,00 EUR**
  - Auskunft über gespeicherte Verkehrsdaten: für jede Kennung, die der Auskunftserteilung zugrunde liegt **30,00 EUR**
  - Auskunft über gespeicherte Verkehrsdaten zu Verbindungen, die zu einer bestimmten Zieladresse hergestellt wurden, durch Suche in allen Datensätzen der abgehenden Verbindungen eines Betreibers (Zielwahlsuche): je Zieladresse **90,00 EUR**
  - Auskunft über gespeicherte Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle (Funkzellenabfrage) **30,00 EUR**
  - Auskunft über den letzten dem Netz bekannten Standort eines Mobiltelefons (Standortabfrage) **90,00 EUR**



Wie sicher muss es zukünftig sein?

- Aufgrund der Sensibilität von Telekommunikations-Verbindungsdaten postuliert das Gericht hohe Anforderungen an deren Sicherheit.
- Gericht schreibt zwar Maßnahmen nicht explizit vor, deutet aber doch recht konkret an, was es sich vorstellt, nämlich *getrennte Speicherung, asymmetrische Verschlüsselung, Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokollierung von Zugriff und Löschung.*
- Gericht diagnostiziert folgende Mängel (Rz. 271):
  - Verweis auf die allgemein im Bereich der Telekommunikation erforderliche Sorgfalt (§ 113a Abs. 10)
  - §§ 88 und 109 TKG erlauben angeblich Relativierungen – stimmt das?
  - Gemeint ist § 109 Abs. 2 S. 7 TKG:
    Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.

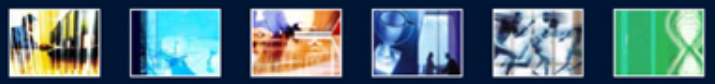





Wie sicher muss es zukünftig sein? (2)

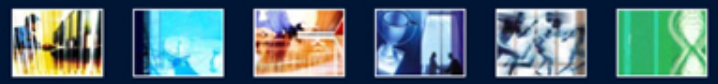
Einwände:

- Relation zu geschützten Rechten wird ausdrücklich in Bezug genommen. Dies erlaubt es, die Sensibilität der Vorratsdaten zu berücksichtigen.
- § 109 Abs. 3 TKG: Pflicht zur Bestellung eines Sicherheitsbeauftragten und Erstellung von Sicherheitskonzepten, die der Kontrolle durch die BNetzA unterliegen.
- Strafbewehrung des Fernmeldegeheimnisses in § 206 StGB wird anscheinend übersehen. (Rz. 275)
- Was helfen eigentlich die Maßnahmen, die dem Gericht vorschweben, wenn die Konzernsicherheitsabteilung Vorratsdaten verlangt?
- Widerspruch zur „Datenhüter“-Funktion der Speicherpflichtigen



Wie sicher muss es zukünftig sein? (3)

- Sind die Anforderungen auf sonstige Verkehrsdaten zu erweitern?
  - Inhaltlich unterscheiden Abrechnungsdaten aus einem Einzelverbindungsnachweis sich nicht maßgeblich von den Vorratsdaten.
  - Das Gericht meint offenbar, insoweit die Anforderungen für Vorratsdaten nicht einfordern zu wollen:
    „Ein Großteil der Daten wird ohnehin für eigene Zwecke gespeichert.“ (Rz. 300 sinngemäß)
  - Abrechnungsdaten werden für andere Zwecke gespeichert und nur, soweit dafür erforderlich (also nicht bei Flatrate).
  - Altes Recht gab Kunden Wahlfreiheit (§ 97 Abs. 4 TKG a.F.). Dies sollte wieder eingeführt werden.



Vielen Dank.

Valerian Jenny
Senior European Consultant,
Telekommunikation
Bird & Bird LLP
+49-69-74222-6235
valerian.jenny@twobirds.com