Ausarbeitung

Rechtlicher Rahmen für eine Regelung der Vorratsdatenspeicherung durch den deutschen Gesetzgeber

[redacted]

Rechtlicher Rahmen für eine Regelung der Vorratsdatenspeicherung durch den deutschen Gesetzgeber

Verfasser/in: [redacted]
Aktenzeichen: WD 3 - 3000 - 071/15
Abschluss der Arbeit: 27. März 2015
Fachbereich: WD 3: Verfassung und Verwaltung
Telefon: [redacted]

1. Fragestellung

In Deutschland wurde die Richtlinie über die Vorratsdatenspeicherung[1] mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 21. Dezember 2007 umgesetzt. Die Änderungen betrafen im Wesentlichen die Strafprozessordnung und das Telekommunikationsgesetz. Das Bundesverfassungsgericht hat die deutsche Umsetzung der Richtlinie mit Urteil vom 2. März 2010 für verfassungswidrig erklärt.[2] Anlässlich von zwei miteinander verbundenen Vorabentscheidungsersuchen, die vom High Court aus Irland und dem Verfassungsgerichtshof aus Österreich vorgelegt wurden, hat der Europäische Gerichtshof mit Urteil vom 8. April 2014 die zugrunde liegende Richtlinie über die Vorratsdatenspeicherung für ungültig erklärt.[3]

Vor diesem Hintergrund wird gefragt, welcher rechtliche Rahmen nunmehr für eine Regelung der Vorratsdatenspeicherung durch den deutschen Gesetzgeber besteht.

2. Rechtsprechung des Bundesverfassungsgerichts

In seinem Urteil zur Umsetzung der Vorratsdatenspeicherungsrichtlinie hat das Bundesverfassungsgericht eine Vorratsdatenspeicherung zwar nicht als von vornherein unvereinbar mit Art. 10 Abs. 1 Grundgesetz (GG) angesehen, jedoch die konkrete Ausgestaltung für unverhältnismäßig und damit verfassungswidrig erklärt. In seiner Entscheidung erläutert das Gericht, unter welchen Maßgaben eine solche Speicherung mit Art. 10 Abs. 1 GG vereinbar sein kann[4]:

Maßgeblich dafür sei zunächst, dass die vorgesehene Speicherung nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht werde.[5] Damit werde gewährleistet, dass die Daten dem Staat nicht unmittelbar als Gesamtheit zur Verfügung stehen.

---

1 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

2 BVerfGE 125, 260.

3 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 ff.

4 Siehe auch die Pressemitteilung Nr. 11/2010 des Bundesverfassungsgerichts vom 2. März 2010, abrufbar unter http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-011.html (letzter Abruf am 24. März 2015), dort zum Folgenden.

5 BVerfGE 125, 260 (321).

Weiter sei Voraussetzung, dass die anlasslose Speicherung der Telekommunikationsverkehrsdaten eine Ausnahme bleibe und nur in einem engen zeitlichen Rahmen erlaubt werde.[6] Eine Speicherungsdauer von sechs Monaten liege an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig sei.[7]

Im Einzelnen fordert das Gericht hinreichend anspruchsvolle und normenklare Regelungen zur Datensicherheit (hierzu 2.1.), zur Begrenzung der Datenverwendung (hierzu 2.2.), zur Transparenz (hierzu 2.3.) sowie zum Rechtsschutz (hierzu 2.4.). Schließlich enthält die Entscheidung des Bundesverfassungsgerichts auch Ausführungen zu den Anforderungen an die mittelbare Nutzung der Daten zur Identifizierung von IP-Adressen (hierzu 2.5.).

2.1. Anforderungen an die Datensicherheit

Das Gericht betont die Bedeutung von Datensicherheit für die Verhältnismäßigkeit entsprechender Regelungen zur Vorratsdatenspeicherung und fordert gesetzliche Regelungen, die ein besonders hohes Maß an Sicherheit jedenfalls dem Grunde nach normenklar und verbindlich vorgeben.[8] Dabei könne der Gesetzgeber die Aufgabe der technischen Konkretisierung des vorgegebenen Maßstabs auch einer Aufsichtsbehörde übertragen. Er habe jedoch sicherzustellen, dass die jeweiligen Telekommunikationsanbieter nicht unkontrolliert die Entscheidungen über Art und Maß der Schutzvorkehrungen treffen.

2.2. Anforderungen an die unmittelbare Datenverwendung

Weiter komme eine Verwendung der Daten nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht.[9] Für die Strafverfolgung bedeute dies, dass ein Abruf zumindest den durch bestimmte Tatsachen begründeten Verdacht einer auch im Einzelfall schwerwiegenden Straftat voraussetze. Für die Gefahrenabwehr gelte, dass ein Abruf der vorsorglich gespeicherten Daten nur bei Vorliegen einer durch bestimmte Tatsachen hinreichend belegten, konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden dürfe. Diese Anforderungen seien auch auf die Nachrichtendienste zu übertragen, da es auch insoweit um eine Form der Gefahrprävention gehe.

Der Verhältnismäßigkeitsgrundsatz fordere zudem, dass für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot geschaffen werde. Dies gelte beispielsweise für telefonische Beratung in seelischen oder sozialen Notlagen.

---

6 BVerfGE 125, 260 (323 f.).

7 BVerfGE 125, 260 (322).

8 BVerfGE 125, 260 (325 ff.).

9 BVerfGE 125, 260 (327 ff.).

2.3. Anforderungen an die Transparenz der Datenübermittlung

Der Gesetzgeber müsse durch wirksame Transparenzregeln der bedrohlichen Wirkung, die Datenspeicherung und -verwendung auf den Bürger haben könne, entgegenwirken.[10] Dazu gehöre auch der Grundsatz der Offenheit der Erhebung und Nutzung personenbezogener Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen sei nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf diene, vereitelt würde. Der Gesetzgeber könne dies für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste grundsätzlich annehmen. Im Rahmen der Strafverfolgung komme auch eine offene Erhebung und Nutzung der Daten in Betracht. In diesem Bereich dürfe eine heimliche Verwendung der Daten nur erfolgen, wenn sie im Einzelfall erforderlich und richterlich angeordnet sei. Erfolge die Datenverwendung heimlich, sei eine nachträgliche Benachrichtigung vorzusehen. Ausnahmen bedürften der richterlichen Kontrolle.

2.4. Anforderungen an den Rechtsschutz und an Sanktionen

Weiter führt das Bundesverfassungsgericht aus, dass eine Übermittlung und Nutzung der gespeicherten Daten grundsätzlich unter Richtervorbehalt zu stellen sei.[11] Sofern ein vorheriger Rechtsschutz nicht möglich sei, solle eine nachträgliche gerichtliche Kontrolle eröffnet werden.

Insbesondere vor dem Hintergrund der Verpflichtung des Staates, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen, sei zudem die Schaffung wirksamer Sanktionen für den Fall von Rechtsverletzungen erforderlich.[12] Der Gesetzgeber besitze diesbezüglich jedoch einen weiten Gestaltungsspielraum.

2.5. Anforderungen an die mittelbare Nutzung der Daten zur Identifizierung von IP-Adressen

Weniger strenge verfassungsrechtliche Anforderungen gelten laut Bundesverfassungsgericht für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter, bereits bekannter IP-Adressen.[13] Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen seien auf der Grundlage solcher Auskünfte nicht möglich.

Der Gesetzgeber dürfe innerhalb des ihm zustehenden Gestaltungsspielraums solche Auskünfte auch unabhängig von begrenzenden Straftaten oder Rechtsgüterkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen. Der Gesetzge-

---

10 BVerfGE 125, 260 (334 ff.).

11 BVerfGE 125, 260 (337 ff.).

12 BVerfGE 125, 260 (339 f.).

13 BVerfGE 125, 260 (340 ff.).

ber müsse jedoch sicherstellen, dass Auskünfte nur aufgrund eines hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen. Der Betroffene müsse zudem vor der Einholung der Auskunft benachrichtigt werden, ein Richtervorbehalt sei jedoch nicht erforderlich. Schließlich sei die Einholung einer solchen Auskunft nur bei solchen Rechtsgutsbeeinträchtigungen gerechtfertigt, denen von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen werde.

3. Rechtsprechung des Europäischen Gerichtshofs

In seinem Urteil vom 8. April 2014 hat der Europäische Gerichtshof die Vorratsdatenspeicherungsrichtlinie mit allgemeiner Wirkung für von Anfang an ungültig erklärt. Damit ist die in der Richtlinie enthaltene Umsetzungspflicht entfallen und das Vertragsverletzungsverfahren gegen Deutschland hat seine Grundlage verloren.

Nach Art. 51 Abs. 1 Grundrechtecharta (GrCh) gilt die Grundrechtecharta für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union. Vor diesem Hintergrund könnte argumentiert werden, dass mit dem Wegfall der Richtlinie über die Vorratsdatenspeicherung insoweit auch die Grundrechtecharta in der Auslegung des Europäischen Gerichtshofs nicht für die Mitgliedstaaten bindend sei. Dem wird jedoch entgegengehalten, dass Deutschland weiterhin an die Datenschutzrichtlinie (Richtlinie 95/46/EG) sowie die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) gebunden sei.[14] Nach dem Wegfall der Vorratsdatenspeicherungsrichtlinie müssten sich nationale Regelungen zur Vorratsdatenspeicherung an den durch Art. 15 Richtlinie 2002/58/EG gezogenen Rahmen halten.[15] Insoweit sei auch der nationale Gesetzgeber an die Grundrechtecharta in der Auslegung des Europäischen Gerichtshofs gebunden.[16] Vor diesem Hintergrund ist hier auch die vom Europäischen Gerichtshof im Zusammenhang mit der Vorratsdatenspeicherungsrichtlinie getätigte Auslegung der Grundrechtecharta zu erörtern.

Der Europäische Gerichtshof prüft die Vorratsdatenspeicherungsrichtlinie am Maßstab von Art. 7 GrCh (Achtung des Privat- und Familienlebens) und Art. 8 GrCh (Schutz personenbezogener Daten) und stellt dabei fest, dass der Unionsgesetzgeber beim Erlass der Richtlinie die sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Grenzen überschritten habe. Aufgrund der Bedeutung der betroffenen Grundrechte sowie der Schwere des Eingriffs fordert der Europäische Gerichtshof klare und präzise Regeln für die Tragweite und Anwendung der fraglichen Maßnahme sowie die Aufstellung von Mindestanforderungen, die einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder

14 Roßnagel, Neue Maßstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung, MMR 2014, S. 372 (376).

15 Priebe, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, EuZW 2014, S. 456 (458); Kunnert, EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen?, DUD 2014, S. 774 (782 f.).

16 Roßnagel, Neue Maßstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung, MMR 2014, S. 372 (376); so im Ergebnis auch Kühling, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, S. 681 (684).

unberechtigten Nutzung ermöglichen.[17] Der Schutz des Grundrechts auf Achtung des Privatlebens verlange, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken.[18] Dies sei bei der Vorratsdatenspeicherungsrichtlinie nicht gewährleistet.

3.1. Differenzierungen, Einschränkungen oder Ausnahmen

Zunächst moniert das Gericht, dass sich die Vorratsdatenspeicherungsrichtlinie auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstrecke, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.[19] Die Richtlinie gelte auch für Personen, bei denen keine Anhaltspunkte dafür bestehen, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Da die Richtlinie keine Ausnahmen vorsehe, erfasse sie auch Personen, für deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften ein Berufsgeheimnis gelte. Die Richtlinie verlange keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen sei, und einer Bedrohung der öffentlichen Sicherheit.

3.2. Objektive Kriterien für den Zugang und die spätere Nutzung der Daten

Weiter kritisiert das Gericht, dass die Vorratsdatenspeicherungsrichtlinie kein objektives Kriterium für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung enthalte.[20] So fehlten materiell- und verfahrensrechtliche Voraussetzungen für den Zugang sowie eine Beschränkung auf Zwecke der Verhütung, Feststellung oder Bekämpfung genau abgegrenzter schwerer Straftaten. Insbesondere sehe die Richtlinie keine vorherigen Kontrollen durch ein Gericht oder eine unabhängige Verwaltungsstelle vor.

3.3. Objektive Kriterien bezüglich der Speicherdauer

In Bezug auf die Speicherdauer moniert der Europäische Gerichtshof, dass die Richtlinie eine Speicherung von mindestens sechs Monaten vorsehe, dabei jedoch nicht zwischen den verschiedenen Datenkategorien differenziere.[21] Zudem könne die Speicherfrist zwischen sechs und 24 Monaten betragen, ohne dass diese auf objektiven Kriterien beruhen müsse, die eine Beschränkung auf das absolut Notwendige gewährleisten.

---

17 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (414 - Rn. 54).

18 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (414 - Rn. 52).

19 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (414 - Rn. 57 ff.).

20 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (414 f. - Rn. 60 ff.).

21 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (415 - Rn. 63 f.).

3.4. Regelungen zur Datensicherheit/Speicherung der Daten auf Unionsgebiet

Weiter führt das Gericht aus, dass die Vorratsdatenspeicherungsrichtlinie keine hinreichenden Garantien dafür biete, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind.[22] Das Gericht stellt dabei vor allem auf zwei Aspekte ab:

Zum einen enthalte die Richtlinie keine speziellen Regelungen, die der großen Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Die Richtlinie gewährleiste auch nicht, dass die Telekommunikationsanbieter durch technische oder organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestatte es ihnen, bei der Bestimmung des Sicherheitsniveaus wirtschaftliche Erwägungen zu berücksichtigen. Vor allem gewährleiste die Richtlinie nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

Zum anderen moniert der Europäische Gerichtshof, dass die Richtlinie nicht die Speicherung der Daten auf Unionsgebiet vorsehe. So sei nicht vollumfänglich gewährleistet, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit durch eine unabhängige Stelle überwacht wird.

[redacted]

22 EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12, MMR 2014, S. 412 (415 - Rn. 66 ff.).