Öffentliches Recht

Frenz

8., neu bearbeitete Auflage 2019
ISBN 978-3-8006-6022-3
Vahlen

gg) Vorratsdatenspeicherung. Einen vergleichbaren Ansatz wählte das BVerfG für die Vorratsdatenspeicherung. Bei dieser müssen die Betreiber öffentlich zugänglicher Telekommunikationsdienste für Endnutzer bestimmte einzeln aufgeführte Verkehrs-, darunter auch Speicherdaten für einen strikt begrenzten Zeitraum speichern und dann unverzüglich löschen (§ 113b TKG[771]). Das erinnert an die Videoüberwachung, nur dass hier keine Inhalte gespeichert werden. Zudem erfolgt die Auswertung der **gespeicherten Daten** nicht selbst. Vielmehr werden diese nach § 113c TKG an die zuständigen Stellen **auf Verlangen übermittelt.** Das liegt parallel zur Rasterfahndung, sodass die dazu entwickelten Maßstäbe Platz greifen. **446**

Erforderlich ist daher ebenfalls eine **konkrete Gefahr von besonderem Gewicht.** Es reicht also nicht die bloße Möglichkeit eines bevorstehenden Geschehensverlaufs, sondern eine dringende Gefahr wird verlangt. Inhaltlich genügt nicht jede Gefahr für die öffentliche Sicherheit, sondern nur eine erhebliche, zu bestimmen nach dem Gewicht der zu schützenden Rechtsgüter. Vielmehr muss es sich um eine **dringende 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** handeln. Dafür muss die Ermächtigungsgrundlage zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter verlangen.[772] **447**

Entsprechendes gilt bei einer **Datenübermittlung** für Aufgaben des **Verfassungsschutzes,** des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes. Wegen der Weite der damit verbundenen Aufgaben müssen die Anlässe bestimmt genug gefasst sein. Auch insoweit müssen landesrechtliche Befugnisnormen den Bestimmtheitsgrundsatz wie bei der Videoüberwachung (→ Rn. 481f.) hinreichend wahren; Vorbildfunktion hat das Artikel 10-Gesetz (G10).[773] **448**

Bei der **Strafverfolgung** ergeben sich die notwendigen gravierenden Anlässe einer Datenübermittlung aus dem **Katalog der Straftaten** nach § 100a II StPO und den Voraussetzungen des § 100a I StPO.[774] Soweit sich daraus Weiterungen gegenüber der Gefahrenabwehr ergeben, liegt das an deren präventivem Charakter mit den daraus folgenden größeren Unsicherheiten. Diese erhöhen die Wahrscheinlichkeit, dass ohne hinreichenden Anlass auf das Kommunikationsverhalten der Betroffenen zugegriffen wird.[775] Bereits daraus kann eine **Änderung des Kommunikationsverhaltens** folgen (→ Rn. 302, 466). **449**

Der **EuGH hat parallel** zu diesen Maßstäben entschieden und aufgrund der Weite und Schwere der Beeinträchtigung des elementaren Grundrechts auf Achtung des Privatlebens (Art. 7 GRCh) **Beeinträchtigungen »auf das absolut Notwendige« beschränkt.** Erforderlich ist ein hinreichender Bezug der Vorratsdatenspeicherung auf bestimmte Straftaten, die Beschränkung des behördlichen Zugangs darauf und eine klare zeitliche Limitierung; dies alles muss von einer unabhängigen Stelle überwacht werden.[776] Diese Grundsätze wurden in § 23 II Nr. 2 lit. b PolG NRW mit der Mög-

771 Telekommunikationsgesetz.
772 BVerfGE 125, 260 (330) = NJW 2010, 833 – Vorratsdatenspeicherung II.
773 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses; BVerfGE 122, 120 (145f., 148) = BeckRS 2008, 40230 – Vorratsdatenspeicherung I.
774 Weitergehend Sondervotum *Schluckebier* NJW 2010, 833 (854).
775 BVerfGE 122, 120 (140f.) = BeckRS 2008, 40230 – Vorratsdatenspeicherung I.
776 EuGH ECLI:EU:C:2014:238 Rn. 52ff. = BeckRS 2014, 80686 – Digital Rights Ireland.

lichkeit der Datenverarbeitung bei innerhalb eines absehbaren Zeitraums drohender Gefahr schwerer Straftaten oder für vergleichbar bedeutsame Rechtsgüter umgesetzt (→ Rn. 867).

450 **Fall** nach EuGH v. 21. 12. 2016 – C-203/15 und C-698/15 = NJW 2017, 717 – Tele2 Sverige und Anm. *Frenz* DVBl. 2017, 183: Nationale Regelungen Großbritanniens und Schwedens ermöglichen eine umfassende und anlasslose Vorratsspeicherung von Verbindungsdaten, ohne dass nähere Grenzen und sichernde Verfahrensvorkehrungen vorgesehen sind. Nationale Gerichte fragen nach der Vereinbarkeit mit EU-Grundrechten.

I. Anwendbarkeit der EU-Grundrechte

Trotz der nationalen Regelungen als Ausgangspunkt der Vorlagefragen nationaler Gerichte nach Art. 267 AEUV sind EU-Grundrechte gem. Art. 51 I GRCh anwendbar. Zur Durchführung von Unionsrecht gehört auch die nationale **Umsetzung von Richtlinien.** Die RL 2002/58 zielt nach ihrem Art. 1 I unter anderem auf die Harmonisierung der Vorschriften der Mitgliedstaaten ab, um die Grundrechte und Grundfreiheiten und dabei insbesondere das Recht auf Privatsphäre und Vertraulichkeit im Hinblick auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation gleichwertig zu schützen (NJW 2017, 717 Rn. 68). Damit ist der Ansatz a priori umfassend.

Ausgenommen werden zwar Tätigkeiten des Staates vor allem im strafrechtlichen Bereich sowie zur öffentlichen Sicherheit (Rn. 69). Indes zeigt die näheren Voraussetzungen unterliegende Möglichkeit der Mitgliedstaaten nach Art. 15 I RL 2002/58, die Rechte und Pflichten der Richtlinie einzuschränken, dass grundsätzlich alle Tätigkeiten umfasst sind. Insbesondere können nicht ganze Bereiche herausgenommen werden, weil ansonsten der effet utile verloren ginge (Rn. 73). Die Herausnahme von »Tätigkeiten des Staates« im strafrechtlichen Bereich sowie zur öffentlichen Sicherheit, der Landesverteidigung und zur Sicherheit des Staates einschließlich seines wirtschaftlichen Wohls nach Art. 1 III RL 2002/58 erstreckt sich nach dem Gesamtsystem der Richtlinie vor allem nicht auf die den Betreibern elektronischer Kommunikationsdienste vorgeschriebene Vorratsspeicherung der Verkehrs- und Standortdaten und den Zugang nationaler Behörden zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten (Rn. 74 f.).

Danach zählt nicht der betroffene Bereich, sondern der Bezug zu Daten und deren Speicherung bzw. Verarbeitung. Zudem handelt es sich bei der **Vorratsdatenspeicherung und deren Anordnung** nicht originär um eine staatliche Tätigkeit, sondern diese knüpft nur an die Tätigkeit Privater an. Auf diese Weise wird allerdings die auf den Daten Privater basierte Verteidigung der staatlichen Sicherheit sowie die Verfolgung schwerer Straftaten durch Unionsrecht erfasst und nicht entsprechend dem Wortlaut »auf keinen Fall« in Art. 1 III RL 2002/58 ausgenommen, der nach seiner Formulierung die nicht den EU-Verträgen unterfallenden Bereiche wie die **Strafrechtsverfolgung** und die Sicherheit nicht dem EU-Datenschutz unterwerfen wollte. Insoweit können auch die EU-Grundrechte einwirken.

II. Vorratsdatenspeicherung als sorgfältig zu begründende Ausnahme

Die RL 2002/58 stellt den **Grundsatz der Vertraulichkeit von Kommunikationen** auf und untersagt es grundsätzlich jeder anderen Person als dem Nutzer, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern (Rn. 85). Dieser Grundsatz ist mithin die Regel, Speicherungen müssen die (begründungspflichtige) Ausnahme bleiben. Schon deshalb konnten die untersuchten nationalen Regelungen nicht durchgreifen, da sie gerade umgekehrt die Vorratsdatenspeicherung der Verkehrs- und Standortdaten zur Regel machten (Rn. 104).

Dementsprechend ist die **Ausnahmebestimmung** des Art. 15 I RL 2002/58, der den Mitgliedstaaten Beschränkungen für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Prävention und Verfolgung von Straftaten ermöglicht, **eng** auszulegen (Rn. 89). Generell sollen nach dem 30. Erwägungsgrund die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden (Rn. 87). Zudem sind die **Grundrechte bei der Auslegung** einzubeziehen, wie dies schon

im Urteil Schrems[777] erfolgte; parallel zu diesem Urteil wird die Überwachung der aufgestellten Datenschutzgrundsätze durch eine unabhängige Stelle entsprechend Art. 8 III GRCh gefordert (Rn. 123). Diese Einbeziehung gilt hier nicht nur für Art. 7 GRCh (Achtung des Privatlebens) und Art. 8 GRCh (Datenschutz), sondern auch für Art. 11 GRCh und das darin verbriefte Recht auf freie Meinungsäußerung, welches eine besondere Bedeutung in jeder demokratischen Gesellschaft hat und bei einer Speicherung aller Verbindungsdaten durch Einschüchterung[778] eingeschränkt zu werden droht. Umso mehr ist der Verhältnismäßigkeitsgrundsatz einzuhalten und ein strikt angemessenes Verhältnis zum intendierten Zweck zu verlangen (Rn. 92–95).

III. Notwendig konkrete Gefahr

Daher kann nach dem EuGH nicht schon die Wirksamkeit der Bekämpfung schwerer Kriminalität und des Terrorismus einen tiefgreifenden Eingriff, wie er durch die Vorratsdatenspeicherung erfolgt, rechtfertigen, sondern es bedarf einer weiteren Einschränkung. Die Umstände und die Voraussetzungen einer Maßnahme der Vorratsdatenspeicherung müssen konkret festgelegt werden (Rn. 102 f., 109 ff.). Es muss auf **objektiver Basis** eine **schwerwiegende Gefahr für die öffentliche Sicherheit** vorliegen bzw. **schwere Kriminalität bekämpft** werden (Rn. 111).

Dabei lässt der EuGH zunächst Öffnungen für eine wirksame **präventive Terrorbekämpfung.** Aufgrund objektiver Anknüpfungspunkte können Personenkreise erfasst werden, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen; dies kann aufgrund geographischer Daten erfolgen, wenn aufgrund objektiver Anhaltspunkte in einem oder mehreren geographischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden (Rn. 111). Die Konsequenz sind Datenspeicherungen etwa für Araber bzw. Nordafrikaner, auch wenn dies auch nach Unionsrecht nicht diskriminierend unter einem Deckbegriff »Nafri«[779] erfolgen darf.

Allerdings erfolgt sogleich eine Einschränkung im Hinblick auf die **Bekämpfung von Straftaten,** um die es gerade bei der Verhinderung von Anschlägen geht. Zwar obliegt den Mitgliedstaaten die Festlegung von Voraussetzungen, unter denen die Betreiber elektronischer Kommunikationsdienste den nationalen Behörden Zugang zu von ihnen gespeicherten Vorratsdaten gewähren müssen (Rn. 118). Indes darf dies nicht lediglich zum Zweck der Bekämpfung schwerer Straftaten erfolgen, sondern unter Hinzufügung näherer materiell- und verfahrensrechtlicher Voraussetzungen.[780] Es dürfen **nur Daten von Personen** erfasst werden, die der Planung oder Begehung oder zumindest der Verwicklung in eine schwere Straftat **verdächtig** sind (Rn. 119).[781]

Immerhin können namentlich bei einer Bedrohung vitaler Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten Daten anderer Personen einbezogen werden. Es muss dann aber **objektive Anhaltspunkte** dafür geben, dass diese Daten **in einem konkreten Fall** effektiv zur Bekämpfung solcher Aktivitäten beitragen können (Rn. 119). Es bedarf mithin konkreter Umstände, dass die betroffenen Daten einen wirksamen Aufklärungsbeitrag zu leisten vermögen. Dies muss nämlich auf einen konkreten Fall bezogen sein. Damit korrespondieren konkrete Anhaltspunkte dafür, dass terroristische Aktivitäten nicht allgemein, sondern spezifisch im Raum stehen. Zu diesen müssen die fraglichen Daten in einem konkreten Fall in Bezug gesetzt werden können. Eine bloß abstrakte Gefahr genügt mithin nicht. So entschied auch das BVerfG:[782] Nur zur Bekämpfung schwerer Straftaten und bei objektiven Anhaltspunkten für terroristische Aktivitäten im konkreten Fall dürfen also die Telefonverbindungsdaten von dem Telekommunikationsunternehmen herausverlangt und gespeichert werden. Damit wird das Urteil des EuGH

777 EuGH ECLI:EU:C:2015:650 insbesondere Rn. 104 = BeckRS 2015, 81250 – Schrems.
778 Vgl. BVerfGE 100, 313 (359) = NJW 2000, 55 – Telekommunikationsüberwachung.
779 S. zur Diskussion im Kontext des Polizeieinsatzes bei der Kölner Silvesternacht 2016/17 F. A. Z. Nr. 2 v. 3.1.2017, 1: »Codewort Nafri«.
780 Vgl. zur RL 2006/24 EuGH ECLI:EU:C:2014:238 Rn. 61 = BeckRS 2014, 80686 – Digital Rights Ireland.
781 Unter Zitierung von EGMR CE:ECHR:2015:1204JUD004714306 Rn. 260 – Zakharov/Russland.
782 BVerfGE 125, 260 (330) = NJW 2010, 833 – Vorratsdatenspeicherung II.

zur Datenschutzrichtlinie (→ Rn. 449)[783], auf welches vielfach Bezug genommen wird, fortgeführt und in seinem Anwendungsbereich erheblich erweitert, bleibt allerdings im Ansatz gleich: Eingriffe in den Datenschutz sind auf das absolut Notwendige zu beschränken (Rn. 96).

IV. Veränderte Notwendigkeit?

Angesichts des Terroranschlags auf den Berliner Weihnachtsmarkt an der Kaiser-Wilhelm-Gedächtnis-Kirche auf dem Breitscheidplatz am 19. 12. 2016 stellt sich allerdings wieder verschärft die Frage: Was ist das absolut Notwendige? Ermittler machen deutlich, dass nur durch ein allumfassendes Speichern von telefonischen Verbindungsdaten bei Terroranschlägen rasch **Täterprofile** erstellt und damit auch **potenzielle Täter ermittelt** werden können. Genau dies sieht der EuGH als zu weit gehenden Eingriff in den Schutz der persönlichen Sphäre. Zugleich zeigt er die Möglichkeiten auf der Basis dieser Daten auf: direkt die Ermittlung der Kommunikationspartner, -dauer und -häufigkeit sowie der Gesprächsorte (Rn. 98), indirekt in der Zusammenschau aller Daten das Erkennen der Lebensgewohnheiten, Aufenthaltsorte, Ortsveränderungen, ausgeübten Tätigkeiten, sozialen Beziehungen und des sozialen Umfeldes, mithin letztlich die Erstellung eines Profils (Rn. 99). So sehr durch solch sensible persönliche Daten in das Grundrecht auf Achtung des Privatlebens eingegriffen wird, ermöglichen sie umgekehrt erst eine effektive Prävention durch das Herausfiltern möglicher Gefährder, obwohl noch keine konkreten Umstände auf einen wirksamen Beitrag zur Bekämpfung terroristischer Aktivitäten vorliegen, wenn die Daten dieser Personen den Behörden zugänglich gemacht, näher betrachtet und ausgewertet werden.

V. Erweiterte konkrete Gefahr

Ein anderer Ansatzpunkt für eine wirksamere Terrorbekämpfung ist eine erweiterte Sicht der vom EuGH geforderten **objektiven Anhaltspunkte in einem konkreten Fall.** Besteht mittlerweile nicht bereits eine latente konkrete Gefahr für das Leben des Bürgers? Nur ist diese **laufende Gefahr** nicht konkret erkennbar. Sie kann sich aber jederzeit aktualisieren. Zudem stellt sich die Frage, ob angesichts der gravierenden Auswirkungen drohender Terroranschläge nicht die **Anforderungen** an das Bestehen einer konkreten Gefahr **herabgesetzt** werden müssen. Genügen dann nicht bereits etwa Anschläge in anderen Staaten oder festgestellte Bewegungen von Gefährdern oder einfach die objektiv unterlegte Gewissheit, dass viele verdeckte Schläfer sich in Deutschland aufhalten, die jederzeit aktiv werden können, um hinreichende Anhaltspunkte für einen konkreten Fall wirksamer Terrorbekämpfung (EuGH) bzw. für eine konkrete Gefahr für Leben und Gesundheit (BVerfG) zu bejahen?

VI. Menschenwürde potenzieller Opfer

Würde der Staat sogar seine Schutzpflichten für Leben und Gesundheit vernachlässigen, wenn er Möglichkeiten der Ermittlung von Terroristen außer Acht lassen würde? Drohte dann nicht der Einzelne zum Spielball von Terroristen zu werden und damit gleichsam zum **Objekt des Terrors** (→ Rn. 265)? Darin kann ein Ansatzpunkt eines **Angriffs auf die Menschenwürde** gesehen werden, die entsprechend der sog. Dürig'schen Objektformel gewährleistet, dass der Einzelne Subjekt bleibt und nicht zum Objekt jedenfalls staatlichen Handelns wird. Wenn der Staat aber duldet, dass der Einzelne zum Objekt des Terrors wird, ist dies einer Behandlung als Objekt gleichzusetzen.[784] Den Ansatz, dass der Einzelne nicht zum Objekt herabgewürdigt werden darf, hat der EuGH in der Frage der möglichen Patentierung von embryonalen Stammzellen gewählt und wegen der Unverfügbarkeit des Menschen einschließlich seiner Teile eine Patentierbarkeit verneint.[785] Im Bereich des Datenschutzes könnte dann eine Abwägung **Würde gegen Würde** erfolgen, wenn auch auf EU-Ebene[786] der Datenschutz an die Menschenwürde angedockt wäre.[787]

783 EuGH ECLI:EU:C:2014:238 = BeckRS 2014, 80686 – Digital Rights Ireland.
784 Näher *Frenz* DÖV 2015, 305.
785 EuGH ECLI:EU:C:2014:2451 Rn. 36 = BeckRS 2014, 82542 – Stemcell; bereits EuGH ECLI:EU:C:2001:523 Rn. 73, 77 = BeckRS 2004, 76869 – Niederlande/Parlament und Rat; EuGH ECLI:EU:C:2011:669 Rn. 49ff. = BeckRS 2011, 81505 – Brüstle.
786 Für das GG etwa BVerfG NJW 2013, 1499 – Antiterrordatei: Art. 2 I iVm Art. 1 I GG.
787 Näher Pechstein/Nowak/Häde/*Frenz*, Frankfurter Kommentar, 2017, GRC Art. 1 Rn. 9ff.

VII. Terrorismus als Hochrisikophänomen mit fortlaufender Beobachtungspflicht
Ein anderer möglicher Ansatzpunkt, um eine Vorratsdatenspeicherung trotz einer Antastung der Persönlichkeitsrechte und des Datenschutzes zu erlauben, ergibt sich aus dem Bundesverfassungsgerichtsurteil zum Atomgesetz v. 6.12.2016. Das Gericht verpflichtete den Gesetzgeber angesichts einer Hochrisikotechnologie zur fortlaufenden Beobachtung und Reaktionspflicht. Daraus entnahm es auch die **Rechtfertigung** für tiefgreifende Inhalts- und Schrankenbestimmungen allein aus neuen Einschätzungen der Gefährdungslage heraus, hier anlässlich des Reaktorunfalls von Fukushima vom Frühjahr 2011.[788] Es mussten keine konkreten neuen Anhaltspunkte vorliegen, damit der Staat trotz Antastung des Eigentumsgrundrechts berechtigt war, die Laufzeit von Kernkraftwerken zu verkürzen – wenn auch bei hinreichendem Vertrauensschutz gegen Entschädigung.
Terroranschläge sind Hochrisikophänomene. Damit hat der Staat erst recht eine **fortlaufende Beobachtungs- und Reaktionspflicht.** Sobald er die Sachlage gravierend anders einschätzt, muss er berechtigt sein, zur Gewährleistung des Schutzes von Leben und Gesundheit seiner Bürger Maßnahmen zu ergreifen, auch wenn diese erhebliche Grundrechtseingriffe mit sich bringen. Dazu gehört dann auch die Vorratsdatenspeicherung.

VIII. Ergebnis
Die Ermöglichung einer umfassenden und anlasslosen Vorratsdatenspeicherung in einer nationalen Regelung verstößt gegen die RL 2002/58 sowie Art. 7, 8 und 11 GRCh. Eine Vorratsdatenspeicherung kann nach dem EuGH nur bezogen auf bestimmte Personen aufgrund objektiver Anhaltspunkte für terroristische Aktivitäten in einem konkreten Fall gerechtfertigt sein. Weiterungen kommen nach Art. 1 GRCh, einer erweiterten Sicht der konkreten Gefahr und einer fortlaufenden staatlichen Reaktionspflicht auf ein Hochrisikophänomen in Betracht.

hh) Sicherheitsbedenken. Im Ergebnis ist damit freilich keine umfassende Prävention möglich, um terroristische Angriffe durch das Ermitteln potenzieller Täter und Unterstützer im Vorfeld zu verhindern, sofern ihr Auftreten nicht durch – zumal konkrete – Tatsachen belegt werden kann.[789] **Rasterfahndung und Vorratsdatenspeicherung können im Einzelfall nur sehr begrenzt angeordnet werden.** Das gilt auch für Zweckänderungen und Weitergaben bereits erhobener Daten an andere Behörden im In- und Ausland (→ Rn. 456). Dabei können terroristische Angriffe vielen Menschen das Leben kosten. Dieser Aspekt muss der Schwere des Eingriffs in die informationelle Selbstbestimmung gegenübergestellt werden, was nicht erfolgte, nicht zuletzt, weil die Schutzpflicht (hier aus Art. 2 II 1 iVm Art. 1 I 2 GG) objektiv-rechtlich und nur als Funktion zur Verstärkung der Grundrechte als Abwehrrechte begründet wird (→ Rn. 264 ff.). Weiter ist Grundlage der Freiheitsgrundrechte die **Gewährleistung der Sicherheit durch den Staat.** Anderenfalls ergibt sich daraus ein Einschüchterungseffekt.[790] Schließlich wird die Schwere des Eingriffs in die informationelle Selbstbestimmung dadurch gemindert, dass zwar viele Personen betroffen sind, aber regelmäßig nur anonym und hinsichtlich ohnehin bekannter Informationen wie Studienfächer, Religionszugehörigkeit etc[791] bzw. bei der Vorratsdatenspeicherung noch ohne spezifische Zuordnung. Eine Rasterfahndung oder Vorratsdatenspeicherung muss daher auch unterhalb der Schwelle einer konkreten Gefahr angeordnet werden können, sofern nur tatsächliche Anhaltspunkte wie Anschläge in anderen Ländern für einen entsprechenden Gefahrenverdacht vorliegen (→ Rn. 1613 f.). Eingriffe in die informationelle Selbstbestimmung sind eher über organisatorische Vorkehrungen ab- **451**

788 BVerfG NJW 2017, 217 Rn. 219, 285 ff. → Rn. 525.
789 Dies billigend BVerfGE 125, 260 (332) = NJW 2010, 833 – Vorratsdatenspeicherung II.
790 Sondervotum *Haas* BVerfGE 115, 320 (374) = NJW 2006, 1939 – Rasterfahndung.
791 Näher Sondervotum *Haas* BVerfGE 115, 320 (371 f.) = NJW 2006, 1939 – Rasterfahndung.

zumildern wie das alsbaldige Löschen nicht benötigter Daten und eine hinreichende Anonymisierung. So können auch heimliche Überwachungsmaßnahmen abgemildert werden, wenngleich bei diesen schärfere Grenzen bestehen müssen, sobald der Kernbereich privater Lebensgestaltung betroffen ist (→ Rn. 454). Aber auch insoweit ist denkbar, dass solche Daten unzugänglich gespeichert werden, bis sich neue Hinweise etwa auf eine Terrorgefährdung ergeben, welche die erneute Durchsicht dieser Daten veranlassen. Dann kann auf sie zurückgegriffen werden, am wirksamsten allerdings, wenn keine konkrete Gefahr verlangt wird, sondern eine abstrakte genügt.

452 **jj) GPS-Observation.** Den Weg über solche **organisatorischen Vorkehrungen** wählte das BVerfG im Hinblick auf Observationen mit einem Global Positioning System (GPS).[792] Solche Maßnahmen sind in § 100j I Nr. 2 StPO in hinreichend bestimmter Weise vorgesehen; sie müssen sich allerdings auf einen Beschuldigten beziehen, setzen also einen Anfangsverdacht voraus. Sie sind dem Betroffenen gegenüber zunächst verborgen (s. § 101 StPO); darin liegt ein **»additiver Grundrechtseingriff«,** der besondere Anforderungen an das Verfahren bedingt. Insbesondere um eine **stets unzulässige »Rundumüberwachung«** auszuschließen, müssen unkoordinierte Ermittlungsmaßnahmen verschiedener Behörden verlässlich verhindert werden, gegebenenfalls durch weitere Regelungen, deren Notwendigkeit sich erst im Laufe der Zeit herausstellt. Daher muss der Gesetzgeber künftige Entwicklungen beobachten.[793]

453 **kk) Heimliche Überwachungsmaßnahmen und Zweckänderungen von Daten: BKA-Urteil.** Auch für Online-Durchsuchungen verlangt das BVerfG eine konkrete Gefahr für hinreichend gewichtige Schutzgüter, und zwar selbst für Leben und Gesundheit, wenn sie durch Terror bedroht sind. Immerhin muss die Gefahr nicht schon in naher Zukunft eintreten. Indes müssen Tatsachen auf eine **im Einzelfall drohende Gefahr** und eine **bestimmte Person** weisen, sodass die Überwachungsmaßnahme gezielt gegen sie gerichtet werden kann.[794] An diesen Grundsätzen hat sich die Eingriffsbefugnis bei drohenden Gefahren nach Art. 11 III BayPAG orientiert (→ Rn. 867). Damit ergeben sich vergleichbare Probleme wie bei der Rasterfahndung. Aber insoweit handelt es sich um einen besonders gravierenden Eingriff, hier in die Integrität und Vertraulichkeit informationstechnischer Systeme (→ Rn. 429). An einem Eingriff fehlt es freilich, wenn im Internet verfügbare Kommunikationsinhalte erhoben werden, die an jeden bzw. an einen nicht abgegrenzten Personenkreis gerichtet sind (zB allgemein zugängliche Website; Interessierten offenstehende Mailingliste im Abo; offener Chat), außer diese Informationen werden gezielt zusammengetragen, gespeichert, ausgewertet bzw. mit anderen Daten vernetzt, sodass sich eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[795]

454 Liegt ein Eingriff vor, wird dessen Intensität weiter durch die **Heimlichkeit** und **mögliche Übergriffe auf** datenmäßig vernetzte unbeteiligte **Dritte** verstärkt. Daher ist schon ein **hinreichend gewichtiger Eingriffsanlass notwendig;** dieser muss zudem einzelfallbezogen **konkret** sein. Schließlich bedarf es geeigneter **Verfahrensvorkehrungen,** insbesondere einer vorbeugenden Kontrolle durch eine unabhängige Instanz

792 S. auch BVerfGE 100, 313 (384) = NJW 2000, 55 – Telekommunikationsüberwachung zu Art. 10 GG.
793 BVerfGE 112, 304 (316f., 319ff.) = NJW 2005, 1338 – GPS-Observationen.
794 BVerfGE 120, 274 (328f.) = BeckRS 2008, 32531 – Online-Durchsuchung.
795 BVerfGE 120, 274 (344f.) = BeckRS 2008, 32531 – Online-Durchsuchung.

und damit einer **richterlichen Anordnung.** Sie muss im Gesetz festgelegt sein. Nur dann ist die **Angemessenheit** gewahrt.[796] Gänzlich unangetastet muss der absolute Kernbereich privater Lebensgestaltung bleiben (→ Rn. 469f.). Auch darauf müssen sich die verfahrensmäßigen Sicherungen beziehen. Erforderlich ist, dass insoweit Datenerhebungen möglichst unterbleiben, nämlich wenn konkrete Anhaltspunkte dafür bestehen. Notwendig ist weiter eine Durchsicht der erhobenen Daten und, wenn sie kernbereichsrelevant sind, deren unverzügliche Löschung.[797] Diese Grundsätze übertrug das BVerfG auf alle heimlichen Überwachungsmaßnahmen. Diese Löschung ist so zu protokollieren, dass eine spätere Kontrolle möglich ist.

Eine konkrete Gefahr verlangt das BVerfG mithin auch für **heimliche Überwachungsmaßnahmen** wie Wohnraumüberwachungen, Online-Durchsuchungen, Telekommunikationsüberwachungen, Telekommunikationsverkehrsdatenerhebungen und Überwachungen außerhalb von Wohnungen mit besonderen Mitteln der Datenerhebung. Diese reichen tief in das Privatleben hinein. Zwar dürfen solche heimlichen Überwachungsmaßnahmen grundsätzlich zur Abwehr von Gefahren des internationalen Terrorismus ergriffen werden. Indes dürfen **nicht verantwortliche Dritte** aus dem Umfeld von Zielpersonen aus dem Terrorismus nur mit spezifischen Regelungen ins Visier genommen werden, um deren **Kernbereich privater Lebensgestaltung** und **Berufsgeheimnisse zu schützen.** Hierfür bedarf es transparenter Vorgehensweisen, individuellen Rechtsschutzes und aufsichtlicher Kontrolle. Die erhobenen Daten müssen wieder gelöscht werden. Hierzu bedarf es gesetzlicher Regelungen.[798] Das gilt auch für die **Nutzung und Übermittlung staatlich erhobener Daten.** Diese sind grundsätzlich **zweckgebunden.** Sie dürfen also nur für den Zweck aus dem jeweiligen Ermittlungsverfahren verwendet werden, zu dem sie erhoben wurden. Eine weitere Nutzung ist grundsätzlich nur durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter zulässig. Für Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme müssen zudem für jede weitere Nutzung auch die Anforderungen an die Gefahrenlage erfüllt sein, welche schon für die Datenerhebung maßgeblich waren.[799] **455**

Diese Zweckbestimmung kann nur sehr begrenzt überschritten werden. Eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung und damit eine Zweckänderung muss dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Es gilt also der **Grundsatz** der **hypothetischen Datenneuerhebung.** Dafür genügt das Vorliegen eines **konkreten Ermittlungsansatzes;** es ist also keine konkretisierte Gefahrenlage wie bei der ursprünglichen Datenerhebung zu verlangen. Auch hier bedarf es aber einer solchen konkretisierten Gefahrenlage, wenn es um Daten aus Wohnraumüberwachungen und Online-Durchsuchungen geht. Damit muss sich also auch dann, wenn eine Ermittlungsmaßnahme auf der Basis konkreter Verdachtsmomente für drohende Straftaten zu Ende geführt wurde, erst wieder ein solcher konkreter Verdacht ergeben, um die bereits erhobenen Daten auch für einen anderen Zweck verwen-

796 BVerfGE 120, 274 (326ff.) = BeckRS 2008, 32531 – Online-Durchsuchung.
797 BVerfGE 120, 274 (338) = BeckRS 2008, 32531 – Online-Durchsuchung.
798 BVerfG NJW 2016, 1781 (Ls. 1) – BKA-Gesetz.
799 BVerfG NJW 2016, 1781 (Ls. 2a und 2b) – BKA-Gesetz.

den zu können. Verlangt man gar dieselben Rechtsgüter, haben sich also etwa Hinweise auf einen Terroranschlag als falsch erwiesen, tauchen aber neue Anhaltspunkte für einen solchen auf, muss erst gewartet werden, bis diese Anhaltspunkte eine konkrete Gefahr sichtbar werden lassen. Erst dann dürfen ursprünglich erhobene Daten durch dieselbe Behörde weiter genutzt werden, sofern es sich um Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme handelt. Entsprechendes gilt, wenn die ursprünglich zur Vereitelung eines Anschlages erhobenen Daten nun verwendet werden sollen, um eine terroristische Vereinigung auszuheben. Von dieser muss dann erst eine konkrete Gefahr drohen.

456 Die vorgenannten Grundsätze der Zweckänderung- und Zweckbindung bestehen auch, wenn **Daten an staatliche Stellen im Ausland** übermittelt werden sollen. Zudem müssen sich dann die deutschen Behörden vergewissern, dass ein hinreichend rechtstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist.[800] Danach durften etwa auch auf verfassungsrechtlicher Grundlage keine Daten in die USA übermittelt werden, solange dort nicht Rechtsschutz für den Einzelnen gewährleistet ist. Dies setzt nunmehr auch das Abkommen zwischen EU und den USA über die **Übermittlung von Fluggastdaten** voraus. Damit reagierte die EU auf das Safe-Harbor-Urteil des EuGH (→ Rn. 43).

ll) Automatisierte Kennzeichenerfassung[801]

457 **Fall** nach BVerfGE 120, 378 = NJW 2008, 1505 und BVerfG Beschl. v. 18.12.2018 – 1 BvR 142/15 sowie 1 BvR 2795/09, 1 BvR 3187/10, NJW 2019, 827 sowie 842: Auch für die automatisierte Erfassung von Autokennzeichen (zur Gesetzgebungskompetenz → Rn. 209) verlangt das BVerfG konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen. Die Frage, ob solche vorhanden sind, kann sich auch für die Überwachung eines Dieselfahrverbotes (dazu auch → Rn. 504: Verhältnismäßigkeit und Entschädigung, → Rn. 829: Betriebsuntersagung wegen Abschalteinrichtung, → Rn. 1050: vorbeugende Unterlassungsklage und → Rn. 1297: Fortschreibung Luftreinhalteplan) stellen. Der Bundesrat hat den eine offene Datenerhebung zum Schutz vor Abgasen vorsehenden Gesetzesentwurf (BR-Drs. 574/18) unter Verweis auf das BVerfG-Urteil am 14.12.2018 in seiner Stellungnahme abgelehnt (BR-Drs. 574/18, B). Zu Recht?

Das Ziel eines Abgleichs mit einem gesetzlich nicht näher definierten Fahndungsbestand, namentlich, aber nicht konkret festgelegt, um ausgeschriebene Fahrzeuge ausfindig zu machen, genügte dem BVerfG nicht. Allerdings richtet sich das Ausmaß der Anforderungen nach der Intensität des Grundrechtseingriffs. Diese hängt davon ab,

- wie persönlichkeitsrelevant die erfasste Information ist,
- wie sie weiterverwendet und verarbeitet wird, zumal wenn daraus Folgemaßnahmen erwachsen können,
- ob der Betroffene einen zurechenbaren Anlass gegeben hat (zB Autodiebstahl),
- die Ermittlungsmaßnahme heimlich erfolgt bzw.
- wie viele (unbeteiligte) Personen erfasst werden.

Nur stichprobenhafte, nicht flächendeckende Kennzeichenerfassungen können gegebenenfalls ohne konkreten Anlass zulässig sein.
An einem Eingriff fehlte es nach der erstgenannten BVerfG-Entscheidung sogar ganz, wenn der Abgleich automatisiert erfasster Kraftfahrzeugkennzeichen mit dem Fahndungsbestand unverzüglich er-

800 BVerfG NJW 2016, 1781 (Ls. 3) – BKA-Gesetz.
801 *Cornils* JURA 2010, 443.