# Kapitel C: Massenüberwachung im Europarecht

Staatliche Überwachungsmaßnahmen kollidieren nicht nur mit den deutschen Grundrechten, sondern auch mit europäischem Primär-, Sekundär- und Konventionsrecht. Auch in diesem findet sich allerdings keine eigenständige Begrifflichkeit der *Überwachung*. Stattdessen wird ebenfalls im Rahmen der Eingriffsbestimmung auf die einzelnen Datenverarbeitungsschritte abgestellt, wobei abermals die Intensitätsbewertung nicht isoliert, sondern im Rahmen einer Gesamtbetrachtung erfolgt, die auf die Wechselwirkung der einzelnen Verarbeitungsschritte abstellt.[314]

Der EuGH hat sich insbesondere mit seiner Rechtsprechung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten („TK-Verkehrsdaten") profiliert. In einer ganzen Reihe von Urteilen hat er nicht nur die unionsrechtliche Verpflichtung zur universellen Verkehrs- und Standortdatenspeicherung in Form der (TK-)VDS-RL[315] aufgehoben[316], sondern auch eigenständig erarbeitete nationale Regelungen der Mitgliedsstaaten für unionsrechtswidrig erklärt.[317]

Auch zur Speicherung und sicherheitsbehördlichen Verwendung von TK-Bestands-[318] sowie von Fluggastdaten[319] hat sich der EuGH geäußert

314 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 59 ff. = NJW 2014, 2169; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

315 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, ABl. 2006 L 105/54.

316 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

317 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531; Urteil v. 2.3.2021, C-746/18 (Prokuratuur) = NJW 2021, 2103; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

318 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

319 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706; Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) = ZD 2018, 23.

und dabei die Erkenntnisse aus den Urteilen zur Vorratsdatenspeicherung übertragen und weiterentwickelt.

Mit der Speicherung und Analyse von Finanzinhaltsdaten sowie dem Zugriff auf solche Daten durch Sicherheitsbehörden hat sich der EuGH bislang noch nicht auseinandergesetzt. Dem Verfasser sind im September 2023 keine anhängigen Verfahren bekannt. Lediglich bestimmte Transparenzregeln der 4./5. Geldwäscherichtlinie (GWRL) über Vermögensberechtigte hat der Gerichtshof auf Verstöße mit Unionsgrundrechten und Datenschutzrecht hin überprüft und aufgehoben.[320] Ein Urteil, das sich allgemein mit den Maßnahmen zur Geldwäschebekämpfung beschäftigt, steht noch aus.

Der unionsrechtliche Rahmen für staatliche (Massen-)Überwachungsmaßnahmen soll in diesem Kapitel anhand der soeben genannten Urteile dargestellt werden, bevor später die in den folgenden Kapiteln thematisierten Maßnahmen auf ihre Vereinbarkeit mit dem Unionsrecht überprüft werden. Dabei soll auch kurz erläutert werden, inwiefern das Unionsrecht für Maßnahmen deutscher Sicherheitsbehörden überhaupt einschlägig ist.

## *I. Kurzübersicht: Europarechtlicher Schutz vor Überwachung*

Wie auch das Grundgesetz hält das Unionsrecht bestimmte Vorschriften bereit, die die Privatheit, insbesondere im Rahmen von Kommunikation, schützen. Sie finden sich nicht nur primärrechtlich in der EU-Grundrechtecharta (EU-GRC)[321], sondern auch in der EMRK und im Unionssekundärrecht, dort in der Datenschutzgrundverordnung (DSGVO)[322], der Richt-

320 EuGH, Urt. v. 22.11.2022 – C-37/20, C-601/20 (WM ua/Luxembourg Business Registers) = NJW 2023, 199.

321 Charta der Grundrechte der Europäischen Union, Abl. 2012 C 326/02.

322 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. 2016 L 119/1.

linie über den Datenschutz bei Sicherheitsbehörden (JI-RL)[323] und der Datenschutzrichtlinie für elektronische Kommunikation (e-Privacy-RL)[324].

### 1. Unionsgrundrechte: Art. 7, 8 EU-GRC, Art. 16 Abs. 1 AEUV

Im Europäischen Primärrecht schützen insbesondere die Art. 7, 8 EU-GRC und Art. 16 Abs. 1 AEUV vor staatlichen Überwachungsmaßnahmen.

Nach Art. 7 EU-GRC hat *jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation*. Art. 8 Abs. 1 EU-GRC bestimmt, dass jeder Person ein Recht auf *Schutz der sie betreffenden personenbezogenen Daten* zusteht. Nach Art. 8 Abs. 2 EU-GRC dürfen solche *Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten, legitimen Grundlage verarbeitet werden*. Jede Person hat danach weiter das Recht, *Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*

Identisch zu Art. 8 Abs. 1 EU-GRC ist Art. 16 Abs. 1 AEUV formuliert. Das ist problematisch, da nach Art. 52 Abs. 2 EU-GRC die subjektiven Rechte der Verträge (EUV/AEUV) vorrangig anwendbar sind und die in der Charta enthaltenen Schranken insofern nicht unmittelbar gelten können.[325] Da Art. 16 Abs. 1 AEUV anders als Art. 8 EU-GRC keine Schranken beinhaltet, liefen die Schranken des Art. 8 Abs. 2, 3 EU-GRC dem Wortlaut nach leer. Dieses Ergebnis wird als offenkundiges Redaktionsversehen aufgefasst, für das verschiedene Lösungsvorschläge angeboten werden. Alle laufen im Ergebnis darauf hinaus, dass die doppelte Niederschrift des Datenschutzrechts keine inhaltlichen Auswirkungen hat und den Schranken des Art. 8

323 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Abl. 2016, L 119/89.

324 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Abl. 2002 L 201/37.

325 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 52 Rn. 11 mwN; aA. *Jarass* in Jarass EU-GRC Art. 52 Rn. 54.

Abs. 2, 3 EU-GRC volle Geltung zukommt.[326] Im Folgenden wird daher das Datenschutzgrundrecht allein anhand des Art. 8 EU-GRC behandelt.

Art. 7 und 8 EU-GRC ließen sich, ähnlich der grundgesetzlichen Konstruktion (s. o. Kap. B. II.), als bereichsspezifisches Privatheits- und allgemeines Datenschutzrecht verstehen, die als eigenständige Grundrechte mit Spezialitätsvorrang behandelt werden könnten.[327] Art. 7 EU-GRC schütze nach dieser in Deutschland gängigen Lesart das Privatleben als solches, während Art. 8 EU-GRC spezifisch solche Daten schützt, die nicht in Zusammenhang mit dem Privatleben stehen.[328]

Der EuGH nahm in seiner früheren Rechtsprechung eine solche getrennte Betrachtungsweise aber nicht vor, sondern behandelte Art. 7, 8 EU-GRC letztlich als einheitlichen Schutz solcher Daten, die das Privatleben betreffen.[329] Erst seit den Urteilen zur Vorratsdatenspeicherung hat ein differenziertes Verständnis Eingang in die Rechtsprechung gefunden, wobei aber weiterhin keine völlig klare Trennung der Grundrechte vorgenommen wird.[330]

Während das BVerfG etwa die TK-Vorratsdatenspeicherung wegen dessen Spezialität allein als Eingriff in das Telekommunikationsgeheimnis i. S. d. Art. 10 Abs. 1 GG bewertete[331], prüfte der EuGH hinsichtlich der unionsrechtlichen und nationalen Regelungen zur TK-Vorratsdatenspeicherung

326 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada), Rn. 120 = ZD 2018, 23; übersichtlich *Wolff* in Frankfurter Kommentar, AEUV Art. 16 Rn. 11 f.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 30.

327 Ausf. zum Verhältnis *Marsch,* Datenschutzgrundrecht, 2018, S. 203 ff.; *J. Kokott/Sobotta*, Int. Data Privacy Law 3 (2013), 222; *Gellert/Gutwirth,* Computer Law & Security Review 29 (2013), 522 (524 ff.); *W. Michl*, DuD 2017, 349.

328 *Generalanwalt Villalón*, Schlussantrag v. 12.12.2013, C-293/12, Rn. 62 ff. – Digital Right Ireland; *Schiedermair,* Schutz des Privaten, 2012, S. 349; *Jarass* in Jarass EU-GRC Art. 8 Rn. 4; *Streinz* in Streinz EUV/AEUV, EU-GRC Art. 8 Rn. 7; *Guckelberger*, EuZW 2011, 126 (128).

329 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435; Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52; Urteil v. 09.01.2008, C–275/06 (Promusicae/Telefónica), Rn. 64; *González Fuster,* Data Protection, 2013, S. 234 ff.; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.; *Streinz* in Streinz EUV/AEUV, EU-GRC Art. 8 Rn. 7; *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 2; zu den Vorteilen dieser Rspr. *Marsch,* Datenschutzgrundrecht, 2018, S. 217 ff.; *W. Michl*, DuD 2017, 349 (353), der aber auch eine vorrangige Anwendung nur des Art. 8 EU-GRC als lex specialis für vertretbar hält.

330 *Marsch,* Datenschutzgrundrecht, 2018, S. 203 f.

331 BVerfGE 125, 260 (309 ff.) – Vorratsdatenspeicherung.

und PNR-Überwachung eine Verletzung „der sich aus *Art. 7, 8 EU-GRC ergebenden (Grund-)Rechte*".[332]

Der EuGH geht mithin offenbar davon aus, dass es sich grundsätzlich um zwei verschiedene Schutzbereiche handelt. Vor allem in *Digital Rights Ireland* und *Ligue des droits humains (PNR)* kommt diese Trennung von Art. 7 und 8 EU-GRC durch eine separate Schutzbereichsbestimmung deutlich zum Ausdruck.[333] Für die Bewertung der geprüften Maßnahmen spielt aber die Dualität der verschiedenen Grundrechte weiterhin keine Rolle. Ähnlich dem BVerfG[334] bewertet der EuGH die Intensität der Eingriffe nicht in Abhängigkeit von den konkret betroffenen Grundrechten, sondern anhand von Maßstäben (dazu unten), die einem einheitlichen Privatheitsschutz entsprechen, und begründet dies mit der *besonderen Bedeutung des Datenschutzes für die Privatheit.*[335] Auf der Prüfungsebene des Schutzbereichs kann daher von einer *parallelen*[336] statt einheitlichen Prüfung der Art. 7 und 8 EU-GRC gesprochen werden.

Der Datenschutz i. S. d. Art. 8 Abs. 1 EU-GRC ist dabei denkbar weit ausgerichtet. Er umfasst sämtliche Informationen über eine identifizierte oder identifizierbare natürliche Person[337] und spiegelt sich insofern in Art. 4 Nr. 1 DSGVO wider.[338] Überhaupt scheint der EuGH die grundrechtliche Ebene mit der einfachgesetzlichen Ausgestaltung zu verknüpfen. Er definiert Eingriffe in Art. 8 Abs. 1 EU-GRC neuerdings anhand Art. 4 Nr. 2 DSGVO

332 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), 100 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 115 = NJW 2021, 531; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 ff. = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), 79 = NJW 2022, 3135.

333 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 ff. = EuZW 2022, 706.

334 Dazu *Gusy*, KritV 2000, 52 (53 ff.); *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 88 f., Fn 470 mwN; S. 165; eindrücklich am Bsp. von BVerfGE 141, 220 – BKA-Gesetz: *Rusteberg*, KritV 2017, 24 (27 ff.).

335 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 53 = NJW 2014, 2169.

336 *Kühling*, NVwZ 2014, 681 (682); *Jarass* in Jarass EU-GRC Art. 8 Rn. 4; *Johlen* in Stern/Sachs EU-GRC Art. 28 Rn. 24, Fn 51.

337 EuGH, Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52.

338 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art.8 Rn. 10; *Jarass* in Jarass EU-GRC Art. 8 Rn. 6.

gleich.[339] Jeder einzelne Verarbeitungsschritt i. S. d. Art. 4 Nr. 2 DSGVO stellt einen Eingriff in Art. 8 Abs. 1, 2 EU-GRC dar.[340]

Der EuGH versteht Art. 8 Abs. 1, 2 EU damit als (Quasi-)Herrschaftsrecht[341] über persönliche Daten, also als Recht einer Person, andere von der Verarbeitung ihrer Daten auszuschließen.[342] Das entspricht der Rechtsprechung des BVerfG zum Recht auf informationelle Selbstbestimmung. Trotz der Kritik an diesem Verständnis, ist im Ergebnis unstreitig, dass sicherheitsrechtliche Überwachungsgesetze konkreten grundrechtlichen Anforderungen unterliegen. Diese werden von der Rechtsprechung des EUGH laufend spezifiziert.

### 2. Konventionsrecht: Art. 8 EMRK und die Datenschutzkonvention

Den Schutz vor staatlicher Überwachung gewährleistet in Europa nicht nur das Unionsrecht, sondern auch die Europäische Menschenrechtskonvention – EMRK.[343]

Wie bereits erwähnt, orientiert sich Art. 7 EU-GRC stark an Art. 8 Abs. 1 EMRK, wonach *jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat.* Ein eigenständiges Datenschutzrecht wie Art. 8 EU-GRC sieht die EMRK nicht vor, weshalb der EGMR bei der Behandlung staatlicher Datenverarbeitungen auf den Privatheitsschutz verwiesen war und ist.

Dabei stellte er schon 1987 hinsichtlich eines Polizeiregisters recht pauschal fest, dass die Speicherung und Freigabe persönlicher Informationen

339 Etwa EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531; zum Verhältnis der DSGVO zu Art. 7, 8 EU-GRC: *Marsch,* Datenschutzgrundrecht, 2018, S. 130 f.; *Schiedermair* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO, Einl. Rn. 169 ff.

340 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 13.

341 *Lynskey*, Int. & Comp. Law Quarterly 63 (2014), 569 (589 ff.); *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art.8 Rn. 10.

342 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435.; krit. *González Fuster/Gutwirth*, Computer Law & Security Review 29 (2013), 531 (537); übersichtlich *Marsch,* Datenschutzgrundrecht, 2018, S. 127 ff.; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 50 f.

343 Europäische Menschenrechtskonvention (Konvetion zum Schutze der Menschenrechte und Grundfreiheiten) vom 04.11.1950, zuletzt geändert durch Protokoll Nr. 15 vom 24.6.2013.

einen Eingriff in das von Art. 8 Abs. 1 EMRK garantierte Recht auf Privatleben darstellen[344] und entwickelte von diesem Ausgangspunkt einen konventionsrechtlichen Datenschutz als Ausprägung der Privatheit.[345] Wie stark dieser Schutz ausgeprägt ist, wird allerdings unterschiedlich beurteilt.[346]

Auffällig an der Rechtsprechung des EGMR zu Art. 8 Abs. 1 EMRK ist die streng kasuistische Vorgehensweise. Bis heute hat der EGMR keine klare Begriffsdefinition des *Privatlebens* bereitgestellt, sondern entscheidet stets im Einzelfall, ob der staatliche (Informations-)Eingriff einen Eingriff in dieses darstellt.[347] Dabei werden zwei Rechtsprechungslinien[348] ausgemacht, wovon eine bei der Schutzbereichsbestimmung an die – weit auszulegende –Persönlichkeitsrelevanz der jeweiligen Daten anknüpft[349] und die andere auf das Ausmaß bzw. die Systematik der Datensammlung abstellt.[350] Aus letzter ließe sich ableiten, dass der EGMR bei Art. 8 Abs. 1 EMRK nicht mehr zwischen Datenschutz und Privatheit trennt, sondern wie das BVerfG jede Datenverarbeitung als Grundrechtseingriff behandelt und somit letztlich ebenfalls ein Recht auf informationelle Selbstbestimmung anerkennt.[351] Als Argument hierfür wurde der Erlass der Datenschutzkonvention[352] durch den Europarat im Jahr 1981 angeführt, die allerdings bis zur Vorlage des Protokolls im Jahr 2018[353] nur für automatisierte Verarbeitungen gilt

344 EGMR, Urt. v. 26.03.1987, 9248/81 (Leander/Schweden), Rn. 47.

345 *Schiedermair,* Schutz des Privaten, 2012, S. 239 ff.; *Marsch,* Datenschutzgrundrecht, 2018, S. 8 ff.

346 Übersichtlich *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 14 ff.; ein „Grundrecht auf Datenschutz" erkennt *Schiedermair,* Schutz des Privaten, 2012, S. 242; ähnlich *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 29; aA *Marsch,* Datenschutzgrundrecht, 2018, S. 12 ff.

347 Vgl. etwa EGMR, Urt. 25.09.2001, Nr. 44787/98 (PG u. JH/Vereinigtes Königreich), Rn. 57.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 14 mwN.

348 So *Gellert/Gutwirth*, Computer Law & Security Review 29 (2013), 522 (526); *Marsch,* Datenschutzgrundrecht, 2018, S. 9 ff.

349 EGMR, Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 65 ff.

350 EGMR, Urt. v. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien), Rn. 43 ff.

351 *Schiedermair,* Schutz des Privaten, 2012, 242 ff.; *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 29.

352 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Sammlung Europäischer Verträge - Nr. 108).

353 Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Sammlung Europäischer Verträge - Nr. 223).

und grundsätzlich keine individuellen Rechte beinhaltet[354], allerdings zum Ausdruck bringen könnte, dass schon damals ein grundrechtlicher Datenschutz anerkannt wurde.[355]

Gegen einen prinzipiellen konventionsrechtlichen Datenschutz sprechen laut den insofern skeptischen Autoren[356] aber jüngere Urteile des EGMR, die weiterhin staatliche Datenverarbeitungsmaßnahmen nur unter bestimmten Voraussetzungen als Eingriff ansehen wollen. Es soll auf den Kontext und das Ausmaß der Maßnahme[357] oder die Privatheitserwartungen der Betroffenen ankommen.[358]

Sind Daten von einer staatlichen Maßnahme betroffen, die der *Wohnung* oder der *Korrespondenz* zugeordnet werden können, ist die Zuordnung zum Privatleben vom Gesetzestext vorgegeben. Anders als im Grundgesetz besteht kein exklusives Spezialitätsverhältnis zwischen einem bereichsspezifischen und einem allgemeinen Privatheitsschutz, wenngleich der Begriff des Privatlebens als Lückenfüller verwendet wird.[359] Vielmehr handelt es sich bei der Wohnung und der Korrespondenz um anerkannte Teilbereiche des Privatlebens.[360] Der EMRK bemüht sich daher nicht um eine eindeutige Abgrenzung, sondern stellt etwa bei Dokumentenbeschlagnahmen schlicht fest, dass durch die Beschlagnahme (auch) von Korrespondenzdokumenten ein Eingriff in das Recht auf Schutz des Privatlebens vorliegt.[361]

Mit „Korrespondenz" war ursprünglich nur der Briefverkehr gemeint, der Begriff wurde vom EGMR jedoch sukzessive erweitert und umfasst heute sämtliche Mittel der Fernkommunikation[362], wobei nicht nur die

354 *Kübler,* Säulen der Europäischen Union, 2002, S. 37 ff.; *Johlen* in Stern/Sachs EU-GRC, Art. 8 Rn. 18 Fn 32.

355 *Schiedermair,* Schutz des Privaten, 2012, S. 242 ff.; s.a. EGMR, Urt. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien), Rn. 43 ff.

356 *Marsch,* Datenschutzgrundrecht, 2018, S. 12 ff.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 15; ähnlich *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 54 f.

357 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 67 = EuGRZ 2009, 299.

358 EGMR Urt. 25.09.2001, Nr. 44787/98 (PG u. JH/Vereinigtes Königreich), Rn. 57.

359 *Schiedermair,* Schutz des Privaten, 2012, S. 232 ff.

360 *Gaede* in MüKo StPO, EMRK Art. 8 Rn. 1 "Oberbegriff".

361 Vgl. EGMR, Urt. v. 16.12.1992, Nr. 13710/88 (Niemitz/Deutschland), Rn. 27 ff; dazu krit. *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022.

362 EGMR, Urt. v. 06.09. 1978, Nr. 5029/71 (Klass u.a./Deutschland), Rn. 41 = NJW 1979, 1755; Urt. v. 05.09.2017, Nr. 61496/08 (Bărbulescu/Rumänien), Rn. 72.

Inhalte, sondern auch die Kommunikationsumstände geschützt werden.[363] Art. 8 Abs. 1 EMRK garantiert also ebenso wie der diesem nachgebildete Art. 7 EU-GRC einen umfassenden Kommunikationsschutz.[364] Im Vergleich zu Art. 10 GG ist der Schutz sogar erweitert, da Art. 8 Abs. 1 EMRK auch vor Kommunikationsverboten, -unterbrechungen und -verzögerungen schützt[365] und ferner auch dann noch gilt, wenn das Kommunikationsmedium sich im Herrschaftsbereich des Empfängers befindet und dort aufbewahrt wird.[366]

## *II. Massenüberwachung in der Rechtsprechung des EuGH*

Soweit staatliche Überwachungsmaßnahmen ihre Grundlage im EU-Recht finden, spielt das Sekundärrecht eine geringe Rolle, da dieses nur einen Rahmen der Verarbeitung vorgibt und sich gegenüber gesetzlichen Ermächtigungen und Abweichungen offen zeigt. Maßgeblich für die Gestaltung sind also weniger die DSGVO und JI-Rl als die Art. 7, 8 EU-GRC bzw. die hierzu ergangene Rechtsprechung des EuGH, die im Folgenden erläutert werden soll. Ganz ähnlich dem BVerfG hat der Gerichtshof in einer Reihe prominenter Urteile spezifische Anforderungen an staatliche Überwachungsmaßnahmen – insbesondere zur Vorratsdatenspeicherung und Datenanalyse – aus dem Grundsatz der Verhältnismäßigkeit entwickelt.

### 1. Telekommunikationsdaten

Die bislang wohl wirkmächtigsten Urteile des EuGH zu sicherheitsrechtlichen Überwachungsmaßnahmen befassen sich mit Telekommunikationsdaten.

---

363 EGMR Urt. v. 03.04.2007, Nr. 62617/00 (Copland/Vereinigtes Königreich), Rn. 41 = MMR 2007, 431.

364 *Gersdorf* in BeckOK Informations-/MedienR, EU-GRC Art. 8 Rn. 41; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 39.

365 *Hermes* in Dreier GG Art. 10 Rn. 7; *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 67.

366 Vgl. EGMR, Urt. v. 16.12.1992, Nr. 13710/88 (Niemitz/Deutschland), Rn. 27 ff.; *Böhringer/Marauhn* in Konkordanzkommentar Kap. 16 Rn. 61 mwN.

### a. TK-Verkehrsdaten

Insbesondere mit den Urteilen zur Vorratsdatenspeicherung von TK-Verkehrsdaten hat sich der Gerichtshof als bedeutende Institution auf dem Gebiet des Sicherheitsverfassungsrechts etabliert. Diese Rechtsprechung nahm ihren Ausgang im Jahr 2006 mit dem Erlass der VDS-RL[367] durch die EU.[368]

Mit dieser Richtlinie wollte die EU sicherstellen, dass bestimmte Daten *zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen*, Art. 1 Abs. 1 VDS-RL.

Nach Art. 3, 5 der VDS-RL sollten die Mitgliedstaaten deshalb vorsehen, dass Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bzw. Betreiber eines öffentlichen Kommunikationsnetzes die bei ihnen anfallenden Telekommunikationsverkehrs- und Standortdaten[369] speichern und zwar nach Art. 6 der Richtlinie für mindestens sechs Monate.

Diese Daten sollten den *zuständigen Behörden* nach Maßgabe mitgliedstaatlicher Vorschriften zugänglich sein, wobei die Ausgestaltung, d. h. das „Wie" dieser Zugangsregeln, vollständig den Mitgliedstaaten überlassen wurde, Art. 4 VDS-RL. Einzig die Umschreibung des Anwendungsbereichs in Art. 1 Abs. 1 der Richtlinie begrenzte die Ausgestaltungsmöglichkeiten, da hiernach die Vorratsdatenspeicherung nur zur Bekämpfung *schwerer* Straftaten vorgesehen war. Es blieb allerdings den Mitgliedstaaten überlassen, zu bestimmen, welche Delikte der nationalen Straftatbestände als schwere Kriminalität in diesem Sinne gelten sollten.[370]

---

367 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, ABl. 2006 L 105/54.

368 Übersichtlich zum Inhalt *Westphal*, EuR 2006, 706; zur Historie statt vieler *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 148 ff. mit umfg. Übersicht zur Lit.; *Szuba,* Vorratsdatenspeicherung, 2011, S. 48 ff.; *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (3 ff.); *Bignami* Chicago J. of Int. Law 2007, 233 (238 ff.).

369 Vgl. heute § 3 Nr. 70, § 176 TKG; *Moser-Knierim*, Vorratsdatenspeicherung, 2014, S. 141; manchmal auch „Metadaten" vgl. Art. 4 Abs. 3 Lit a) b) c) e-Privacy-VO (Vorschlag der EU Kommission, COM(2017) 10 final - 2017/0003 (COD)); zu den Begriffen auch *Schramm/Shvets*, MMR 2019, 568 (569 (Fn. 24)).

370 Hierzu früh krit. *Breyer*, StV 2007, 214 (217 f.).

aa. Unionsrechtswidrigkeit der VDS-RL: *Digital Rights Ireland*

Gegen die VDS-RL erhoben die NGO *Digital Rights Ireland* vor dem Irischen High Court sowie die Kärntner Landesregierung gemeinsam mit über 11.000 Personen vor dem österreichischen Verfassungsgerichtshof Klagen, die jeweils zu Vorabentscheidungsverfahren am EuGH führten und dort zusammengefasst behandelt wurden.[371]

Der EuGH sollte insbesondere prüfen, ob die VDS-RL mit Unionsprimärrecht, insbesondere dem Recht auf Privatheit nach Art. 7 und dem Recht auf Datenschutz nach Art. 8 EU-GRC, sowie mit dem eng verwandten (s.o. I. 1. a.) Recht auf Privatheit nach Art. 8 EMRK vereinbar ist.

(1) Formelle Rechtswidrigkeit mangels Kompetenz der EU?

Dabei wurde bereits vor der Entscheidung an der formellen Rechtmäßigkeit der Richtlinie gezweifelt, da die Kompetenz der EU fraglich erschien.[372] Der EU-Gesetzgeber stütze die VDS-RL auf Art. 95 Abs. 1 EG[373] (heute 114 Abs. 1 AEUV). Dieser räumte der EU die Kompetenz zur Angleichung von Rechtsnormen ein, *die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.* Die Kommission argumentierte, dass aufgrund der bisherigen Rechtslage unterschiedliche Regelungen einer sicherheitsrechtlichen Vorratsdatenspeicherung möglich seien und deshalb eine Harmonisierung erforderlich sei.[374] Tatsächlich dürfte die Wahl der Kompetenzgrundlage aber schlicht auf einer politischen Notwendigkeit beruht haben, da auf Art. 95 Abs. 1 EG gestützte Richtlinien anders als Rahmenbeschlüsse i. S. d. Art. 34 Abs. 2 EG[375] (Art. 29 EUV) lediglich eine qualifizierte Mehrheit im Rat erforderten, Art. 251 Abs. 2 EG.[376]

371 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 17 ff. = NJW 2014, 2169; *Tracol*, Computer Law & Security Review 30 (2014), 736 (737).

372 BT-Drs. 16/1622, S. 4 ff.; *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel*, MMR 2007, 411 (412 f.); *Breyer*, StV 2007, 214 (215 f.); *Flynn* UC Dublin Law Rev. 8 (2008), 1.

373 Vertrag zur Gründung der Europäischen Gemeinschaft, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

374 Erwägungsgründe Nr. 1, 5, 6 VDS-RL.

375 Vertrag über die Europäische Union, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

376 *Wissenschaftliche Dienste des Bundestags,* Vorratsdatenspeicherung, 2006, S. 8.

Zuvor war der EuGH hinsichtlich der bilateral vertraglich eingeführten Verpflichtung von Airlines, Fluggastdaten an US-Sicherheitsbehörden weiterzugeben (dazu unten II. 2.)[377], zu dem Ergebnis gelangt, dass eine solche Datenverarbeitung zu Sicherheitszwecken nicht in den Anwendungsbereich des Europäischen Datenschutzrechts fiel. Mangels einer solchen Verbindung der Regelung zum Unionsrecht komme Art. 95 Abs. 1 EG als Kompetenznorm nicht infrage. Die Verpflichtung zur Weitergabe von Fluggastdaten per Rahmenbeschluss hielt der Gerichtshof daher für rechtswidrig.[378]

Da die VDS-RL ebenfalls Private zu Datenverarbeitungen verpflichtete, die *schwerpunktmäßig*[379] sicherheitsrechtlichen Pflichten dienen sollten, wurde eine Übertragung dieser Rechtsprechung erwartet.[380] Die Republik Irland, unterstützt von weiteren Mitgliedstaaten, erhob denn auch noch im Jahr 2006 Nichtigkeitsklage und rügte die fehlende Kompetenz der Union.

Der EuGH wies diese Klage zurück.[381] Die VDS-RL betreffe unmittelbar keine Datenverarbeitung zum Schutz der öffentlichen Sicherheit. Sie adressiere unmittelbar nur die (privatwirtschaftlichen) Anbieter von Telekommunikationsdiensten im Binnenmarkt, da die Umstände, unter denen die Sicherheitsbehörden der Mitgliedstaaten auf die zu speichernden Daten zugreifen könnten, in der Richtlinie nicht geregelt seien.[382] Bei der Weiterleitung von Fluggastdaten an die US-Sicherheitsbehörden habe der Fall anders gelegen, da dort unmittelbar eine Verarbeitung durch die Sicherheitsbehörden der Mitgliedstaaten vorgesehen sei.[383]

377 Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security, ABl. 2004, L 183/83.

378 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA) = NJW 2006, 2029; dazu *Simitis*, NJW 2006, 2011.

379 Zur „Schwertpunktheorie" EuGH, Urteil vom 30.01.2001, C-36/98 (Spanien/Rat), Rn. 59 = EuZW 2001, 208; Urt. v. 11.06.1991, C-300/89 (Titanoum Dioxid); *Terhechte* in Frankfurter Kommentar, AEUV Art. 114 Rn. 33; gegen die Anwendung bei vertikalen Konflikten *Tietje* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 114 Rn. 125.

380 *Flynn* UC Dublin Law Rev. 8 (2008), 1 (11 f.); *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel, MMR* 2007, 411 (412 f.); *Breyer*, StV 2007, 214 (215 f.).

381 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.).

382 Idem, Rn. 91.

383 Ibid.

(2) Unvereinbarkeit mit Primärrecht wegen unverhältnismäßiger Beschränkung der Art. 7, 8 EU-GRC

Erfolgreicher als der irische Staat war die Gruppe *Digital Rights Ireland* mit ihrer Grundrechtsklage bzw. dem daraus folgenden Vorabentscheidungsverfahren.

(a) (Schutzbereichs-)Parallelität von Art. 7 und 8 EU-GRC und Eingriffskomplex

Bei dieser Entscheidung war zunächst bemerkenswert, dass der EuGH die Möglichkeit eines Eingriffs hinsichtlich Art. 7 und 8 EU-GRC separat prüfte. Bislang hatte der Gerichtshof nicht zwischen diesen Grundrechten differenziert, sondern diese als Einheit geprüft (s.o.).[384] Nun stellte er klar, dass die Pflicht der Telekommunikationsanbieter, Verkehrsdaten universell zu speichern sowohl in den Schutzbereich des Art. 7 EU-GRC[385] als auch in jenen des Art. 8 EU-GRC[386] eingreife.

Darüber hinaus trennte er nicht nur zwischen den Schutzbereichen von Art. 7 und 8 EU-GRC, sondern auch zwischen den verschiedenen Datenverarbeitungsschritten, zu denen die Richtlinie verpflichtete.[387] Der EuGH erkannte, dass sowohl die verpflichtende Speicherung der Verkehrsdaten als auch deren Abruf durch die Sicherheitsbehörden jeweils einen eigenständigen Eingriff darstellten, die allerdings als Einheit geprüft werden müssten, da sich die Intensität der einzelnen Eingriffe nur aus der Gesamtschau ergebe.[388] Das Urteil zur Vorratsdatenspeicherung bringt damit das oben beschriebene Verständnis von Massenüberwachungsmaßnahmen zum Aus-

384 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435; Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52; Urteil v. 09.01.2008, C–275/06 (Promusicae/Telefónica), Rn. 64; dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 203 ff.; *González Fuster,* Data Protection, 2013, S. 234 ff.; *J. Kokott/Sobotta*, Int. Data Privacy Law 3 (2013), 222; *Gellert/Gutwirth*, Computer Law & Security Review 29 (2013), 522 (524 ff.); *W. Michl*, DuD 2017, 349; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.

385 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 38 ff. = NJW 2014, 2169.

386 Idem, Rn. 36.

387 Idem, Rn. 34 ff.

388 Idem, Rn. 54 ff.

druck, deren grundrechtliche Sensibilität sich daraus ergibt, dass mehrere aufeinander abgestimmte Datenverarbeitungsschritte kombiniert werden (s. o. Kap. B. I. 1. c.).

Im Ausgangspunkt stellte der EuGH also fest, dass die Richtlinie zwei Eingriffe umfasste, die jeweils zwei Grundrechte betrafen, wobei die Eingriffe nicht als Einheit,[389] sondern korrekterweise als Komplex behandelt wurden. Entsprechend wäre eine separate und umfassende Prüfung von Art. 7 sowie Art. 8 EU-GRC „der Reihe nach"[390] zu erwarten gewesen.

Eine solche Trennung der Grundrechte fand sich im Rahmen der Rechtfertigungsebene allerdings nur in der (Vorab-)Prüfung des unantastbaren Wesensgehalts der beiden Grundrechte i. S. d. Art. 52 Abs. 1 EU-GRC.[391] Für die Verhältnismäßigkeit spielte diese Parallelität[392] dann plötzlich keine Rolle mehr. Dort war nur noch von einem (einheitlichen) *Eingriff in die Rechte des Art. 7, 8 EU-GRC* die Rede.[393] Im Rahmen der Verhältnismäßigkeit scheint der EuGH demnach weiterhin von einer möglichen Kombination[394] der Grundrechte aus Art. 7 und 8 EU-GRC auszugehen.

### (b) Verhältnismäßigkeit: Normenklarheit als Erforderlichkeitsgewährleistung

Bei der Prüfung stand die Verhältnismäßigkeit im Fokus, also die Frage, ob der Eingriffskomplex der Vorratsdatenspeicherung für die in der Richtlinie genannten Ziele geeignet, erforderlich und angemessen war.[395] An der Eignung zweifelte der EuGH nicht. Auch eine vorratsmäßige Speicherung nur

389 *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139).

390 Vgl. zur entsprechenden Methodik im GG *Dreier* in Dreier GG, Vorb. Art. 1 Rn. 155; *Stern,* StaatsR Bd. III/2, 1994, S. 1366 ff.

391 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 39 ff. = NJW 2014, 2169.

392 *Jarass* in Jarass EU-GRC, Art. 8 Rn. 4; *Johlen* in Stern/Sachs EU-GRC, Art. 28 Rn. 24, Fn 51.

393 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 45 ff., angedeutet schon in der Überschrift von Rn. 38 ff. "Rechtfertigung des Eingriffs" = NJW 2014, 2169.

394 *Marsch,* Datenschutzgrundrecht, 2018, S. 217 ff.; *W. Michl*, DuD 2017, 349 (353); allg zu Grundrechtskombinationen *Breckwoldt,* Grundrechtskombinationen, 2014; Spielmann*,* Konkurrenz, 2008, S. 190 ff.; *Heß,* Grundrechtskonkurrenzen, 2000, S. 84 f.

395 Der EuGH nimmt traditionell eine (manchmal unsystematische) dreiteilige Verhältnismäßigkeitsprüfung vor, da das (legitime)Gemeinwohlziel eigenständig in Art. 52

bestimmter Daten – hier TK-Verkehrsdaten – sei prinzipiell nützlich für strafrechtliche Ermittlungen.[396]

Die Erforderlichkeit hingegen zweifelte der EuGH an. Dabei stellte er zunächst fest, dass man aus der Dringlichkeit des Ziels der Richtlinie nicht automatisch auf deren Erforderlichkeit schließen könne. Die Erforderlichkeit i. S. d. Art. 52 Abs. 1 S. 2 EU-GRC verlange vielmehr, dass nur solche grundrechtsbeschränkenden Maßnahmen erlassen werden, die zur Förderung des Ziels *absolut notwendig* sind.

Dies erfordere zunächst, dass die Tragweite der Maßnahme durch *klare und präzise Regeln* bestimmt wird, *sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen*.[397] Der Gerichtshof versteht insofern das, was in Deutschland als Bestimmtheitsgrundsatz bekannt ist, als Teil der Erforderlichkeit.[398] Das ergibt insofern Sinn, als nur durch eine ausreichende Normenklarheit eine Überwachungsermächtigung auf das *absolut Notwendige* beschränkt werden kann. Analog zu dieser Idee verhält sich die frühe Rechtsprechung des BVerfG zu Überwachungsmaßnahmen, in der die Notwendigkeit von Eingriffsschwellen noch aus dem Bestimmtheitsgrundsatz abgeleitet wurde.[399]

Die entscheidenden Ausführungen des EuGH verstehen sich also als Erforderlichkeits- und damit als Teil der europarechtlichen Verhältnismäßigkeitsprüfung.[400] Der Generalanwalt hingegen hatte die Anforderungen an die Ausgestaltung der Zugriffsregeln zur Einhegung der Eingriffsintensität als Problem der „Gesetzesqualität" i. S. d. Art. 52 Abs. 1 EU-GRC diskutiert.[401]

---

Abs. 1 EU-GRC genannt wird, vgl. *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC, Rn. 52 Rn. 35 ff.; *Pache* in Frankfurter Kommentar, EU-GRC Art. 52 Rn. 24.

396 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 49 = NJW 2014, 2169.

397 Idem, Rn. 54.

398 *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC Art. 52 Rn. 31.

399 BVerfGE 110, 33 (55 ff.) – Außenwirtschaftsgesetz.

400 Vgl. *Granger/Irion*, Eur. Law Rev. 2014, 834 (841 f.); *Tracol*, Computer Law & Security Review 30 (2014), 736 (742).

401 *Generalanwalt Villalón*, Schlussantrag v. 12.12.2013, C-293/12, Rn. 108 ff. – Digital Right Ireland.

Das Vorgehen des EuGH entspricht inhaltlich jenem des BVerfG. Zwar liegt der Fokus anders als beim BVerfG[402] nicht ausdrücklich auf der Angemessenheit, sondern der Erforderlichkeit. Schon hier werden jedoch abwägende Elemente eingebaut, sofern die Intensität der Maßnahme mit den vorgesehenen Zugriffseinschränkungen abgeglichen wird. Die Prüfung vermengt also Aspekte von Erforderlichkeit und Angemessenheit, wie sie in der deutschen Grundrechtslehre verstanden würde.[403]

### (c) Intensitätsbestimmung

Der EuGH beginnt damit, intensivierende Aspekte der Vorratsdatenspeicherung hervorzuheben, wobei er sich in bemerkenswerter Weise an der Rechtsprechung des EGMR orientiert und diesen immer wieder zitiert.[404]

Schon zu Abschluss der Eingriffsdarstellung hatte der EuGH festgestellt, dass die heimliche Aufbewahrung der Verkehrsdaten geeignet ist, bei den Betroffenen ein Gefühl ständiger Überwachung auszulösen und schon deshalb besonders schwer wiege.[405] Wie auch das BVerfG[406] (s. o.) berücksichtigt der EuGH also Einschüchterungseffekte, die weniger auf der konkreten Speicherung beruhen als auf der abstrakten Gesetzesexistenz bzw. dem Wissen der Grundrechtsträger um die gesetzliche Obliegenheit der Speicherung. Was der EuGH dabei nicht bespricht, ist die Tatsache, dass eine gesetzlich obligatorische Speicherung jedenfalls diesen Teil der Überwachung gerade nicht zu einem heimlichen macht.[407] Soweit die Ein-

402 Vgl. BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; NJW 2022, 1583 (1585 Rn. 152 ff.) – Bayerisches Verfassungsschutzgesetz; dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 39.

403 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 52 Rn. 69.

404 Insbesondere EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich) = EuGRZ 2009, 299; zur Bezugnahme auf den EGMR durch den EuGH in *Digital Rights Ireland*: *Grabenwarter* in Stumpf/Kainer/Baldus (Hrsg.), Privatrecht Wirtschaftsrecht Verfassungsrecht, 2015, S. 1386 (1392 f.); *Boehm/Cole* ZD 2014, 553; s.a. *Boehm/Andrees*, CR 2016, 146.

405 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 37 = NJW 2014, 2169.

406 BVerfGE 65, 1 (43) – Volkszählung; E 120, 378 (402) – Autom. Kennzeichenkontrolle I; E 125, 260 (332) – Vorratsdatenspeicherung; krit. hierzu *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011; *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915 (918 f.); Nachweise zur Rspr. und Übersicht zur Kritik bei *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 f.

407 *Schluckebier* abw. Meinung BVerfGE 125, 260 (366).

schüchterungseffekte mit der Heimlichkeit begründet werden, kann korrekterweise also nur auf die jederzeitige Zugriffsmöglichkeit abgestellt werden. Wie auch das BVerfG lässt der Gerichtshof eine tiefergehende Auseinandersetzung mit den empirischen[408] und theoretischen Schwächen der auf den Einschüchterungseffekten aufbauenden Argumentation vermissen.

Ebenfalls knapp wendet sich der EuGH dem Ausmaß des Grundrechtseingriffs zu. Er stellt fest, dass die Speicherung sämtlicher Verkehrsdaten verschiedenster technischer Kommunikationsgeräte aufgrund deren weiteren Verbreitung im Alltag letztlich einen Eingriff in die Grundrechte der gesamten europäischen Bevölkerung darstellt.[409] Der EuGH zieht die Menge der Grundrechtsbetroffenen also in die Intensitätsbestimmung mit ein.

Dabei ergibt sich aus den Ausführungen, dass der EuGH, ganz ähnlich dem BVerfG, die große Menge der Grundrechtsbetroffenen mit der damit natürlicherweise einhergehenden Anlasslosigkeit in Verbindung bringt. Aufgrund der Universalität der Speicherung würden auch Daten von Personen zur später eventuellen Nutzung durch die Sicherheitsbehörden verarbeitet, die im Moment der Speicherung überhaupt keinen Anlass zur Strafverfolgung gegeben hätten.[410] So wäre es etwa denkbar gewesen, die Speicherung nur auf bestimmte Personenkreise, Zeiten oder Orte zu beschränken, bei denen eine erhöhte Wahrscheinlichkeit gegeben wäre, auch solche Daten zu speichern, die später tatsächlich notwendig würden.[411]

### (d) Ergebnis und Zusammenfassung

Aufgrund der geringen Regelungsdichte der Richtlinie befand der EuGH somit letztlich, dass der Eingriff in die Privatheitsgrundrechte nicht auf das Notwendige beschränkt sei, und erklärte die Richtlinie für primärrechtswidrig und nichtig.

Anders als das BVerfG, das den Grad der Regelungsdichte aus der Angemessenheit heraus entwickelt, stützt sich der EuGH auf die Erforderlichkeit, ausgeprägt durch den Bestimmtheitsgrundsatz. Im Ergebnis beurteilt aber auch der Gerichtshof die Grundrechtskonformität nach dem Effekti-

408 Zu diesen insbesondere *Rath* in *Kritische Justiz* (Hrsg.), 60 Jahre GG, 2009, S. 65.
409 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169.
410 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 58 = NJW 2014, 2169.
411 Idem, Rn. 59.

vitätsgrad der Überwachungsmaßnahme. Methodisch scheint dieser Weg überzeugend, da sich die Erforderlichkeitsprüfung als Standort für Effektivitätsfragen durchaus aufdrängt. Das Vorgehen des BVerfG entspricht jedoch dessen mittlerweile eingeübten Priorisierung der Angemessenheit.[412]

Für die Speicherpflicht verlangte der Gerichtshof insofern eine Beschränkung *auf einen bestimmten Zeitraum und/oder ein bestimmtes geografisches Gebiet und/oder einen bestimmten Personenkreis, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, bzw. auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.*[413] Die Speicherpflicht dürfe zudem nicht auf ein Minimum von sechs und Maximum von 24 Monaten festgelegt werden.[414]

Weiter verlangte der EuGH eine Beschränkung des Zugriffs auf das absolut Notwendige in materieller und formeller Hinsicht. Die entsprechenden Vorschriften müssten voraussetzen, dass auf die betroffenen Daten nur zugegriffen werden dürfe, wenn dies die Verhütung, Feststellung oder strafrechtliche Verfolgung genau abgegrenzter Straftaten (tatsächlich) bezwecke.[415] Außerdem verlangte er, dass der Zugriff nur auf Antrag zulässig sein solle, der einer unabhängigen Vorabkontrolle unterzogen wurde.[416]

Letztlich formulierte der EuGH spezifische Anforderungen an die Datensicherheit und -transparenz, wobei er jedoch den Diensteanbietern einen gewissen Spielraum beließ.[417]

Mit der Entscheidung hat sich der EuGH dennoch als entscheidende Stelle bei der Bewertung sicherheitsrechtlicher Überwachungsmaßnahmen, ja als aktives Grundrechtsgericht überhaupt etabliert.[418] Das Vorgehen gleicht jenem des BVerfG darin, dass aus denselben Intensitätsmaßstäben

412 dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 39.

413 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 59 = NJW 2014, 2169.

414 Idem, Rn. 63 f.

415 Idem, Rn. 61 f.

416 Idem, Rn. 62.

417 Idem, Rn. 66 ff.

418 *Kühling*, NVwZ 2014, 681 (684 f.); *Granger/Irion*, Eur. Law Rev. 2014, 834 (844 ff.); *Wendel,* Wider die Mär vom Grundrechtsblinden, 09.04.2014, https://verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/, zuletzt aufgerufen am 12.01.2025; *Prantl* – Ende der Maßlosigkeit SZ vom 08.04.2014, https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057, zuletzt aufgerufen am 12.01.2025.

letztlich Anforderungen an die Regelungsdichte abgeleitet werden, deren Zweck eine möglichst effektive Massenüberwachung darstellt. Es soll also mit möglichst wenigen und geringen Eingriffen ein relatives Maximum an Sicherheitsgewährleistung erzielt werden. Dies kann nur durch materielle Eingriffsschwellen und Verfahrens- sowie Datenschutzvorschriften erzielt werden.

bb. Unionsrechtswidrigkeit nationaler Vorratsdatenspeicherung

Mit der Nichtigkeitserklärung der VDS-RL durch *Digital Rights Ireland* war die Rechtsprechung des EuGH zur anlasslosen Speicherung von TK-Verkehrsdaten aber nicht am Ende. Sie nahm hierdurch erst ihren Anfang.

In den verschiedenen Mitgliedstaaten wurde unterschiedlich auf das Urteil des EuGH reagiert.[419] Weitgehende Einigkeit bestand – auch in der Literatur – dahingehend, dass aufgrund der spezifischen Regelung in Art. 15 Abs. 1 S. 2 e-Privacy-RL ein Anwendungsfeld des EU-Rechts, jedenfalls im Sinne der Rechtsprechung des EuGH[420], vorliegt und nationale Regelungen folglich mit den Anforderungen der Art. 7, 8 EU-GRC in der Auslegung des Gerichtshofs in Einklang stehen müssten.[421]

Nur einige Mitgliedstaaten änderten ihre bestehenden Regelungen aber proaktiv ab. Andere bestanden darauf, die Anwendung der vom EuGH postulierten Grundsätze durch die nationalen Gerichte abzuwarten. Drittens gab es auch noch eine Gruppe an Mitgliedstaaten, darunter die Bundesrepublik Deutschland, die das Urteil als Anlass nahmen, von der Implementation einer vorratsmäßigen Verkehrsdatenspeicherung erst einmal ganz abzusehen.[422]

419 Übersichtlich *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (268 ff.); *Vainio/Miettinen*, Int. J. of Law and Information Technology 23 (2015), 290 (299 ff.).

420 EuGH Urt. v. 26.2.2013, C-617/10 (Åkerberg Fransson), Rn. 17 ff. =NVwZ 2013, 561; Urt. v. 10.7.2014, C-198/13 (Hernández), Rn. 41 = EuZW 2014, 795; dazu *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 51 Rn. 8 ff.; *Hancox*, Common Market Law Rev. 50 (2013), 1411.

421 *Boehm/Cole*, ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267); aA. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); für eine selbstständige Primärrechtswidrigkeit des Art. 15 Abs. 1 S. 2 e-Privacy-RL: *Sandhu*, EuR 2017, 453 (462 ff.).

422 *Roßnagel*, NJW 2016, 533 (534 f.).

Diese unterschiedlichen Reaktionen basierten auf der Unklarheit[423], ob durch *Digital Rights Ireland* die anlasslose Vorratsdatenspeicherung generell unzulässig[424] oder nur von der konkreten Ausgestaltung insbesondere der Zugriffsregelungen abhängig geworden war.[425]

(1) *Tele2Sverige/Watson*: Keine nationale Vorratsdatenspeicherung zur Verbrechensbekämpfung.

Diese Fragen hatte der EuGH im Urteil *Tele2Sverige/Watson*[426] erstmals zu beantworten, in dem er zusammengefasst über Vorabentscheidungsvorlagen aus Schweden und dem Vereinigten Königreich entschied. Beide (damals noch) Mitgliedstaaten hatten nach der Nichtigkeitserklärung der VDS-RL weiterhin Normen implementiert, die eine Vorratsdatenspeicherung von TK-Verkehrsdaten vorsahen. Das britische Modell unterschied sich vom schwedischen jedoch insoweit, dass im Vereinigten Königreich keine generelle Pflicht zur Speicherung bestand, sondern eine solche gegenüber einzelnen Betreibern vom Innenministerium erst angeordnet werden musste und mit verschiedenen Einschränkungen versehen werden konnte.[427]

Hinsichtlich des schwedischen Rechts stand also die Frage im Raum, ob eine gesetzlich universelle Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten – in diesem Falle erneut für mindestens sechs Monate – durch nationale Gesetzgebung mit Europäischem Recht vereinbar war. Insofern entsprach die Ausgangslage hinsichtlich des schwedischen Verfahrens ganz jener aus dem Urteil *Digital Rights Ireland*.

423 Vgl. GA *Saugmandsgaard Øe*, Schlussantrag v. 16.07.2016, C-203/15,C-698/15 (Tele2Sverige/Watson ua.), Rn. 192 ff.

424 *Leutheusser-Schnarrenberger*, DuD 2014, 589 (592); ähnlich *Nachbaur*, ZRP 2015, 215 (216).

425 etwa England and Wales Court of Appeal, 20.11.2015 (Secretary of State for the Home Department v Davis MP c Ors) [2015] EWCA Civ 1185, Rn. 48 mit Verweis auf das Instanzgericht.; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); zuvor schon BVerfGE 125, 260 (347 ff.) – Vorratsdatenspeicherung.

426 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717.

427 Idem, Rn. 15 ff. (schwedisches Recht), Rn. 29 ff. (Recht des Vereinigten Königreichs); übersichtlich *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (268 ff.).

(a) Geltung der Art. 15 Abs. 1 e-Privacy-RL und Art. 7, 8 EU-GRC für nationale Vorratsdatenspeicherungsregime?

Dabei stellte der EuGH zunächst fest, dass solche nationalen Regelungen den Anwendungsbereich des Unionsrechts i. S. d. Art. 51 Abs. 1 EU-GRC betrafen, da die Einführung sicherheitsrechtlicher Vorratsdatenspeicherung als Einschränkung der sich aus Art. 5 e-privacy-RL ergebenden Rechte in Art. 15 Abs. 1 S. 1, 2 e-Privacy-RL spezifisch determiniert wurde.[428] Dass Art. 1 Abs. 3 e-Privacy-RL *Tätigkeiten im Bereich der öffentlichen Sicherheit und der Strafverfolgung* vom Anwendungsbereich dieser Richtlinie generell ausnahm, stand mit diesem Ergebnis zwar auf den ersten Blick im Widerspruch. Dieses Spannungsverhältnis[429] zwischen Art. 15 Abs. 1 S. 1, 2 und Art. 1 Abs. 3 e-Privacy-RL löste der EuGH aber auf, indem er Art. 1 Abs. 3 e-Privacy-RL eng auslegte und damit nur solche sicherheitsrechtlichen Datenverarbeitungen vom Anwendungsbereich ausnahm, die unmittelbar durch die zuständigen (Sicherheits-)Behörden erfolgten. Andernfalls käme Art. 15 Abs. 1 S. 1, 2 e-Privacy-RL kein Anwendungsbereich mehr zu.[430]

Es oblag dem EuGH daher zu entscheiden, inwieweit Art. 15 Abs. 1 S. 2 e-Privacy-RL der nationalstaatlichen Einführung einer TK-Vorratsdatenspeicherung entgegensteht. Die Norm selbst bleibt insofern vage. Art. 15 Abs. 1 S. 1 e-Privacy-RL statuiert lediglich einen Verhältnismäßigkeitsvorbehalt von sicherheitsrechtlichen Eingriffen in die von der Richtlinie garantierten Rechte, also der Vertraulichkeit elektronischer Kommunikation. Art. 15 Abs. 1 S. 2 e-Privacy-RL nennt als Beispiel für einen solchen Eingriff, *dass Daten während einer begrenzten Zeit aufbewahrt werden*.

Um konkrete Anforderungen an die Verhältnismäßigkeit von Vorratsdatenspeicherungsregimen herauszuarbeiten, bemühte der EuGH eine Auslegung des Art. 15 Abs. 1 S. 1 e-Privacy-RL im Lichte der Art. 7, 8 EU-GRC. Nationalstaatliche Eingriffe in die Telekommunikationsvertraulichkeit wären danach von Art. 15 Abs. 1 S. 2 e-Privacy-RL untersagt, soweit sie unverhältnismäßig in Art. 7, 8 EU-GRC eingriffen. Ausgangspunkt dieser Prüfung waren wiederum die Maßstäbe, die der Gerichtshof in *Digital Right Ireland* aufgestellt hatte.

428 *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); dazu auch *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2080 f.).

429 *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

430 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; s.a. *Boehm/Cole* ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267).

(b) Verhältnismäßigkeitsprüfung

Die Intensitätsfestlegung begann der EuGH in der Folge aber nicht mehr mit der Hervorhebung der Streubreite und Anlasslosigkeit, sondern stellte die Sensibilität von Verkehrsdaten heraus.[431] Die Speicherung solcher Daten sei schon deshalb ein besonders schwerwiegender Eingriff.[432]

Als mögliche Rechtfertigung dieses Eingriffs komme nur die Bekämpfung schwerer Straftaten in Betracht. Hierfür aber sei eine universelle Speicherpflicht nicht erforderlich, da sie das *absolut Notwendige* überschreite. Es würden zu viele Daten erhoben, die sich aufgrund der Anlasslosigkeit letztlich als für das Maßnahmenziel völlig unbrauchbar erwiesen .[433]

Der EuGH elaborierte ausführlich, dass Speicherpflichten, die auf der Grundlage spezifischer Erkenntnisse zeitlich und örtlich begrenzt seien, ebenso geeignet seien.[434] Unabhängig von den Zugriffsrechten komme eine universelle Pflicht der Telekommunikationsdienstleister zur Vorhaltung von TK-Verkehrsdaten also nicht in Betracht.

Damit war die erste Frage des Oberverwaltungsgerichts Stockholm beantwortet und die Diskussion um die Möglichkeit allgemeiner Vorratsdatenspeicherungen bei ausreichender Limitierung der Zugriffsmöglichkeiten (eigentlich) entschieden (dazu gleich unten).

Der EuGH widmete sich nun den Fragen aus Schweden und dem Vereinigten Königreich hinsichtlich der Ausgestaltung der Zugriffsregeln. Wie bereits dargelegt unterfielen auch diese dem Anwendungsbereich des EU-Rechts i. S. d. Art. 51 Abs. 1 EU-GRC, da der Gerichtshof die Vorratsdatenspeicherung zu Recht als Maßnahmenkomplex begreift und Art. 15 Abs. 1 e-Privacy-RL deshalb dahingehend auslegt, dass dieser auch die Zugriffsebene reglementiert.[435]

Auch für die Zugriffsregeln müssten die Mitgliedstaaten sicherstellen, dass sie verhältnismäßig sind, was wiederum nur dann möglich sei, wenn sie der Bekämpfung schwerer Kriminalität dienten und insofern erforderlich seien.[436] Der EuGH begrenzte also nicht nur selbstständig die Spei-

431 Dazu *Brkan*, German Law Journal 20 (2019), 864 (872 f.).
432 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717.
433 Idem, Rn. 106.
434 Idem, Rn. 108 ff.
435 Idem, Rn. 118; aA. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).
436 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 113 ff. = NJW 2017, 717.

cherpflichten, sondern auch den Zugriff, da Speicherung und Zugriff nur zusammengedacht werden können.[437] Er erteilte somit der Überlegung, dass eine allgemeine Speicherpflicht verhältnismäßig sein könnte, wenn nur der Zugriff ausreichend limitiert würde, eine recht deutliche Absage.[438]

Die materiellen Anforderungen an die Zugriffsregeln konkretisierte der EuGH noch etwas näher und schuf insbesondere eine neue Ausnahmekonstellation. Die Mitgliedstaaten müssten den Zugang zu vorratsmäßig gespeicherten Daten grundsätzlich auf solche Fälle beschränken, in denen bei der betroffenen Person ein Verdacht auf die Begehung einer schweren Straftat vorliegt. Abweichungen hiervon seien nur denkbar, wenn sich der Mitgliedstaat in einer Situation befindet, in der *vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind*.[439]

In formeller Hinsicht forderte der EuGH weiterhin, dass der Zugriff auf Vorratsdaten nur auf Antrag zulässig sein sollte, der vorab einer unabhängigen Prüfung durch eine Kontrollstelle unterzogen wurde.[440] Insofern ergab sich aus dem Urteil gegenüber der vorherigen Rechtsprechung nichts Neues. Dasselbe lässt sich über die abermals formulierten Anforderungen an die Datensicherheit und -transparenz sagen.[441]

(2) *La Quadrature du Net*: Ein Schritt zurück?

Die Hauptleistung von *Tele2Sverige/Watson* wurde überwiegend in der Übertragung der Rechtsprechung aus *Digital Rights Ireland* auf die nationalen Regeln erblickt, da die Unterschiede zu diesem Urteil in der Sache bei

437 *Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (4).

438 Vgl. *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (8 ff.); *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (142 f.); *Roßnagel*, NJW 2017, 696 (697 ff.); *Priebe*, EuZW 2017, 136-130 (138).

439 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

440 Idem, Rn. 120 mit Verweis auf EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 62 = NJW 2014, 2169.

441 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 122 f. = NJW 2017, 717 mit Verweis auf Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 66 ff. = NJW 2014, 2169.

einer strengen Lesart eher gering ausfielen.[442] Jedenfalls bestand nun kein Zweifel mehr daran, dass universelle TK-Vorratsdatenspeicherungspflichten kaum mit den Unionsgrundrechten vereinbart werden konnten und laxe Zugriffsregelungen ohnehin nicht.

In den darauffolgenden Entscheidungen und deren Umsetzung durch nationale Gerichte sollte jedoch vor allem der in *Tele2Sverige/Watson* erstmals formulierten Ausnahmeregelung für besondere Bedrohungssituationen Bedeutung zukommen. Diese wurde in dem Urteil *La Quadrature du Net (ua.)* über die französischen und belgischen Regeln zur retrograden und zukunftsgerichteten Vorratsdatenspeicherung noch weiter ausdifferenziert.[443] Der EuGH bewegte sich damit weg vom absoluten Verbot der Vorratsdatenspeicherung und hin zu einer detaillierten *Prozeduralisierung*[444] im Sinne einer rechtsfortbildenden Verhältnismäßigkeitsprüfung.[445]

(a) Geltung der e-Privacy-RL bei Tätigkeit für Nachrichtendienste?

Anders als in den vorherigen Urteilen richteten sich die in *La Quadrature du Net* besprochenen Überwachungsmaßnahmen allerdings nicht auf die Strafverfolgung, sondern etablierten Datenverarbeitungspflichten der Telekommunikationsdienstleister für die Nachrichtendienste. Sowohl das französische als auch das belgische Recht sahen weiterhin vor, dass TK-Provider zur universellen Speicherung von Verkehrsdaten verpflichtet werden konnten, die dann u. a. den Nachrichtendiensten zur Verfügung gestellt werden mussten. Das französische Recht enthielt darüber hinaus die Ermächtigung der Nachrichtendienste, sich von den Anbietern spezifische Verkehrsdaten in Echtzeit übermitteln zu lassen. Außerdem wurden die Anbieter verpflichtet, ihre gespeicherten Daten mittels Datenanalyse nach

442 *Kipker/Schefferski/Stelter* ZD 2017, 124 (131 f.); vgl. auch *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (99 f.); s.a. die Nachweise zu (teils sehr) krit. Reaktionen bei *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (12).

443 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

444 *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.); s.a. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (104 ff.).

445 Vgl. (zum BVerfG) *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

terrorismusverdächtigen Verbindungen zu durchsuchen und Treffer an die Nachrichtendienste zu übermitteln.[446]

Der sicherheitsrechtliche Zweck wurde zur Grundlage genommen, um abermals den Anwendungsbereich des Unionsrechts anzuzweifeln.[447] Ausgangspunkt hierfür war Art. 4 Abs. 2 S. 3 EUV, wonach die *nationale Sicherheit*, unter die insbesondere das Recht der Nachrichtendienste fällt[448], im alleinigen Verantwortungsbereich der Mitgliedstaaten verbleiben soll.

Der EuGH räumte diese Bedenken aus, indem er abermals eine Unterscheidung zwischen unmittelbar staatlicher Datenverarbeitung bzw. Überwachungstätigkeit und der entsprechenden Inpflichtnahme Privater vornahm.[449] Wie schon hinsichtlich des Spannungsverhältnisses zu Art. 1 Abs. 3 e-Privacy-RL[450] bemerkte er, dass Art. 15 Abs. 1 e-Privacy-RL zwangsläufig eine unionsrechtliche Determination für das Sicherheitsrecht herbeiführe. Es entspreche der gefestigten Rechtsprechung des Gerichtshofs, dass eine nationale Maßnahme nicht schon deshalb aus dem Anwendungsbereich des Unionsrechts falle, weil sie der nationalen Sicherheit diene.[451] Wie auch Art. 1 Abs. 3 e-Privacy-RL legte der EuGH also Art. 4 Abs. 2 S. 3 EUV letztlich eng aus und begrenzte dessen Zuständigkeitsabgrenzung auf staatliche Maßnahmen, an denen keine Private beteiligt sind.[452] Dazu verwies er insbesondere auch auf den mittlerweile in Kraft getretenen Art. 23 Abs. 1 lit. d) DSGVO, aus dem sich ebenfalls ergebe, dass private Datenverarbeitungen im Rahmen staatlicher Sicherheitsinteressen dem europäischen Datenschutz unterlägen.[453]

---

446 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 31 ff. = NJW 2021, 531.

447 Idem, Rn. 89; Vgl. *Sandhu*, EuZW 2021, 209 (221); GA *Campos Sánchez-Bordona*, Schlussantrag v. 15.01.2020, C-511/18, C-512/18 (la Qudadrature du Net ua.), Rn. 77 ff.

448 *Sule* in Dietrich/Sule (Hrsg.), Intelligence Europe, 2019, Chapt. 2 Rn. 19 ff.; s.a. *Cameron*, Int. J. of Intelligence and CounterIntelligence 33 (2020), 452 (454 ff.); *Karpenstein/Sangi*, GSZ 2020, 162 (167).

449 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 91 ff. = NJW 2021, 531.

450 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 99 = NJW 2017, 717; krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

451 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 91 ff. = NJW 2021, 531.

452 Ebenso, GA *Campos Sánchez-Bordona*, Schlussantrag v. 15.01.2020, C-511/18, C-512/18 (la Qudadrature du Net ua.) Rn. 77 ff.; dazu krit. *Cameron*, Int. J. of Intelligence and CounterIntelligence 33 (2020), 452 (459).

453 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 102 = NJW 2021, 531.

(b) Ausnahme vom Verbot der Vorratsdatenspeicherung in nationalen Bedrohungssituationen

Abermals stand daher infrage, ob die zu prüfenden nationalstaatlichen Regelungen nach Art. 15 Abs. 1 e-Privacy-RL, ausgelegt im Lichte der Art. 7, 8 EU-GRC, zulässig waren.

Einen bedeutenden Unterschied zu den vorher entschiedenen Fällen zur Vorratsdatenspeicherung erkannte der EuGH hier in der Zielsetzung von Vorratsdatenspeicherungsregimen, die der *nationalen Sicherheit* i. S. d. Art. 4 Abs. 2 EUV dienen. Diese gehe über die konkreteren in Art. 15 Abs. 1 e-Privacy-RL genannten Sicherheitszwecke, wie etwa der Bekämpfung von (auch schwerer) Kriminalität, hinaus.[454] Wie auch das BVerfG[455] geht der EuGH also von einer abstrakteren, gesamtheitlichen Sicherheitsgewährleistung der Nachrichtendienste aus, die den Staat in seiner Integrität schützt[456] und intendiert damit – ebenfalls gleich dem BVerfG–, dass für Überwachungsmaßnahmen zum Schutz der nationalen Sicherheit i. S. d. Art. 4 Abs. 2 EUV geringere Anforderungen gelten, wenngleich das BVerfG stets daran erinnert, dass sich die erweiterten Vorfeldbefugnisse der Nachrichtendienste nur rechtfertigen lassen, weil ihnen operative Möglichkeiten fehlen.[457] Dies ist in anderen EU-Ländern nicht zwingend der Fall.

Auch in formal-methodischer Hinsicht schlägt das Urteil eine etwas andere Richtung ein. Stand bei *Digital Rights Ireland* und *Tele2Sverige/Watson* noch der Grundsatz der Erforderlichkeit im Sinne *absoluter Notwendigkeit* im Vordergrund, erklärte der EuGH nunmehr, dass die schwere Beeinträchtigung der Art. 7, 8 EU-GRC zu den verfolgten Sicherheitsinteressen der Bevölkerung, wie sie in verschiedenen Rechten zum Ausdruck kommen[458], in einem *strikt angemessenen Verhältnis* stehen müsse. Neben der Beschränkung auf das absolut Notwendige müsse *darüber hinaus auch eine ausge-*

454 Idem, Rn. 136 f.

455 Vgl. BVerfGE 156, 11 (51 f.) – Antiterrordatei II; E 133, 277 (325 f.) – Antiterrordatei I; *Poscher/Rusteberg* KJ 2014, 57 (62 f.).

456 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 135 f. = NJW 2021, 531; so schon ausf. *Sule* in Dietrich/Sule (Hrsg.), Intelligence Europe, 2019, Chapt. 2 Rn. 19 ff., insbesondere Rn. 69 ff.

457 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.);, NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gusy*, GA 1999, 319 (327) *Gärditz*, JZ 2013, 633 (634); *Gusy*, GA 1999, 319 (327).

458 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 123 ff. = NJW 2021, 531.

*wogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen werden.*[459]

Im Ergebnis wirkte sich die Neuausrichtung auf den Angemessenheitsaspekt nicht aus. Weiterhin nutzte der EuGH die Verhältnismäßigkeitsprüfung dazu, die Effektivität[460] der Überwachung (dazu oben) zu gewährleisten, indem die Zulässigkeit der einzelnen Datenverarbeitungsschritte von bestimmten Anforderungen abhängig gemacht und damit eine Verknüpfung zum verfolgten Zweck hergestellt wurde.[461]

Solch eine ausreichende Verknüpfung zum Schutz der nationalen Sicherheit sah der EuGH grundsätzlich auch bei der Anordnung einer universellen Vorratsdatenspeicherungen gegeben. Anders als im Rahmen der Strafverfolgung oder der Gewährleistung der öffentlichen Sicherheit stünde Art. 15 Abs. 1 e-Privacy-RL hier nicht unbedingt entgegen. Voraussetzung sei jedoch, dass *hinreichend konkrete Umstände die Annahme zuließen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersähe.*[462] Die in solchen Situationen gespeicherten Daten dürften auch automatisch analysiert werden (näher zur Datenanalyse unten II. 2. b. & c.).[463]

Über das Vorliegen einer solchen Bedrohung müsse vorab aber ein Gericht oder eine unabhängige Verwaltungsstelle entscheiden.[464]

Eine solche Ausnahme vom grundsätzlichen Verbot der Vorratsdatenspeicherung bei akuten, die nationale Sicherheit betreffenden Bedrohungslagen hatte der EuGH zwar schon in *Tele2Sverige/Watson* angedeutet.[465]

---

459 Idem, Rn. 129 f. mit Verweis auf EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 55 = NJW 2019, 655.

460 Vgl. zum Effektivitätsaspekt bei der Verhältnismäßigkeit von Überwachungsmaßnahmen *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82 f., 14 ff.; *Stern,* StaatsR Bd. III/2, 1994, S. 836; aus der Rspr etwa BVerfGE 115, 166 (197 f.); insbesondere aber BVerfGE 141, 220 (268 ff.) – BKA-Gesetz.

461 Vgl. *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (148).

462 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

463 Idem, Rn. 178.; s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 176 ff. = EuZW 2022, 706.

464 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 139 = NJW 2021, 531.

465 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

Dass er damit nun ernst machte und mit dieser Möglichkeit das bisher verteidigte absolute Verbot der anlasslosen Vorratsdatenspeicherung von TK-Verkehrsdaten aufweichte, wurde in der Literatur dennoch mit einiger Ernüchterung aufgenommen[466] und teilweise auf politischen Druck der Mitgliedstaaten zurückgeführt.[467]

### (c) Möglichkeiten bei der Kriminalitätsbekämpfung: anlasslose IP-Adressen-Speicherung, „Targeted Retention" und „Quick Freeze"

Was die Ziele der Verhütung und Verfolgung schwerer Straftaten anbelangte, verblieb der EuGH bei seiner bisherigen Einschätzung, dass eine universelle Vorratsdatenspeicherung von TK-Verkehrsdaten nicht angeordnet werden dürfe. Nur die „targeted retention"[468], also eine zielgerichtet persönliche und/oder zeitlich bzw. örtlich begrenzte Anordnung, könnte sich insofern im Rahmen des absolut Notwendigen bewegen. Für diese Feststellung zog er sämtliche in den vorherigen Urteilen aufgestellten Intensitätsparameter heran, stellte also sowohl auf die Datenqualität im Sinne der Möglichkeit eines Profiling als auch auf die Menge der betroffenen Grundrechtsträger und die damit verbundene Anlasslosigkeit ab.[469]

Auch hier differenzierte der EuGH nun aber weiter und schuf erstmals eine Ausnahme von den genannten Grundsätzen für die vorratsmäßige Speicherung der IP-Adressen von Internetnutzern im Rahmen der Bekämpfung schwerer Kriminalität.

Zwar seien auch diese als Verkehrsdaten zu qualifizieren, obwohl sich aus den Adressen lediglich ergebe, welches Endgerät bzw. welcher Nutzer eine Internetkommunikation über den jeweiligen Provider aufgebaut habe. Insofern handele es sich um weniger sensible Daten.[470] Mittelbar ergebe sich aus dieser Zuordnung allerdings die Möglichkeit nachzuvollziehen, welche Internetadressen ein Nutzer aufgebaut hat (etwa, weil die zugreifenden

466 *Ogorek*, NJW 2021, 531 (547): „Pyrrhussieg"; *Sandhu*, EuZW 2021, 209 (222); differenziert *Tzanou/Karyda*, European Public Law 28 (2022), 123.

467 *Zalnieriute*, Modern Law Rev. 85 (2022), 198 (213 ff.).

468 Vgl. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (101); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1449); *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (149).

469 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 140 ff. = NJW 2021, 531.

470 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 152, 157 = NJW 2021, 531.

IP-Adressen von den jeweiligen Servern protokolliert werden[471]). Auch die IP-Adressen könnten demnach zur Erstellung von Persönlichkeitsprofilen verwendet werden.[472]

Da jedoch die Bekämpfung bestimmter, mit dem Internet untrennbar verbundener Kriminalitätsformen, etwa der Kinderpornografie, unmöglich würde, wenn die IP-Adressen nicht gespeichert würden, sah der EuGH eine universelle Vorratsdatenspeicherung als verhältnismäßig an, wenn nur der Zugriff strikt genug ausgestaltet würde.[473]

Ebenfalls äußerte sich der EuGH zur zukunftsgerichteten Verkehrsdatenspeicherung in Echtzeit, dem sogenannten „Quick-Freeze"[474]. Bei Vorliegen bestimmter Anhaltspunkte dürften die Mitgliedstaaten Anordnungen regeln, die den Providern auferlegen, die aktuell vorhandenen und in Zukunft anfallenden Verkehrsdaten einer oder mehrerer Personen zu speichern, wenn dies zur Bekämpfung schwerer Kriminalität oder dem Schutz der nationalen Sicherheit notwendig ist.[475] Betroffen von solch einer Maßnahme dürfe nicht nur der jeweils Verdächtige sein, sondern auch Personen in dessen *sozialem oder beruflichem Umfeld oder in bestimmten geografischen Zonen, etwa an den Orten, wo die fragliche Straftat oder Beeinträchtigung der nationalen Sicherheit begangen oder vorbereitet wurde*.[476]

471 Dazu EuGH, Urteil vom 19.10.2016, C-582/14 (Breyer/Deutschland) = NJW 2016, 3579; zum Unterschied der IP-Abfrage und der Nutzung der IP in Folgeermittlungen vgl. *Kamp/Ebeling* in BeckOK POR NRW, PolG NRW § 20a Rn. 50 ff.; dazu auch BVerfGE 130, 151 (198 f.) – Bestandsdatenauskunft I.

472 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 153 = NJW 2021, 531.

473 Idem, Rn. 155 ff.

474 Dazu *Juszczak/Sason*, eucrim 2021, 238 (247); zur Rechtslage in der StPO: *Rückert* in MüKo StPO, § 100g Rn. 116; mittlerweile liegt allerdings ein Referentenentwurf des *BMJ* vor https://kripoz.de/wp-content/uploads/2022/10/refE-quick-freeze.pdf, zuletzt aufgerufen am 12.01.2025.

475 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 163 ff. = NJW 2021, 531.

476 Idem, Rn. 165.

### (3) *Spacenet/Telekom*: Das (vorläufige) Aus der Vorratsdatenspeicherung in Deutschland

Die Grundsätze des EuGH aus *La Quadrature du Net* wurden jüngst hinsichtlich der deutschen Regelung zur Vorratsdatenspeicherung bestätigt.[477]

Die Bundesrepublik hatte Ende 2015 die Wiedereinführung der Vorratsdatenspeicherung überraschend[478] beschlossen[479] und dabei versucht, die damals vorliegenden Urteile des BVerfG und EuGH umzusetzen.[480] Die Speicherfrist wurde in § 113b a.F. TKG (heute § 176 TKG) auf 10 Wochen beschränkt und die Zugangsmöglichkeiten der Sicherheitsbehörden von hohen Anforderungen abhängig gemacht, § 113c a.F. TKG (heute § 177 TKG), vgl. etwa § 100g Abs. 2 StPO. Es handelte sich aber weiterhin um eine universelle Pflicht der TK-Provider, für die Strafverfolgungs- und Gefahrenabwehrbehörden Verkehrsdaten anlasslos zu speichern. Insofern schlug sich in der deutschen Regelung eine Lesart von *Digital Rights Ireland* nieder, die kein absolutes Verbot der Vorratsdatenspeicherung zur Verhütung und Verfolgung schwerer Kriminalität erkennen wollte (s. o.).[481]

Erwartungsgemäß regte sich denn auch gleich großer Widerstand gegen die deutsche Regelung. Zwar wies das BVerfG sämtliche Eilanträge gegen die neuen Regelungen ab.[482] Aufgrund der Ergänzungen des EuGH in der Sache *Tele2 Sverige* kamen jedoch verschiedene Verwaltungsgerichte zu dem Ergebnis, dass auch die aktuelle Version der Vorratsdatenspeicherung in der Bundesrepublik jedenfalls mit europäischen Grundrechten nicht zu vereinbaren sei.[483] Das BVerwG leitete deshalb ein Vorabentscheidungs-

477 EuGH, Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

478 *Roßnagel*, NJW 2016, 533 (534); zur Genese auch *Oehmichen/Mickler*, NZWiSt 2017, 298 (298 ff.).

479 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218).

480 Dazu krit. *Wissenschaftliche Dienste des Bundestags,* WD 3 - 3000 - 108/15, Vorratsdatenspeicherung, 2015; *Roßnagel*, NJW 2016, 533 (538 ff.); *ders.*, NJW 2017, 696 (697 ff.); *Gercke*, ZUM 2016, 825 (826).

481 Vgl. *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.).

482 BVerfG, ZD 2016, 433; auch noch nach Erlass von *Tele2 Sverige*: BVerfG ZD 2017, 300.

483 OVG Münster, NVwZ-RR 2018, 43; VG Köln, ZD 2019, 187; Übersicht bei *Bär* in BeckOK StPO, § 175 TKG Rn. 15 ff.

verfahren ein.[484] Die Bundesnetzagentur setzte die Speicherpflichten der TK-Diensteanbieter nicht mehr aktiv durch.[485]

Der EuGH bestätigte vorhersehbar[486] die von den Verwaltungsgerichten vertretene Ansicht und erkannte in der deutschen Regelung über die Vorratsdatenspeicherung einen Verstoß gegen Art. 15 Abs. 1 e-Privacy-RL, interpretiert im Lichte der Art. 7, 8 EU-GRC.[487]

### cc. Ausweitung der Rechtsprechung auf sämtliche Verkehrsdatenübermittlungen durch Private

Sämtliche bisher beschriebenen Urteile befassten sich im Kern mit Regelungen, die den Anbietern von Telekommunikationsdiensten selbst die Speicherung von Verkehrs- und Standortdaten auferlegten. Unterschiede bestanden nur dahingehend, dass Daten für verschiedene Behörden und folglich zu unterschiedlichen Zwecken aufbewahrt wurden.

Die Inpflichtnahme Privater war für den EuGH entscheidend, da sich erst daraus die Eröffnung des Anwendungsbereichs des EU-Rechts ergab.[488] Der Gerichtshof machte sich insofern die typische Struktur von Massenüberwachungsmaßnahmen zu eigen, die ohne eine Inpflichtnahme Privater kaum möglich wären und deshalb einen wirtschaftsrechtlichen Einschlag haben.

Die Mitgliedstaaten sahen und sehen diese Rechtsprechung insofern kritisch, als sich der EuGH über diesen Weg ein intensives Mitspracherecht bei der Zulässigkeit nationalstaatlicher Strafverfolgungs-, Gefahrenabwehr- und nachrichtendienstlicher Maßnahmen einräumt. Ein solches Mitspracherecht wähnten die Mitgliedstaaten durch Regelungen wie Art. 4 Abs. 2

484 BVerwG, NVwZ 2020, 1108.

485 *BNetzA,* Mitteilung zu § 113b TKG, 2017, https://web.archive.org/web/20210307231333/https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html , zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im Juli 2021); *Rückert* in MüKo StPO, § 100g Rn. 15.

486 *Roßnagel*, ZD 2022, 650 (651).

487 EuGH, Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 66 ff. = NJW 2022, 3135.

488 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

EUV, Art. 3 Abs. 2 e-Privacy-RL und Art. 2 Abs. 2 lit. d) DSGVO aber gerade ausgeschlossen.[489]

Das stärkste Argument des EuGH dafür, nationale TK-Vorratsdatenspeicherungspflichten dem Anwendungsbereich des EU-Rechts zu unterstellen, war stets, dass Art. 15 Abs. 1 e-Privacy-RL ausdrücklich die Notwendigkeit vorsah, solche Regime verhältnismäßig auszugestalten. Es ist völlig richtig, dass die Norm keinen Sinn mehr hätte, wenn man Art. 3 Abs. 2 e-Privacy-RL weit auslegen und sämtliche sicherheitsrechtlichen Inpflichtnahmen der TK-Provider aus dem Geltungsbereich der Richtlinie herauslösen würde.[490]

Der Gerichtshof beließ es allerdings nicht dabei, allein die Pflichten zur Vorratsdatenspeicherung und sinnvollerweise die damit verwobenen Zugriffsregeln dem Anwendungsbereich des Unionsrechts, insbesondere der Charta nach Art. 51 Abs. 2 EU-GRC, zu unterstellen.

In den beiden bedeutenden Urteilen *Privacy International*[491] und *Prokuratuur*[492] erweiterte er seine Kompetenz dahingehend, dass sämtliche Überwachungsmaßnahmen im Bereich der Telekommunikationsdaten dem Unionsrecht unterfielen, solange die privaten Dienstleister auch nur irgendwie an dem Prozess beteiligt würden.[493] Diese Urteile stehen deshalb beispielhaft für die immer stärkere Europäisierung des Strafverfahrens[494] bzw. des Sicherheitsverfassungsrechts.

### dd. Zusammenfassung und Fazit

Der EuGH hat mit seiner Rechtsprechung in den vergangenen knapp zehn Jahren eine bedeutende sicherheitsrechtliche Überwachungsmaßnahme maßgeblich rechtlich geprägt.

---

489 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 65 ff. = NJW 2017, 717; krit. auch *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, 397 f.; *dies.*, NJW 2021, 2079 (2081); *A. Baumgartner*, GSZ 2021, 36.

490 *Classen*, JZ 2019, 1057 (1062).

491 EuGH, Urteil v. 6.10.2020, C-623/17 (Privacy International), Rn. 30 ff. = GSZ 2021, 36.

492 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 32 ff. = NJW 2021, 2103; s.a. Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 35 ff. = NJW 2019, 655 zu den Bestandsdaten.

493 *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2082).

494 Dazu allg. *Safferling/Rückert*, NJW 2021, 287 (288 ff.).

Die Entscheidungsserie hat dem EuGH aufgrund seiner Positionierung als *Grundrechtsgericht* zwar viel Lob eingebracht[495], allerdings auch erheblichen Widerstand der Mitgliedstaaten hervorgerufen. Kritiker werfen dem Gerichtshof vor, mittels weiter Auslegung der e-Privacy-RL letztlich eine vollständige unionsrechtliche Überformung des nationalen Sicherheitsrechts eingeleitet zu haben. Der Gedanke, dass die nationalen Sicherheitsgesetze aufgrund der Inpflichtnahme Privater Teil des von der Union geprägten Wirtschafts- bzw. in diesem Rahmen geltenden Datenschutzrechts sein sollten[496], machten einige Mitgliedstaaten als reinen Vorwand des EuGH aus und sperrten sich gegen dessen Einmischung im Sicherheitsbereich.[497]

Der Gerichtshof hatte selbst zugegeben, dass die Pflicht zur Vorratsdatenspeicherung mitnichten auf eine Harmonisierung im Interesse der Provider abzielte, sondern ganz primär dem staatlichen Sicherheitsinteresse diente.[498] Entsprechend bleibt der Widerstand gegen die Aktivität des EuGH im Bereich der TK-Verkehrsdaten enorm.[499]

---

495 *Kühling*, NVwZ 2014, 681 (684 f.); *Granger/Irion*, Eur. Law Rev. 2014, 834 (844 ff.); *Wendel,* Wider die Mär vom Grundrechtsblinden, 09.04.2014, https://verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/, zuletzt aufgerufen am 12.01.2025; *Prantl* – Ende der Maßlosigkeit, SZ vom 08.04.2014, https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057, zuletzt aufgerufen am 12.01.2025.

496 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 85 ff. = NJW 2021, 531; dazu *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap G Rn. 397 f.; *dies*., NJW 2021, 2079 (2080 f.); *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); *A. Baumgartner*, GSZ 2021, 36 (43).

497 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 65 = NJW 2017, 717; *Zalnieriute*, Modern Law Rev. 85 (2022), 198 (207 ff.); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1458 f.); zu den Konsequenzen der Infpflichtnahme Privater für die grundrechtliche Bewertung vgl. BVerfGE 125, 260 (321) – Vorratsdatenspeicherung; *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff.; zur entsprechenden Diskussion im Geldwäscherecht vgl. *Degen,* Geldwäsche, 2009, S. 130 ff.; *Dahm/Hamacher*, wistra 1995, 206.; *Herzog*, WM 1996, 1753 (1762).

498 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 41 = NJW 2014, 2169; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 84 = NJW 2021, 531.

499 Vgl. *Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (23 ff.); *Rojszczak*, Computer Law & Security Review 2021, 105572 (7 ff.).

Wie auch das BVerfG[500] betrachtete der Gerichtshof die Vorratsdatenspeicherung von TK-Verkehrsdaten als zweifachen Eingriff in den unionsgrundrechtlichen Schutz privater Daten, wobei er erstmals eine differenzierte Darstellung der Schutzbereiche von Art. 7 und 8 EU-GRC versuchte.[501] Entscheidend für die grundrechtliche Bewertung waren für den EuGH dann aber nicht die einzelnen Datenverarbeitungsschritte, die jeweils eigens einen Eingriff darstellten, sondern die Nachteile der Betroffenen, die sich gerade aus der finalen Kombination der Verarbeitungsschritte ergäben.[502] Damit prägte der EuGH die Art und Weise, wie sicherheitsrechtliche Maßnahmen der Massenüberwachung grundrechtlich zu fassen sind.

Das ursprünglich rigide Verbot der Vorratsdatenspeicherung ist mittlerweile zwar einem eher unübersichtlichen System verschiedener Ausnahmen und davon abhängender Gestaltungsformen gewichen.[503] In allen Fällen der zulässigen Speicherung sind aber stets strenge Anforderungen an die Verhältnismäßigkeit zu beachten. Dazu gehört insbesondere, dass der Zugang zu den gespeicherten Daten durch materielle und formelle Anforderungen, insbesondere durch eine unabhängige Vorabkontrolle der Zulässigkeit, eng begrenzt wird und datenschutzrechtliche Sicherheits- und Transparenzvorschriften flankierend erlassen werden.[504] Auch eine Unterrichtungspflicht gehört zu den unionsgrundrechtlichen Anforderungen.[505]

---

500 BVerfGE 125, 260 (309 f.) – Vorratsdatenspeicherung.

501 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 38 ff. = NJW 2014, 2169; dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 202 ff.; *W. Michl*, DuD 2017, 349; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.

502 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169; „*Mitsilegas/Guild/Kuskonmaz ua.*, European Law Journal 2022 (online preprint), 1 (4): "holistic approach".

503 Vgl. *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143; übersichtlich die Tabelle bei *Mitsilegas/Guild/Kuskonmaz ua.*, European Law Journal 2022 (online preprint), 1 (7).

504 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 54 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 113 ff. = NJW 2017, 717; Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 31 ff. = NJW 2021, 2103; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 126 ff. = NJW 2022, 3135.

505 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 121 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 190 ff. = NJW 2021, 531.

b. Bestandsdaten: Ministerio Fiscal

Die Rechtsprechung des EuGH ist nicht auf TK-Verkehrsdaten begrenzt. Auch zum Zugriff auf bei den Providern gespeicherten Identitäts- bzw. Bestandsdaten hat der Gerichtshof mittlerweile in der Sache *Ministerio Fiscal*[506] entschieden.

Bestandsdaten sind allerdings im europäischen Recht nicht ausdrücklich definiert. Die e-Privacy-RL kennt nur den Begriff der Verkehrsdaten, Art. 2 lit. b), der Vorschlag zur e-Privacy-VO nur die „Metadaten", Art. 4 Abs. 3 Lit a) b) c) e-Privacy-VO.[507] Entsprechend sieht die e-Privacy-RL auch keinen spezifischen Schutz der Bestandsdaten vor.

Der Begriff der Bestandsdaten findet sich hingegen ausdrücklich im deutschen Recht. § 3 Nr. 6 TKG definiert sie etwa als Daten, „die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste", also Daten, die die Identität des Vertragspartners und die Umstände des Vertrags betreffen.

Der Sache *Ministerio Fiscal* lag ein Strafverfahren zugrunde, in dem der Täter eines Handydiebstahls ermittelt werden sollte. Von dem Gerät war die IMEI-Nummer (International Mobile Station Equipment Identity)[508] bekannt, weshalb die Ermittler bei verschiedenen TK-Dienstleistern anfragten, ob sich in einer bestimmten Zeit eine SIM-Karte ihres Dienstes mit der bekannten IMEI in ein Netz eingewählt hatte, und wenn ja, welche Personendaten mit dieser SIM-Karte verbunden waren.[509] Es wurde also nicht nach den TK-Verbindungen gesucht, sondern allein nach der Identität einer Person.

Der EuGH nahm mangels gesetzlicher Definition keine dem deutschen Recht entsprechende formalistische Einteilung der angefragten Daten vor, sondern stellte lediglich fest, dass Art. 3 Abs.1 e-Privacy-RL die *Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommu-*

506 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

507 Vorschlag der EU Kommission, COM(2017) 10 final - 2017/0003 (COD); zu den Begriffen auch *Schramm/Shvets*, MMR 2019, 568 (569 (Fn. 24)).

508 Teil der Bestandsdaten, wenn bei Vertrag überlassen, *Graf* in BeckOK StPO, § 100a Rn. 29.

509 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 19 ff. = NJW 2019, 655.

*nikationsnetzen* regle.[510] Somit fielen sämtliche Daten, die TK-Provider im Rahmen ihrer Tätigkeit verarbeiten, in den Geltungsbereich der Richtlinie.

Der Anwendungsbereich des Unionsrechts sei deshalb eröffnet, wenn solche Daten verarbeitet würden. Dies schließe den Zugriff staatlicher Behörden auch dann ein, wenn keine korrespondierende Speicherpflicht existiere, da der Zugriff durch Übermittlung der Provider erfolge, was zwangsläufig eine Verarbeitung durch diese mit sich bringe.[511]

Für die dem Fall zugrunde liegenden Daten gelte daher im Grunde nichts anderes als für Verkehrsdaten. Da die Übermittlung eine Verarbeitung darstelle, die die von Art. 5 Abs. 1 e-Privacy-RL geschützte Vertraulichkeit der Kommunikation betreffe, richte sich die Zulässigkeit nach Art. 15 Abs. 1 e-Privacy-RL im Lichte der Art. 7, 8 EU-GRC.[512]

Danach kommt es auf die Verhältnismäßigkeit der Maßnahme an. Diese wiederum ist von der Intensität der Maßnahme abhängig. Aus den Urteilen zur Speicherung und Abfrage von Verkehrsdaten ergibt sich insofern nur, dass schwere Eingriffe nur zur Bekämpfung schwerer Kriminalität gerechtfertigt sein können. Schwache Eingriffe sind schon zur Bekämpfung allgemeiner Kriminalität zulässig.[513]

Um Letztere handelt es sich bei der Abfrage von Daten, aus denen sich nur die Identität eines TK-Nutzers ergibt, da sich aus diesen keine umfangreichen Schlüsse über das Privatleben der betroffenen Person ableiten lassen.[514] Die Abfrage von Bestandsdaten ist danach also auch zur allgemeinen Verbrechensbekämpfung zulässig.

### 2. Fluggastdaten

Neben den Telekommunikationsdaten war auch schon die sicherheitsrechtliche Überwachung von Fluggastdaten (*Passenger Name Records* - PNR) Gegenstand der Rechtsprechung des EuGH.

Bei den PNR ist eine Einteilung in verschiedene Datenkategorien analog zu der Dreiteilung der Kommunikationsdaten in Bestands-, Verkehrs- und

510 Idem, Rn. 33 ff.
511 Idem, Rn. 35 ff.; bestätigt durch EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 35 = NJW 2021, 2103.
512 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 48 ff. = NJW 2019, 655.
513 Idem, Rn. 56 f.
514 Idem, Rn. 69.

Inhaltsdaten nicht möglich. Die Bezeichnung stellt daher stets auf sämtliche Umstände eines Passagierfluges ab. Die aktuelle europäische PNR-Richtlinie[515] ist umfangreich und erfasst nicht nur die Adress- und Identitätsdaten des Passagiers und der Eigenschaften des jeweiligen Flugs, etwa Start- und Zielflughafen, Abflugdatum, Start- und Landezeit sowie der Flugscheindaten bzw. -Nummer, sondern unter anderem auch Namensangaben der Sitznachbarn oder den Vielfliegereintrag nach Art. 6 Abs. 2 PNR-RL, § 2 Abs. 2 FluGDaG.

### a. PNR-Abkommen mit den USA

Seinen Ursprung nahm die sicherheitsrechtliche Verwendung von Fluggastdaten in den entsprechenden Abkommen der EU mit den USA, die als Reaktion auf die Terroranschläge von 2001 abgeschlossen wurden.[516]

Schon nach der EU-Datenschutzrichtlinie (DSRL)[517] war eine Datenübermittlung in Drittländer nur zulässig, wenn die Übermittlung im Rahmen einer Angemessenheitsentscheidung der Kommission nach Art. 25, 31 Abs. 2 EU-Datenschutz-Rl für zulässig erachtet wurde. Da aber stets auch eine rechtliche Grundlage für die Datenübermittlung nötig war, ging die Kommission davon aus, dass ein begleitendes Abkommen abgeschlossen werden musste – auch, um solche Rechtsfragen zu klären, die nicht in der Angemessenheitsentscheidung adressiert werden konnten.[518]

515 Richtlinie (EU) 2016/681 des europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. 2016, L 119/132.

516 Ausf. zur Historie *Baumann,* Datenschutzkonflikte, 2016, S. 412 ff.

517 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995, L 281/31; konsolidierte Fassung: Dokument 01995L0046-20031120.

518 *Europäische Kommission*, Commission Staff Working Paper – An EC-U. S. Agreement on Passenger Name Records (PNR) vom 31.01.2004, SEC(2004) 81, S. 3

aa. EuGH-Entscheidung zum PNR-Abkommen USA 2004

Ein erstes solches Abkommen wurde am 17.05.2004 vom Rat beschlossen[519] und trat am 28.05.2004 mit der Unterzeichnung durch die USA und Ratifizierung durch das EU-Parlament in Kraft.[520]

Das Abkommen blieb hinsichtlich seines Inhalts noch ziemlich vage. Auf gerade einmal zwei Seiten wurde vor allem vereinbart, dass das Bureau of Customs and Border Protection (CBP) des United States Department of Homeland Security (DHS) *elektronischen Zugriff auf PNR-Daten aus den von den Fluggesellschaften im Hoheitsgebiet der EG betriebenen Buchungssysteme erhält, solange kein befriedigendes System für die Übermittlung solcher Daten durch die Fluggesellschaften vorhanden ist.*

Die eigentlichen Regelungen des Abkommens ergaben sich erst aus einer Zusammenschau mit der Angemessenheitsentscheidung[521] i. S. d. Art. 25, 31 Abs. 2 EU-Datenschutz-Rl, die die Kommission kurz zuvor erlassen hatte, und die wiederum eine Verpflichtungserklärung des CBP als Anhang enthielt, in dem die US-Behörde über die rechtlichen Umstände der von ihr geplanten Datenverarbeitung aufklärte.

Der Zugriff des CBP sollte danach nur für Flüge in die und aus den USA ermöglicht werden. Der Katalog der PNR-Daten war umfassend und enthielt im Prinzip sämtliche Daten, die die Fluggesellschaften über die Passagiere anlegten: vom Namen des Passagiers über die Flugscheindaten bis hin zum zuständig gewesenen Bearbeiter im Reisebüro.[522]

Gegen das Abkommen und die Angemessenheitserklärung der Kommission erhob das EU-Parlament Klage vor dem EuGH.

Als Kernargument wurde vorgetragen, dass die für die Rechtmäßigkeit der Datenübermittlung in ein Drittland (unbestritten) notwendige Ange-

519 Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika uber die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security, ABl. 2004, L 183/83.

520 Vgl. EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 32 = NJW 2006, 2029; *Nitschke* Jahrbuch Terrorismus 2007, 209 (209 Fn 1); zur Historie *Baumann,* Datenschutzkonflikte, 2016, S. 424 ff.; *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (901 ff.);

521 Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden, Abl. 2004, L 235/11.

522 Anhang A Verpflichtungserklärung CBD, Abl. 2004, L 235/11(21).

messenheitsentscheidung der Kommission i. S. d. Art. 25, 31 Abs. 2 DS-RL nicht ergehen hätte dürfen, da ihr Regelungsziel nicht in den Anwendungsbereich der Richtlinie fiel.[523] Art. 3 Abs. 2 der DSRL nahm Verarbeitungen vom Anwendungsbereich der Richtlinie aus, die *die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich* [betrafen].

Dieser Argumentation folgte der Gerichtshof. Zwar würden die Daten von privaten Wirtschaftsteilnehmern erhoben, die konkrete Übermittlung erfolgt aber allein aufgrund der staatlichen Rahmensetzung und diente der öffentlichen Sicherheit.[524] Insofern legte der EuGH den Anwendungsbereich der DSRL deutlich enger aus als bei der Vorratsdatenspeicherung von Verkehrsdaten im Rahmen der e-Privacy-RL.[525]

Auch dem Beschluss des Rats der EU (und damit dem Abkommen selbst) wurde primär die fehlende Kompetenz entgegengehalten. Als Rechtsgrundlage wurde – wie später abermals bei der TK-Vorratsdatenspeicherung (s. o. II. 1. aa. (1))[526] – Art. 95 Abs. 1 EG[527] (heute Art. 114 Abs. 1 AEUV) herangezogen, der die EU zur Harmonisierung der Wirtschaft ermächtigte.

Der EuGH folgte konsequent dem Vortrag des Parlaments. Er befand, dass die Richtlinie tatsächlich nicht primär der Harmonisierung diente, sondern der öffentlichen Sicherheit. Die Rechtsgrundlage hätte daher in der „dritten Säule“[528] der EU gesucht werden müssen.[529] Von dieser Ansicht rückte der Gerichtshof hinsichtlich der Vorratsdatenspeicherung von

523 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 51 = NJW 2006, 2029.

524 Idem, Rn. 57 f.

525 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; so auch *Boehm/Cole* ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267); krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

526 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.).

527 Vertrag zur Gründung der Europäischen Gemeinschaft, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

528 Vgl. *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (888 ff.).

529 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 67 ff. = NJW 2006, 2029.

TK-Verkehrsdaten später ab. Er begründete dies damit, dass dort nur eine Speicherung und keine Übermittlung geregelt worden war.[530]

Unabhängig davon, dass der „Erfolg" von kurzer Dauer war, wurde das Urteil im Nachgang als Pyrrhussieg[531] bezeichnet, da es sich inhaltlich nicht mit der Rechtmäßigkeit der PNR-Sammlung und Übermittlung auseinandersetzte und durch die rein formelle Argumentation die Gesetzgebung allenfalls zu einem neuen Versuch aufforderte.

### bb. PNR-Abkommen EU-USA 2007 und 2012

Das Urteil des EuGH brachte die Airlines in die Bredouille. Die amerikanische Rechtslage verpflichtete sie zur Datenübermittlung an das DHS, während das Europäische Datenschutzrecht eine solche mangels gültiger Kommissionsentscheidung untersagte. Es stand bereits der Vorschlag im Raum, keine Flüge zwischen den USA und der EU zuzulassen, da nur so ein (global) rechtmäßiges Verhalten der Airlines gesichert werden könnte.[532] Im Jahr 2007 kam es deshalb zu einem neuen Abkommen[533] zwischen der EU und den USA – diesmal gestützt auf die Art. 24, 38 des EUV[534] (Nizza).[535]

Das Abkommen war wieder vage und kurzgehalten. Substanziell ergänzt wurde es, ähnlich dem Abkommen von 2004, durch eine Erklärung des DHS, das sogenannte „DHS-Schreiben", auf das in Nr. 1 der Erwägungsgründe des Abkommen ausdrücklich Bezug genommen wurde.[536]

---

530 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.); s.a. *Flynn* UC Dublin Law Rev. 8 (2008), 1 (11 f.); *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel*, MMR 2007, 411 (412 f.) *Breyer*, StV 2007, 214 (215 f.).

531 *Maxian Rusche/Kullak* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 100 Rn. 147.

532 *Nitschke*, Jahrbuch Terrorismus 2007, 209 (210).

533 Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007), ABl. 2007, L 204/18.; zur Historie ausf. *Baumann,* Datenschutzkonflikte, 2016, S. 461 ff.

534 Vgl. Beschluss 2007/551/GASP/JI des Rates vom 23. Juli 2007, ABl. 2007, L 204/16.

535 Konsolidierte Fassung des Vertrags über die Europäische Union, ABl. 2002, C 325/01.

536 Dazu krit. *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (910 ff.).

Obwohl mit dem Abkommen von 2007 eine weitreichende Zugriffsmöglichkeit für die US-Behörden geschaffen worden war, herrschte auf beiden Seiten des Abkommens Unzufriedenheit.[537] Daher wurde das Abkommen revidiert und 2012 durch ein Drittes ersetzt[538], das nunmehr nach dem Verfahren des Art. 218 AEUV und daher mit Zustimmung des EU-Parlaments zustande kommen musste.[539]

Es enthielt erstmals selbstständig eine ausführliche Regelung, ohne auf Zusatzerklärungen wie das „DHS-Schreiben" zu verweisen. Inhaltlich wurden die bestehenden Intensitätsmerkmale allerdings erneut ausgeweitet.

Das PNR-Abkommen mit den USA stand und steht ebenso wie die entsprechenden Abkommen mit Australien[540] und Kanada in der Kritik[541], auch aufgrund der heute strengen Rechtsprechung des EuGH hinsichtlich der Übermittlung persönlicher Daten in Drittstaaten.[542] Diese soll nach Erwägungsgrund 102 der DSGVO zwar bei entsprechenden Abkommen weiterhin möglich sein, ohne dass die Bedingungen der Art. 45 ff. DSGVO erfüllt sein müssen. Der EuGH leitet die Notwendigkeit einer Schutzäquivalenz aber aus den EU-Grundrechten ab und stellt somit auch an die Abkommen hohe Anforderungen, wie sogleich zu zeigen sein wird. Zum heutigen Zeitpunkt haben die PNR-Abkommen mit den USA und Australien jedoch weiterhin Bestand.

537 Vgl. *Baumann,* Datenschutzkonflikte, 2016, S. 476 ff.; *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (917 ff.).

538 Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, ABl. 2012, L 215/15.

539 *Baumann,* Datenschutzkonflikte, 2016, S. 476 ff.

540 Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service, ABl. 2012, L 186/3, berichtigt in Abl. 2012, L 302/14.

541 Übersichtlich *Gleß/Wahl* in Schomburg/Lagodny, Int. Rechtshilfe Strafsachen, III B 4ab FlugastAbkEU-USA Rn. 8 ff.

542 Zur USA insbesondere EuGH, Urt. v. 06.10.2015, C-362/14 (Schrems I) = NJW 2015, 3151; Urt. v. 16.07.2020, C-311/18 (Schrems II) = NJW 2020, 2613

### b. EuGH-Gutachten zum PNR-Abkommen EU – Kanada

Das geplante PNR-Abkommen mit Kanada[543] ist hingegen nicht zustande gekommen, da es der EuGH in einem Gutachten für rechtswidrig befand.[544] Inhaltlich entsprach das geplante Kanada-Abkommen weitestgehend jenem mit den USA. Die Fluggesellschaften sollten bei Flügen zwischen der EU und Kanada verpflichtet werden, umfangreiche PNR-Daten an eine kanadische Behörde zu übermitteln. Dort hätten die Daten insgesamt für fünf Jahre gespeichert werden sollen, wobei nach dreißig Tagen eine erste und nach zwei Jahren eine weitere Anonymisierung vorgeschrieben war, Art. 16 PNR-Abkommen-Kanada. Die Daten sollten nach Aussage des Generalanwalts hauptsächlich *automatisierten Analysen unterzogen werden, die auf im Voraus festgelegten Modellen und Kriterien und dem Abgleich mit verschiedenen Datenbanken* beruhten und vor Ankunft des Flugzeugs stattfinden sollten.[545] Diese automatisierte Analyse wurde im Abkommen allerdings nicht ausdrücklich geregelt, sondern lediglich in Art. 15 vorausgesetzt, nach dem Kanada *Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten treffen sollte.*

Bei dem PNR-Abkommen mit Kanada sollten also verschiedene Überwachungsformen, namentlich die automatische Datenanalyse und die Vorratsdatenspeicherung, miteinander verknüpft werden.[546] Aufgrund der deshalb absehbaren Grundrechtsrelevanz forderte das Europäische Parlament ein Gutachten des EuGH nach Art. 218 Abs. 11 AEUV an.

Der Gerichtshof erkannte zunächst, dass aufgrund des PNR-Abkommens in Art. 7 *und* 8 EU-GRC eingegriffen werden sollte, und zwar eigen-

543 Empfehlung für einen Beschluss des Rates zur Genehmigung der Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und Kanada über die Übermittlung und Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität vom 18.10.2017, COM(2017) 605.

544 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 154 ff. = ZD 2018, 23.

545 Idem, Rn. 130 ff. mit Verweis auf, GA *Mengozzi,* Schlussanträge v. 08.09.2016, Gutachten 1/15 (PNR Canada), Rn. 252; s.a. *Europäische Kommission,* Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer vom 21.09.2010, KOM(2010) 492 e, S. 4 ff.

546 Vgl. zum FlugDaG: *Ruthig* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, FlugDaG Vorb Rn. 3.

ständig jeweils durch die Datenübermittlung der Airlines, die Speicherung bei der kanadischen Behörde und die Möglichkeit der Weitergabe an Behörden in Kanada und weiteren Drittstaaten.[547] Durch das Abkommen würden die PNR-Daten sämtlicher Fluggäste zwischen der EU und Kanada überwacht.[548]

Sodann widmete sich der Gerichtshof der Frage, ob diese Eingriffe gerechtfertigt wären. Dabei bemühte er die aus *Digital Rights Ireland* bekannte Vermischung aus Bestimmtheit und Erforderlichkeit (s. o. II. 1. a. aa. (2) (b)).[549]

Erste Mängel identifizierte der EuGH bei der Bestimmtheit einzelner PNR-Datenrubriken, da diese durch offene Aufzählungen wie etwa „sämtliche verfügbaren Kontaktangaben" oder der Verwendung von „etc." nicht hinreichend klar zu erkennen geben, welche Daten gemeint sind.[550] Die Umschreibungen waren insofern nicht auf das Notwendigste beschränkt

Einen weiteren Grundrechtsverstoß hinsichtlich der zu verarbeitenden Daten erkannte der EuGH in dem fehlenden Ausschluss besonders sensibler Daten. Deren Verarbeitung lässt sich nicht mit der Bekämpfung von Terrorismus und schwerer Kriminalität rechtfertigen, denn dies müsste konsequenterweise bedeuten, dass Kenntnisse über sensible Merkmale (Herkunft, Rasse, Religion etc.) bei der Bekämpfung hilfreich bzw. notwendig sein könnten. Darin läge eine immanente Diskriminierung.[551]

Zu den Datenverarbeitungen selbst äußerte sich der EuGH weniger absolut. Hinsichtlich der automatischen Datenanalyse etwa folgte er den Ausführungen des Generalanwalts dahingehend, dass das Eingriffsgewicht insbesondere von der Fehlerquote und dem Diskriminierungspotential abhängen würde, was wiederum von den verwendeten Modellen, Kriterien und Datenbanken abhängig sei, anhand derer der Abgleich durchgeführt wurde. Um die Verhältnismäßigkeitsbedingungen zu erfüllen, *müsse deren Zuverlässigkeit und Aktualität unter Berücksichtigung statistischer Daten*

547 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 125 = ZD 2018, 23

548 Idem, Rn. 127.

549 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 54 = NJW 2014, 2169; vgl. dazu *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC, Art. 52 Rn. 31.

550 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 155 ff. = ZD 2018, 23

551 Idem, Rn. 165.

*und der Ergebnisse der internationalen Forschung, Gegenstand einer gemeinsamen Überprüfung seiner Durchführung sein.*[552]

Wie auch in den Urteilen zur Vorratsdatenspeicherung kritisierte der Gerichtshof aber, dass auch solche Daten übermittelt und analysiert wurden, bei denen im (Moment der Verarbeitung) keine Hinweise darauf bestehen, dass die Verarbeitung für den sicherheitsrechtlichen Zweck des Abkommens förderlich ist. Anders als noch hinsichtlich der universellen Speicherung von Verkehrsdaten bemerkte der EuGH aber ausdrücklich, dass gerade in der Universalität der Sinn der Analyse liege, da erst aus dem Abgleich aller verfügbaren Daten eine automatische Identifizierung verdächtiger Muster möglich würde.[553] Außerdem erfolgten auch die bei der Ankunft stets notwendigen Grenzkontrollen im Ergebnis anlasslos, weshalb Flugpassagiere universell mit einer Verarbeitung ihrer Daten im Rahmen von Flugreisen rechnen müssten.[554] Dass die Datenanalyse sämtliche Fluggäste betraf, stellte für den EuGH deshalb keine Verletzung der Art. 7, 8 EU-GRC dar.

Anders begegnete er der Speicherung der PNR-Daten. Bei diesem Verarbeitungsschritt differenzierte der EuGH zwischen der Ankunft der Fluggäste, der Zeit des Aufenthalts in Kanada und der Ausreise.

Die Speicherung und Verwendung bei der Anreise sah der Gerichtshof grundsätzlich als unproblematisch an, da in dieser Zeit die Daten schon zur Abwicklung der Grenzkontrollen sinnvoll sein könnten und außerdem das Ergebnis der automatischen Analyse gerade dann zur Terrorismus- und Kriminalitätsbekämpfung sinnvoll zu weiteren Maßnahmen führen könnte. [555] Allerdings sei zu beachten, dass mit der Gestattung der Einreise trotz durchgeführter Analyse letztlich zum Ausdruck gebracht wird, dass in diesem Moment keine entsprechende Gefährdung durch die jeweilige Person vorliegen kann. Daher müsse für die Zeit des Aufenthalts in Kanada ein eigenständiger Grund für die Speicherung vorliegen.[556] Mangels einer solchen Bedingung im Abkommen sei dieses schon deshalb unverhältnismäßig.

552 Idem, Rn. 174.
553 Iden, Rn. 187.
554 Idem, Rn. 188; ähnlich der Vergleich anlassloser Kennzeichenüberwachung mit Grenzkontrollen bei *Möstl*, GSZ 2019, 101 (105 ff.).
555 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 197 ff. = ZD 2018, 23.
556 Idem, Rn. 200.

Noch strenger aber behandelte der EuGH die Speicherung von PNR-Daten nach der Ausreise der betroffenen Personen. Da diese im Zeitpunkt der Ausreise mindestens zweimal kontrolliert würden, sei in diesem Moment sichergestellt, dass die Verarbeitung ihrer Daten den Zweck des Abkommens nicht mehr fördern könnte. Insofern handelt es sich um eine anlasslose Speicherung, die entsprechend den Erkenntnissen aus *Tele2Sverige/Watson* (s.o.)[557] nicht mit der Bekämpfung von Terrorismus und schwerer Kriminalität gerechtfertigt werden kann.[558]

Aufgrund all dieser Mängel erklärte der EuGH das geplante Abkommen der EU mit Kanada für unvereinbar mit Art. 7, 8 EU-GRC. Von einem Beschluss des Abkommens wurde entsprechend abgesehen. Stattdessen empfahl die Kommission, neue Verhandlungen mit Kanada anzutreten.[559] Ein Ergebnis solcher Verhandlungen liegt aktuell noch nicht vor.

### c. Das EuGH-Urteil zur PNR-Richtlinie

Parallel zu den Abkommen mit Drittstaaten etablierte die EU ein für die Mitgliedstaaten verpflichtendes PNR-System für Flüge zwischen Drittstaaten und der EU in Form der PNR-RL,[560] die in Deutschland durch das FluGDaG umgesetzt wurde.[561]

Die Airlines sollen vor dem Start von Flügen in und aus der EU, von oder in Drittstatten die Fluggastdaten per Push-Verfahren an eine zentrale Meldestelle des Mitgliedstaates übermitteln, aus dem der Flug startet bzw.

557 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

558 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 207 = ZD 2018, 23.

559 *Europäische Kommission,* Empfehlung für einen Beschluss des Rates zur Genehmigung der Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und Kanada über die Übermittlung und Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität vom 18.10.2017, COM(2017) 605 final.

560 Richtlinie (EU) 2016/681 des europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. 2016, L 119/132).

561 Zur Historie *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 248 ff.; *Kostov*, GSZ 2022, 267 (267 ff.); *Orrù*, Information Polity 27 (2022), 131 (132 ff.); *Lowe*, ICLR 17 (2017), 78 (85 ff.).

in dem er landet, Art. 8 Abs. 1 PNR-RL. Dabei ist zu beachten, dass die Mitgliedstaaten ermächtigt wurden, die Richtlinie auf Flüge innerhalb der EU auszuweiten, Art. 2 PNR-RL.

Bei der zentralen Meldestelle können die PNR-Daten nach Art. 6 Abs. 3 PNR-RL abgeglichen werden mit *Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken, betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und* Unionsvorschriften (lit. a), oder *anhand im Voraus festgelegter Kriterien*. Im letzten Fall ist sicherzustellen, dass die Kriterien nicht auf sensiblen bzw. diskriminierenden Faktoren beruhen (Art. 6 Abs. 4 PNR-RL.

Die Daten werden bei der zentralen Meldestelle für fünf Jahre gespeichert, wobei nach sechs Monaten eine Anonymisierung stattfindet, die nur unter strengen Auflagen rückgängig gemacht werden kann, Art. 12 PNR-RL. Die zentrale Meldestelle soll bei begründeten Anfragen zuständiger Behörden PNR-Daten zur Verfügung stellen und verarbeiten bzw. die Ergebnisse der Verarbeitung zur Verfügung stellen und zwar in *besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität*, Art. 6 Abs. 2 lit. b) PNR-RL.

Dieses PNR-Überwachungsregime wurde jüngst vom EuGH in der Entscheidung *Ligue des droits humains* auf seine Vereinbarkeit mit europäischen Grundrechten, insbesondere Art. 7, 8 EU-GRC, überprüft.[562]

Dabei wählte der EuGH eine fragwürdige Vorgehensweise.[563] Er beanstandete zwar viele Inhalte der Richtlinie, anstatt sie aber deshalb aufzuheben, gab er lediglich vor, wie die Richtlinie an den entsprechenden Stellen ausgelegt werden muss, um nicht gegen Art. 7, 8 EU-GRC zu verstoßen. In manchen Fällen handelt es sich dabei um eine Auslegung *contra legem*.

Die Ausweitung auf EU-interne Flüge etwa hielt der EuGH nur für gerechtfertigt, wenn der Mitgliedsstaat sich in einer spezifischen Bedrohungs-

562 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706.

563 Krit. *Thönnes*, Die Verwaltung 2022, 527 (531 ff.); *ders.*, directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

situation befände.[564] Insofern übertrug er die aus *La Quadrature du net* bekannte Ausnahmeregel[565] auf die Ausweitung der PNR-Überwachung. Obwohl aber in Art. 2 PNR-RL nichts von einer solchen Begrenzung steht, durfte die Vorschrift in Kraft bleiben. Hier handelt es sich um eine teleologische Reduktion. Auch bei der Bestimmtheit der im Katalog des Anhang 1 aufgeführten PNR-Daten monierte der Gerichtshof mehrere Rubriken, stellte dann aber fest, dass diese klar und präzise formuliert sind, wenn man sie nur anhand der Urteilserwägungen auslegt.[566]

Der Effekt dieser Methode ist, dass der EuGH faktisch eine neue Richtlinie geschaffen hat, deren Inhalt sich nur aus dem Gesetzestext in gemeinsamer Lesung mit dem hierzu ergangenen Urteil erschließt.[567]

Inhaltlich entsprechen diese verhältnismäßigkeitswahrenden Auslegungsanforderungen weitestgehend dem Gutachten des EuGH zum PNR-Abkommen mit Kanada. Der Gerichtshof ging allerdings noch spezifischer auf die Zweckbindung der PNR-Datenverarbeitung ein.

Da das PNR-System zu einer anlasslosen, kontinuierlichen Überwachung der Fluggäste führt, handelt es sich um einen schwerwiegenden Eingriff, der nur dann gerechtfertigt sein kann, wenn er unmittelbar zu den mit der Richtlinie verfolgten Zwecken in Zusammenhang steht. Die einzelnen Datenverarbeitungsschritte der Fluggastüberwachung kommen daher nur infrage, wenn die verfolgten Zwecke derart mit Flugreisen in Zusammenhang stehen, sodass die Überwachung des Flugverkehrs insofern sinnvoll erscheint. Dies sei bei Terrorismus grundsätzlich anzunehmen, bei schwerer Kriminalität allerdings nicht. Die Richtlinie muss daher so interpretiert werden, dass das Überwachungssystem nur zur Bekämpfung solch schwerer Kriminalität verwendet werden darf, die *wenigstens mittelbar in objektivem Zusammenhang mit der Beförderung von Fluggästen* steht.[568] Hierbei ist etwa an den Menschenhandel, Handel mit Drogen und

564 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 166 ff. = EuZW 2022, 706.

565 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

566 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 155 ff. = EuZW 2022, 706.

567 Dazu krit. *Thönnes*, Die Verwaltung 2022, 527 (531 ff., 539); ders., Die Verwaltung 2022, 527 *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

568 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 140 = EuZW 2022, 706.

Waffen, Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt oder auch an Flugzeugentführungen zu denken.[569] Anhand dieser engeren[570] Zweckbestimmung als Auslegungsgrundsatz untersuchte der EuGH dann die einzelnen Datenverarbeitungsschritte.

Wie schon im Kanada-Gutachten kam er zu dem Ergebnis, dass eine automatisierte Datenanalyse vor der Landung grundsätzlich mit Art. 7, 8 EU-GRC vereinbar ist, wenn ausreichende Kontrollmechanismen eingeführt würden. Um die enge Bindung an den Richtlinienzweck zu gewährleisten, dürfen zum Abgleich nur Datenbanken verwendet werden, in denen Daten von Personen gespeichert sind, bei denen ein objektiver Verdacht auf einen Zusammenhang mit Terrorismus oder (grenzübergreifender) schwerer Kriminalität besteht, und nach denen deshalb gefahndet wird.[571] Der Datenbankabgleich muss also auf einen speziellen Fahndungsabgleich hinauslaufen.

Weiter muss gesichert sein, dass keinerlei weitere nachteilige Grundrechtseingriffe allein auf Grundlage des automatisierten Abgleichs erfolgen.[572] Stets muss der „Treffer" menschlich nachgeprüft werden. Insofern erkannte der EuGH ein Recht auf menschliche Entscheidung und brachte den persönlichen Datenschutz gegen die aufkommende Tendenz zum Einsatz künstlicher Intelligenz in Stellung.[573] Diesen Ansatz verfolgte er weiter, indem er den alleinigen Einsatz künstlicher Intelligenz bei der Bestimmung der *im Voraus festgelegter Kriterien* zum Datenabgleich i. S. d. Art. 6 Abs. 3 lit. b) PNR-RL ausschloss. Stets müssten die Kriterien durch den Menschen – insbesondere auf deren Diskriminierungsfreiheit – kontrolliert werden.[574]

Auch bei der Weiterübermittlung von Daten durch die Zentralstelle auf Anfrage muss die enge Zweckbindung beachtet werden, damit die Voraussetzungen an die automatisierte Datenverarbeitung nicht unterlaufen werden. Die Ergebnisse der automatisierten Verarbeitung sind daher nur zu

569 Vgl. insofern zum Anhang 2 der PNR-RL: *Wissenschaftliche Dienste des Bundestags,* PNR-Urteil, 2022, S. 8.
570 *Kostov*, GSZ 2022, 267 (271).
571 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 182 ff. = EuZW 2022, 706.
572 Idem, Rn. 179.
573 Dazu *Orrù, Information Polity* 27 (2022), 131 (135 ff.).
574 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 193 ff. = EuZW 2022, 706.

übermitteln, wenn sich aus ihnen ein objektiver Verdacht auf Terrorismus oder schwerer Kriminalität ergibt.[575]

Überhaupt ist die Weiterleitung der Daten im Hinblick auf die strenge Rechtsprechung zur Vorratsdatenspeicherung nur unter engen Voraussetzungen möglich. Soweit die Anfrage nach der Ankunft im Zielland stattfindet, muss beachtet werden, dass die automatisierte Überprüfung offensichtlich ergeben hat, dass die betroffene Person keine Anhaltspunkte für ihre *mögliche Beteiligung an terroristischen Straftaten oder an schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen* geliefert hat. Die Gründe der Abfrage müssen daher im Nachhinein entstanden sein.[576]

Dabei ist eine Abfrage grundsätzlich nur bei entsprechendem Anlass möglich, es sei denn, dass der jeweilige Mitgliedstaat sich in einer außergewöhnlichen Bedrohungssituation für seine nationale Sicherheit befindet.[577] Außer in besonderen Eilfällen ist dabei stets ein Richtervorbehalt zu implementieren, und zwar entgegen Art. 12 Abs. 3 lit. b) PNR-Richtlinie auch innerhalb der ersten sechs Monate, d. h. bevor die Daten anonymisiert wurden.[578]

Die anlasslose Speicherung der PNR-Daten bei der zentralen Stelle (und mithin die massenhafte Übermittlung durch Private) für sechs Monate hielt der Gerichtshof überraschenderweise für zulässig.[579] Art. 12 Abs. 1 PNR-RL steht nur nationalen Vorschriften entgegen, die eine anlasslose Speicherung über sechs Monate vorsehen. Allein solche Daten, die im Rahmen der Vorabprüfung auffällig wurden und daher im Verdacht stehen, eventuell für die Bekämpfung schwerer Kriminalität oder Terrorismus im Zusammenhang mit der Fluggastbeförderung relevant zu werden, könnten länger gespeichert werden, wobei auch für solche Daten die Pflicht zur Depersonalisierung nach sechs Monaten gilt, Art. 12 Abs. 2 PNR-RL.

In diesen beiden Aspekten dürfte der bedeutsamste Teil der Entscheidung liegen. Das allgemeine Verbot anlassloser Speicherung im Sicherheitsrecht kann nach dieser Entscheidung nicht mehr als universelles Prinzip betrachtet werden, sondern gilt (mit vielen Ausnahmen) nur bei TK-Ver-

575 Idem, Rn. 204.
576 Idem, Rn. 218 mit Verweis auf EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 200 = ZD 2018, 23.
577 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 ff. = EuZW 2022, 706.
578 Idem, 220 ff.
579 Idem, 248 ff.

kehrsdaten. Weiter ist die Entscheidung aufgrund der kuriosen Methodik, eine Richtlinie durch Auslegung völlig zu entstellen, als Schritt hin zu einer stärker balancierten Rechtsprechung gegenüber staatlicher Massenüberwachung zu bewerten.[580] Aus grundrechtlicher Sicht stellt die Entscheidung gegenüber den Entscheidungen zur Verkehrsdatenspeicherung insofern einen Rückschritt dar.

### 3. Zusammenfassung

Der EuGH kann mittlerweile also ebenfalls auf eine umfassende Rechtsprechungshistorie zu staatlichen Massenüberwachungsmaßnahmen zurückschauen. Durch eine weitgehende Kompetenzwahrnehmung hat er sich als bedeutende Institution im Sicherheitsrecht etabliert und als *Grundrechtsgericht* eigene Maßstäbe – auch für die nationalen Gesetzgeber – gesetzt.

Das Vorgehen entspricht dabei grob demjenigen des BVerfG.[581] Im Grunde entwickelt der Gerichtshof durch Anwendung des Verhältnismäßigkeitsgrundsatzes spezifische Voraussetzungen für staatliche Überwachungsmaßnahmen in Abhängigkeit von deren Intensität.[582] Überwachungsmaßnahmen werden nicht mehr prinzipiell verboten, sondern *prozeduralisiert.*[583]

Dogmatisch zeichnet sich die Rechtsprechung des EuGH aber durch eine geringere Komplexität gegenüber dem BVerfG aus. Zwar ordnet der Gerichtshof ebenfalls Maßnahmen schematisch in Schwerekategorien, er unterscheidet bislang aber nur zwischen *schweren* und *nicht schweren* Ein-

580 Vgl. *Thönnes*, Die Verwaltung 2022, 527 (531 ff.)M *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025

581 Beispielhaft BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84: "Operationalisierung der Verhältnismäßigkeit"; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.); *Volkmann*, NVwZ 2022, 1408 (1411): „Steuerungsmodell"; *Trute*, Die Verwaltung 2009, 85 (85 ff; 96 ff.); *Groß* KJ 2002, 1 (9 ff.); krit. *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., insbesondere 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (67 ff.).

582 Jüngst EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 112 ff. = EuZW 2022, 706. mwN.

583 *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.); s.a. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (104 ff.).

griffen, die dann entsprechend nur zur Bekämpfung und Verhütung von schwerer oder allgemeiner Kriminalität zulässig sind[584].

Unterschiede bei den Merkmalen, anhand derer die Intensität bestimmt wird, bestehen dabei kaum. Die Heimlichkeit, Streubreite und Datenqualität stehen auch beim Gerichtshof im Vordergrund, wenngleich Letztere gegenüber der Rechtsprechung des BVerfG zuletzt eine besonders prominente Stellung eingenommen hat.[585] Auf theoretische Erklärungen der Intensitätsmerkmale verzichtet der EuGH allerdings völlig und begnügt sich stets mit der pauschalen Feststellung, dass heimliche Massenüberwachungsmaßnahmen aufgrund möglicher Einschüchterungen das Gefühl totaler Überwachung herbeiführen könnten.

Die anlasslose Vorratsdatenspeicherung von TK-Verkehrsdaten lehnte der EuGH zunächst prinzipiell ab,[586] schuf aber im Laufe der Zeit doch eine Reihe von Ausnahmen.[587] Eine anlasslose, vorratsmäßige Speicherung ist danach nur noch zulässig zum Schutz der *nationalen Sicherheit* und auch dann nur, wenn für diese eine besondere Bedrohungslage besteht.[588] Ansonsten ist der Sicherheitsgesetzgeber auf die *targeted retention*[589] und das *quick freezing*[590] verwiesen.[591]

Der EuGH hat sich nicht auf eine schematische Gleichbehandlung sämtlicher Daten festgelegt, sondern behält sich offenbar vor, je nach Daten-Art unterschiedliche Anforderungen und Grundsätze zu entwickeln. Eine anlasslose Speicherung von Fluggastdaten hält der Gerichtshof auch

584 Vgl. EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 54 ff. = NJW 2019, 655.

585 Vgl. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 100 = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 71 = NJW 2022, 3135.

586 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

587 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 137 ff. = NJW 2021, 531; übersichtlich *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (148 ff.).

588 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

589 Dazu Vgl. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (101); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1449); *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (149).

590 Dazu *Juszczak/Sason*, eucrim 2021, 238 (247); zur Rechtslage in der StPO: *Rückert* in MüKo StPO, § 100g Rn. 116.

591 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 140 ff., 160 ff. = NJW 2021, 531.

zur Kriminalitätsbekämpfung für eine Dauer von sechs Monaten nicht für grundsätzlich unverhältnismäßig.[592] Dasselbe gilt in diesem Zeitraum für die Analyse der PNR-Daten, solange die zur Analyse herangezogenen Daten bestimmten Kriterien unterliegen, kein Maschinenlernen eingesetzt und jeder Treffer vor der Weiterverarbeitung einer menschlichen Kontrolle unterzogen wird.[593]

Jedenfalls seit dem PNR-Urteil ist also offen, inwiefern der EuGH seine Rechtsprechung zu sicherheitsrechtlichen Überwachungsmaßnahmen auf Regelungen zur Finanzdatenüberwachung übertragen würde. Soweit bei Speicherung, Zugriff und Analyse dieser Daten-Art besondere Umstände hinzukommen, werden diese bei der Verhältnismäßigkeit Beachtung finden müssen.

Das PNR-Urteil ist jedoch auch insoweit richtungsweisend, als der EuGH eine neue, äußerst fragwürdige Methode zum Einsatz bringt. Anstatt die mit den Art. 7, 8 EU-GRC nicht vereinbarten Bestimmungen der Richtlinie aufzuheben, gab der EuGH vor, wie diese Normen vor dem grundrechtlichen Hintergrund auszulegen sind. Dabei reizte er den Wortlaut nicht nur aus, sondern änderte die Richtlinie letztlich so stark ab, dass von ihrem eigentlichen Wortlaut kaum mehr etwas übrigblieb.[594]. Die Rechtsanwendung wird für somit jeden, der mit dem PNR-Urteil nicht vertraut ist, unmöglich.

### *III. Rechtsprechung des EGMR*

Auch der EGMR hat sich zu sicherheitsrechtlichen Überwachungsmaßnahmen, insbesondere im Hinblick auf Art. 8 EMRK, bereits geäußert. Da sich die Rechtsprechung des EGMR nach Art. 53 EU-GRC auf die Auslegung der Unionsgrundrechte auswirkt und dementsprechend bei der Bewertung der Geldwäschemaßnahmen eine Rolle spielen könnte, soll auch die EGMR-Rechtsprechung hier kurz vorgestellt werden.

592 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 255 = EuZW 2022, 706.

593 Idem, Rn. 176 ff.

594 *Thönnes*, Die Verwaltung 2022, 527 (531 ff., 539); *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

### 1. Frühe Rspr. des EGMR zu sicherheitsrechtlichen Überwachungsmaßnahmen, insbesondere Verkehrsdatenabfrage

Urteile des EGMR zu staatlichen Überwachungsmaßnahmen gibt es nunmehr schon seit fast fünfzig Jahren.[595] Als erster *landmark case*[596] gilt das Urteil *Klass/Bundesrepublik Deutschland*[597], in dem über die Legalität heimlicher nachrichtendienstlicher Maßnahmen nach dem G-10 gestritten wurde.

Die Kläger zweifelten zwar nicht an der grundsätzlichen Zulässigkeit, nachrichtendienstlicher Kommunikationsüberwachung, waren aber überzeugt, dass solche stets mit Benachrichtigungspflichten versehen werden müssen, damit (nachträglicher) Rechtsschutz möglich bleibt. Der EGMR gab ihnen insofern auch recht, entscheidend war aber schon, dass der Gerichtshof die Klage überhaupt für zulässig hielt, da nicht belegt werden konnte, ob die Kläger selbst von den fraglichen Maßnahmen *betroffene Opfer* i. S. d. Art. 25 EMRK waren. Der EGMR stellte im Sinne eines effektiven Rechtsschutzes fest, dass die jeweiligen Antragsteller bereits dann gegen heimliche Überwachungsmaßnahmen bzw. deren gesetzliche Grundlagen vorgehen können, wenn es nicht ausgeschlossen scheint, dass sie von den Maßnahmen betroffen sein könnten.[598] Der Gerichtshof eröffnete damit die Möglichkeit einer objektiven Kontrolle sicherheitsrechtlicher Überwachungsgesetze am Maßstab der EMRK und schuf so die Grundlage für seine künftige Rechtsprechungslinie.

Schon 1984 urteilte der EGMR daraufhin, dass der sicherheitsrechtliche Zugriff auf TK-Verkehrsdaten einen Eingriff in Art. 8 Abs. 1 EMRK darstellt.[599] Er hatte sich hier aber noch nicht zu der Frage zu äußern, ob schon die Speicherung bzw. die Pflicht zur Speicherung einen Grundrechtseingriff in Art. 8 Abs. 1 EMRK konstituiert, sondern lediglich, ob für die polizeiliche Abfrage von TK-Verkehrsdaten eine ausreichend bestimmte Rechtsgrundlage in England und Wales bestand. Dies wurde schließlich verneint, wobei der EGMR schon früh forderte, Ermächtigungen zu staatlichen Überwachungsmaßnahmen mit bestimmten Voraussetzungen zu versehen , die auf

595 Ausf. *Marsch,* Datenschutzgrundrecht, 2018, S. 8 ff.; *Schiedermair,* Schutz des Privaten, 2012, 167 ff.
596 *Górski* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 19 (20).
597 EGMR, Urt. v. 06.09. 1978, Nr. 5029/71 (Klass u.a./Deutschland) = NJW 1979, 1755.
598 Idem, Rn. 34 ff.
599 EGMR, Urt. v. 02.08.1984, Nr. 8691/79 (Malone/Vereinigtes Königreich), Rn. 83 f.

legislativer Ebene eine Verhältnismäßigkeitsgewähr darstellten, ohne aber näher zu spezifizieren, welche dies sein könnten.[600]

## 2. (Vorrats-)Datenspeicherungen als Beeinträchtigung von Art. 8 Abs. 1 EMRK

Inwiefern Datenspeicherungen Art. 8 Abs. 1 EMRK beeinträchtigen, sprach der EGMR allgemein erstmals in der Entscheidung *Leander/Schweden*[601] an. Dieser lag ein Streit um die Beschäftigungsmöglichkeit des Betroffenen in einem Militärmuseum zugrunde, im Zuge dessen persönliche Informationen über ihn in einem Polizeiregister angelegt wurden, ohne dass dessen Inhalt je offenbart wurde. Der EGMR stellte hier pauschal fest, dass schon das Anlegen solcher Informationen in einem Register einen Eingriff in Art. 8 Abs. 1 EMRK darstellt.[602]

Über die anlasslose Vorratsdatenspeicherung war damit aber noch nichts gesagt, da spezifische Registereinträge gerade nicht anlasslos (und somit auch nicht universell) erfolgen. Diese Problematik wurde erstmals in *Marper/Vereinigtes Königreich*[603] angesprochen.

In dieser Entscheidung ging es um die Speicherung von Fingerabdrücken und DNA-Proben von Straftatverdächtigten, die im Rahmen des Ermittlungsverfahrens angelegt wurden. Nach der britischen Rechtslage sollten diese auch dann noch weiterhin gespeichert werden, wenn das Verfahren eingestellt wurde oder es nach einer Verhandlung zu einem Freispruch gekommen war. Der Fall betraf also eine sicherheitsrechtliche Speicherung von Daten, die im ersten Moment zwar anlassbezogen erfolgte, deren Anlasszweck aber nachträglich entfiel.

Zuvor hatte der EGMR bereits entschieden, dass eine systematische Vorratsdatenspeicherung von DNA-Material strafrechtlich Verurteilter keine Verletzung von Art. 8 Abs. 1 EMRK darstellt.[604] Die vorratsmäßige Speicherung der Fingerabdrücke von nur Tatverdächtigen, bei denen es zu einer

600 Idem, Rn. 69 ff, zum „Metering" Rn. 83 ff.
601 EGMR, Urt. v. 26.03.1987, Nr. 9248/81 (Leander/Schweden).; ähnlich EGMR, Urt. v. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien).
602 Idem, Rn. 84; s.a. EGMR, Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 69.
603 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich) = EuGRZ 2009, 299.
604 EGMR, Urt. 07.12.2006, Nr. 29514/05 (van der Welden/Niederlande); bestätigt in Entsch. V. 04.06.2013, Nr. 7841/08, 57900/12 (Peruzzo/Deutschland); kritischer

Einstellung oder einem Freispruch kam, behandelt der EGMR nun aber strenger.

Für die Bewertung kommt es dabei nach Art. 8 Abs. 2 EMRK darauf an, ob der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft *für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer* notwendig ist.

Auch der EGMR nimmt bei staatlichen Datenverarbeitungen also primär eine Verhältnismäßigkeitsprüfung vor.[605] Dabei räumt der Gerichtshof den nationalen staatlichen Stellen aber einen Ermessenspielraum ein, dessen Ausmaß von der Intensität des Eingriffs und der Bedeutung des jeweiligen Konventionsrechts abhängt, wobei sich letzterer aus dem Konsens der Mitgliedstaaten ergeben soll.[606]

In England und Wales wurde seinerzeit auch bei der Speicherung der Daten von Strafverdächtigen nicht zwischen unterschiedlichen Delikten unterschieden, sondern eine Speicherung bei Straftaten jeder Schwere vorgenommen. Außerdem war keine zeitliche Begrenzung der Speicherung vorgesehen. Diese unterschiedslose Sammlung von Fingerabdrücken und DNA-Daten hielt der EGMR im Ergebnis für unverhältnismäßig.[607]

Nun unterscheidet sich die Speicherung solcher Daten aber maßgeblich von der Speicherung von TK-Verkehrsdaten. Anders als die alltägliche Telekommunikation fällt die Speicherung einzelner persönlicher Daten bei der Bevorratung von Fingerabrücken u. ä. einmalig an und dient dann mehr als Register, denn als laufende Überwachung.

Dennoch lassen sich aus der Entscheidung wichtige Erkenntnisse für die Bewertung staatlicher Überwachungsmaßnahmen durch den EGMR ziehen. So wies der Gerichtshof das Argument der Regierung des Vereinigten Königreichs zurück, dass sich aus der Datenverarbeitung unmittelbar keine Nachteile für die Betroffenen ergäben.

---

jüngst zu DNA, Fingerabdrücken und Fotografien: Urt. v. 13.2.2020, Nr. 45245/15 (Gaughran/Vereinigtes Königreich) = NJOZ 2022, 476

605 Vgl. *Górski* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 19 (35).

606 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 102 = EuGRZ 2009, 299; Urt. v. 18.4.2013, Nr. 19522/09 (M.K./. Frankreich), Rn. 34 = NJOZ 2014, 1278; s.a. *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer EMRK, Art. 8 Rn. 111 ff.; allg. *Frowein* in Frowein/Peukert EMRK, 3. Aufl. 2009, Vorb. Art. 8-11, Rn. 13 ff.

607 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 125 = EuGRZ 2009, 299.

Die Speicherung selbst führe tatsächlich zu einer *Stigmatisierung* Nicht-Verurteilter, die mit der konventionsrechtlichen Unschuldsvermutung i. S. d. Art. 6 Abs. 2 EMRK nicht vereinbar sei.[608] Würde man dem Argument der Regierung folgen, wäre eine universelle Speicherung der Fingerabdrücke u. ä. sämtlicher Bürger ebenfalls verhältnismäßig, was laut späterer Entscheidungen des EGMR *zweifellos übermäßig und nicht angemessen wäre*.[609] Auch der EGMR hält universelle Überwachungsmaßnahmen also für grundsätzlich unzulässig und fordert stets eine angemessene Ausgestaltung der Datenverarbeitungsmaßnahmen, die wiederum von der Intensität abhängt. Diese bestimmt er zunächst nach den Eigenschaften der jeweiligen Datenkategorie, nimmt aber zur abstrakten Bewertung des Eingriffs auch rechtsstaatliche Gesichtspunkte, wie den Stigmatisierungseffekt, in den Blick.

Ausgehend von der danach festgestellten Eingriffsintensität soll sich die Verhältnismäßigkeit danach bestimmen, ob das staatliche Recht *angemessene Sicherungen vorsieht, um eine Verwendung solcher Daten zu verhindern, die mit den Garantien jener Vorschrift nicht vereinbar wäre*.[610]

### 3. Verhältnismäßigkeit durch *Sicherungsvorkehrungen* am Beispiel der TKÜ: *Zakharov/Russland*

*Marper/Vereinigtes Königreich* legte somit den Grundstein für eine Rechtsprechungslinie des EGMR, die sich letztlich stark am Vorgehen des BVerfG und EuGH orientiert.

Anstatt einer reinen Rationalitätskontrolle leiten diese Gerichte aus den verfassungs- bzw. primärrechtlichen Bestimmungen spezifische Anforderungen an die gesetzlichen Grundlagen im Sicherheitsrecht ab, die schon auf dieser Ebene einen Ausgleich von sicherheits- und grundrechtlichen Interessen gewährleisten sollen.[611]

608 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 122 = EuGRZ 2009, 299

609 EGMR, Urt. v. 18.4.2013, Nr. 19522/09 (M.K./. Frankreich), Rn. 40 = NJOZ 2014, 1278; Urt. v. 13.2.2020, Nr. 45245/15 (Gaughran/Vereinigtes Königreich), Rn. 89 = NJOZ 2022, 476

610 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 103 = EuGRZ 2009, 299

611 Vgl. BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245

Ein solches Vorgehen lässt sich mittlerweile auch beim EGMR beobachten, wenngleich dessen Rechtsprechung insgesamt noch kasuistisch geprägt ist[612] und kein ganz so nuanciertes Schema etabliert hat wie das BVerfG (das aber auch entsprechend kritisiert wird).[613]

Dies lässt sich an einer Überprüfung der Vorschriften zur Telekommunikationsüberwachung im Fall *Zakharov/Russland*[614] darstellen.

Mit den einzelnen Anforderungen der russischen TKÜ setzte sich der Gerichtshof intensiv auseinander. Anders als das BVerfG war seine Betrachtungsweise allerdings negativ in dem Sinne, dass er nicht selbstständig spezifische Anforderungen aufstellte und dann prüfte, ob die vorhandenen damit übereinstimmten, sondern er zeigte nur die Mängel bzw. das *Missbrauchspotential* der bestehenden gesetzlichen Grundlagen konkret auf. Dies tat er allerdings so ausführlich, dass sich im Wege eines Umkehrschlusses positive Anforderungen an die gesetzlichen Tatbestände ableiten lassen.

Konkret kritisierte der EGMR vor allem die Ausgestaltung der formellen Sicherungsvorkehrungen. Der vorgesehene Richtervorbehalt würde in der Praxis wenig nutzen, da das russische Gesetz keine Verhältnismäßigkeitsprüfung der Maßnahme durch die Gerichte vorsah und in Eilfällen vom Vorbehalt abgesehen werden durfte. Der Richtervorbehalt würde praktisch nur eine Formalie darstellen, die keinen effektiven Schutz der Betroffenen gewährleiste.[615]

Weiter kritisierte der EGMR die Anordnungspraxis in Bezug auf die materiellen Anforderungen. Die Ermächtigungsgrundlage der Nachrichtendienste war nicht auf konkretisierte Personen begrenzt, sondern erlaubte auch Anordnungen, die sich auf nur umrissene Personenkreise oder örtliche Begrenzungen bezogen, bzw. sie wurden für solche verwandt.[616]

Letztlich beanstandete der Gerichtshof auch die Kontrollmechanismen in der russischen Föderation. Die einzige Aufsichtsmaßnahme bestand in der (mangelhaften) Vorabprüfung im Rahmen des Richtervorbehalts. Ab dieser Zulassung wurden die Rechtmäßigkeit der Maßnahme bzw. deren

(253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84.

612 Vgl. *Schiedermair,* Schutz des Privaten, 2012, S. 238 ff.

613 *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (66 ff.); *Wolff*, ZG 2016, 361 (366 f.).

614 EGMR, Urt. v. 4.12.2015, 47143/06 (Zhakarov/Russland) = NMLR 2015, 509.

615 Idem, Rn. 259 ff.

616 Idem, Rn. 265.

Ausgestaltung und Durchführung nur noch von den Staatsanwälten kontrolliert, deren Unabhängigkeit allerdings zweifelhaft sei und, für die eine öffentliche Kontrollaufsicht nicht etabliert war.[617] Insofern war eine rechtliche Überprüfung kaum effektiv möglich. Dies galt erst recht, wenn die Informationen nicht zu einem Verfahren führten, da Benachrichtigungspflichten nicht existierten und die technischen Vorrichtungen zum Abhören in den Endgeräten keine Protokolle anlegten.[618]

### 4. Strategische Fernmeldeüberwachung: *Big Brother* und *Rättvisa*

Zu klassischen Vorratsdatenspeicherungen im Rahmen der Strafverfolgung und Gefahrenabwehr durch Inpflichtnahme Privater hat sich der EGMR bislang nur bzgl. TK-Bestandsdaten geäußert und diese, wie auch das BVerfG und der EuGH, prinzipiell für verhältnismäßig befunden.[619] Dabei ist zu sehen, dass die Bestandsdaten, insbesondere die Vertragsdaten, bei den jeweiligen Unternehmen ohnehin vorliegen werden. Die Bestandsdatenspeicherungskomplexe sind grundrechtlich nur insofern problematisch, wie sie auch die Speicherung eigentlich nicht notwendiger Daten vorsehen und weil sie den Zugang für staatlicher Sicherheitsbehörden zentralisieren und automatisieren (zur Kontostammdatenspeicherung s. Kap D. I. und zur Diskussion Kap. F. I.).

Über diese Kategorie der Telekommunikationsdaten hinaus liegen nur Urteile[620] vor, die sich mit der strategischen Kommunikationsüberwachung durch die Nachrichtendienste beschäftigen, wobei diese auch die Sammlung von Verkehrsdaten ermöglicht.[621]

Die entscheidenden Urteile zur strategischen Fernmeldeüberwachung ergingen parallel im Jahr 2021 und betrafen die Nachrichtendienste des Vereinigten Königreichs und den Militärgeheimdienst von Schweden.[622] In

617 Idem, Rn. 272 ff.
618 Idem, Rn. 289 ff.
619 EGMR, Urt. v. 30.1.2020, Nr. 50001/12 (Breyer/Deutschland) = NJW 2021, 999.
620 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich) = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden) = NVwZ-Beil. 2021, 30.; zuvor schon Entsch. vom 29.06.2006, Nr.54934/00 (Weber u. Saravia/Deutschland) = NJW 2007, 1433.
621 Vgl. Zur Übersicht *B. Huber*, NVwZ-Beilage 2021, 3; *Ibel* ZD-Aktuell 2021, 5246.
622 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich) = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden) = NVwZ-Beil. 2021, 30

älteren Verfahren, insbesondere zum G-10,[623] hatte der EGMR schon entschieden, dass Massenüberwachung nicht grundsätzlich unzulässig sei.[624] Da sich die Telekommunikation und deren Stellenwert in der Gesellschaft seither aber enorm verändert habe und in den früheren Entscheidungen weder die speziellen Eigenschaften der Verkehrsdaten noch der Unterschied von Massenüberwachung zu individueller Überwachung ausreichend berücksichtigt wurde, sah sich der EGMR zu einer ausführlichen Neubearbeitung veranlasst,[625] die hier allein thematisiert werden soll.

Bemerkenswert ist dabei zunächst, wie intensiv der EGMR sich mit den einzelnen Datenverarbeitungsschritten der Überwachung auseinandersetzt, und auf deren Verknüpfung eingeht.[626] Dabei stellt der Gerichtshof zunächst fest, welche einzelnen grundrechtsrelevanten Schritte sich bei der strategischen Überwachung identifizieren lassen (dazu auch oben Kap. B. I.2).[627]

Zunächst werden Kommunikationsinhalts- und Verkehrsdaten durch die Nachrichtendienste massenweise durch „Pakete" erhoben. In einem nächsten Schritt werden all diese Daten dann automatisiert auf bestimmte Suchbegriffe hin bzw. mit *umfassenden Abfragemechanismen* durchsucht. Im dritten Schritt werden die so erhobenen Daten von Analysten untersucht. Daran schließt sich eventuell ein vierter Schritt an: die tatsächliche Nutzung der Daten durch den Geheimdienst in Form von Berichten oder durch eine Weitergabe an andere Sicherheitsbehörden bzw. ausländische Dienste.

In diesem graduellen Prozess erkennt der EGMR eine fortschreitende Eingriffsintensivierung.[628] Während also die Datenerhebung und das erstmalige Aussortieren noch keine intensive Belastung herbeiführen, steigt

623 In der Fassung des Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28.10.1994, BGBl. I 1994, S. 3186; dazu auch BVerfGE 100, 313 – Strategische Fernmeldeaufklärung.

624 EGMR, Entsch. vom 29.06.2006, Nr.54934/00 (Weber u. Saravia/Deutschland) = NJW 2007, 1433; Urt. v. 01.07.2008 , Nr. 58243/00 (Linerty/Vereinigtes Königreich).

625 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 340 ff. = NVwZ-Beil. 2021, 11.

626 Idem, Rn. 324 ff.

627 Vgl. zum deutschen G-10 *Marxsen*, DÖV 2018, 218 (219 f.); *Papier*, NVwZ-Extra 15/2016, 1; *Schantz*, NVwZ 2015, 873 (874); *Bäcker*, K&R 2014, 556 (557).

628 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325. = NVwZ-Beil. 2021, 11.

die Intensität mit jedem weiteren Schritt. Entsprechend müssen die Sicherheitsvorkehrungen graduell angepasst werden. [629]

Bei der darauf aufbauenden Bewertung der Verhältnismäßigkeit trifft der EGMR zu Beginn eine prägnante Feststellung: Heimliche Massenüberwachung könnten zwar durchaus zum Schutz der nationalen Sicherheit geeignet und somit auch gerechtfertigt sein, gleichzeitig hätten sie aber das Potential, das ordnungsgemäße *Funktionieren demokratischer Prozesse unter dem Vorwand, sie zu verteidigen, zu unterminieren und sogar zu zerstören*.[630] Der EGMR betrachtet die Überwachung also nicht nur aus einer individuellgrundrechtlichen Perspektive, sondern aus einer abstrakten Perspektiven mit Bezügen zu demokratietheoretischen und rechtsstaatlichen Aspekten. Diese Perspektive drängt sich stärker als im Rahmen des GG oder der EU-GRC auch auf, denn Art. 8 Abs. 2 EMRK verlangt nicht nur allgemein eine Verhältnismäßigkeit von Eingriffen in die Privatheit, sondern deren Notwendigkeit *in einer demokratischen Gesellschaft*. Die eigentlich rechtsstaatlichen Elemente, die auch das BVerfG in seiner Perspektive berücksichtigt (siehe oben Kap. B. III. 2. c.), werden hier also vom Grundrechtstext unmittelbar eingefordert.

Dogmatisch sortiert der Gerichtshof die einzelnen Datenverarbeitungsschritte in unterschiedliche Problemkategorien ein. Die späteren Schritte, bei denen es tatsächlich zu einer relevanten Verarbeitung durch die Sicherheitsbehörden kommt, lassen sich wie die individuellen Überwachungsmaßnahmen ganz klassisch als intensive Eingriffe verstehen, da sie die Privatheit tatsächlich einschränken. Die frühen Stadien von Massenüberwachungsmaßnahmen sind aus anderen Gründen problematisch, weil sie demokratische bzw. rechtsstaatliche Prinzipien gefährden.

Dass die Schritte nicht losgelöst voneinander betrachtet werden können, stellt der EGMR anhand der Missbrauchsmöglichkeiten fest. Da in der graduellen Betrachtung mit der steigenden Intensität höhere Vorkehrungen einhergehen, darf nicht schon auf Ebene der Massenüberwachung eine individuelle Überwachung stattfinden, um diese Vorkehrungen zu umgehen. Suchkriterien, die eine individuelle Überwachung ermöglichen würden (etwa spezifische Emailadressen), sind daher nicht zulässig.[631] Es bedarf insofern auf dieser Ebene vor allem einer typisierten Kontrolle der Selektoren durch eine unabhängige Stelle.[632] Überhaupt ist die Kontrolle durch

629 Idem, Rn. 330, 347.
630 Idem, Rn. 339.
631 Idem, Rn. 348 ff.
632 Idem, Rn. 350 ff.

eine unabhängige Stelle in formeller Hinsicht für sämtliche Schritte der Massenüberwachung notwendig.

Darüber hinaus muss die gesetzliche Ermächtigung auch in materieller Hinsicht regeln: „*1.) die Gründe, aus denen die Massenüberwachung genehmigt werden kann, 2.) die Umstände, unter denen die Kommunikationen eines Einzelnen überwacht werden können, 3.) das Verfahren, das bei der Genehmigung einzuhalten ist, 4.) das Verfahren bei der Auswahl, Auswertung, und Verwendung des abgefangenen Materials, 5.) die Vorsichtsmaßnahmen, die bei Weitergabe des Materials an andere zu treffen sind, 6.) die zeitliche Begrenzung der Überwachung und Speicherung des erhobenen Materials sowie die Umstände, unter denen dieses Material gelöscht und vernichtet werden muss, 7.) das Verfahren und die Einzelheiten der Überwachung durch eine unabhängige Stelle, ob die genannten Garantien beachtetet wurden, und die Befugnis dieser Stelle, bei Verstößen zu entscheiden und 8.) das Verfahren für eine unabhängige, nachträgliche Kontrolle der Einhaltung dieser Garantien und die Befugnis der zuständigen Stelle zu entscheiden, wenn das nicht der Fall war.*“[633]

Diese Regeln gelten für die nachrichtendienstliche Verarbeitung von sowohl Inhalts- als auch Verkehrsdaten[634], wobei der EGMR sich nicht dazu verhält, wie eine Speicherung von Verkehrsdaten (nur) bei den Privatunternehmen zu bewerten wäre.

Die Einhaltung der vage umschriebenen Anforderungen prüfte der EGMR anhand der britischen und schwedischen Regelungen negativ und kasuistisch, machte also nur auf einzelne Mängel aufmerksam, anstatt konkrete Regeln positiv zu formulieren.[635]

### 5. Zusammenfassung

Resümierend lässt sich also feststellen, dass der EGMR gegenüber staatlicher Überwachung eine ähnliche „Ja-Aber-Haltung“[636] eingenommen hat wie das BVerfG. Soweit die Ermächtigungsgrundlagen hinreichend bestimmt sind und Regeln enthalten, die ausreichend von einer missbräuchlichen Verwendung der Überwachungsmaßnahmen schützen, steht Art. 8

633 Idem, Rn. 361.
634 Idem, Rn. 363 f.
635 Übersichtlich *B. Huber*, NVwZ-Beilage 2021, 3.
636 *Ibel* ZD-Aktuell 2021, 5246.

Abs. 2 EMRK selbst einer universellen Überwachung der (Auslands-)Kommunikation nicht entgegen.[637]

Die Herangehensweise des Gerichtshofs fällt jedoch kasuistischer aus. Konkrete Anforderungen in Form von „Handlungsanweisungen" ergeben sich nur dann, wenn der Gerichtshof Mängel der geprüften Normen konkret feststellt. Eine immer weiter ausdifferenzierte Je-Desto-Formel wie jene des BVerfG, die sich letztlich zu einer nuancierten *Handlungsanweisung*[638] entwickelt hat, findet sich in der Rechtsprechung des EGMR nicht.

Auch in dogmatischer Hinsicht zeigt sich dessen Rechtsprechung als wenig komplex. Anstatt über einen Katalog theoretisch fragwürdiger Intensitätsmerkmale die Eingriffsschwere von Überwachungsmaßnahmen zu bestimmen, stellt der Gerichtshof primär auf die tatsächliche Beschränkung der Privatheit ab und sieht diese bei Massenüberwachungen erst in den Stadien, die eine relevante Verwendung der individuellen Daten vorsehen, als verletzt an,[639] wenngleich er konsequent in jedem Datenverarbeitungsschritt einen Grundrechtseingriff erkennt[640]. Die graduelle Bewertung dieser Schritte erfolgt dann, ausgehend von Art. 8 Abs. 2 EMRK, dergestalt, dass bei den frühen Stadien rechtsstaatliche Erwägungen in den Vordergrund gerückt und entsprechende Verfahrensgarantien gefordert werden, die eine Umgehung der strengen Voraussetzungen individueller Überwachung verhindern.[641]

Aus der Rechtsprechung des EGMR ergeben sich für die Bewertung von Überwachungsmaßnahmen in Hinsicht auf Finanzdaten also nicht unbedingt konkrete Anforderungen an Speicherpflichten und Zugangsrechte, jedoch folgt aus ihr, dass Überwachungsmaßnahmen strukturell betrachtet werden müssen. Die Speicherung, Analyse und Weiterleitung von Daten

637 Vgl. Jüngst EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 334 ff. = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden), Rn. 248 ff. = NVwZ-Beil. 2021, 30

638 Insofern krit. *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (66 ff.); *Wolff*, ZG 2016, 361 (366 f.).

639 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325 ff. ff. = NVwZ-Beil. 2021, 11

640 EGMR, Urt. v. 26.03.1987, Nr. 9248/81 (Leander/Schweden), Rn. 84; Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 69.

641 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 348 ff. = NVwZ-Beil. 2021, 11

sind nicht nur individuell, sondern mit Rücksicht auf deren Synergieeffekte zu bewerten.