Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage

GRCh Art. 7, 8, 11, 52 I; RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) Art. 15 I; VO (EU) Nr. 2016/679 Art. 23 I

Der EuGH bekräftigt mit dieser Entscheidung seine generelle Ablehnung zur nicht anlassbezogenen Vorratsdatenspeicherung. Eine Ausnahme könne aber erlaubt sein, wenn eine konkrete und erhebliche Gefahr für die öffentliche Sicherheit bestehe, so der EuGH in der Urteilsbegründung.

Tenor des Gerichts:

1. Art. 15 I RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 I genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 I RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta der Grundrechte Rechtsvorschriften nicht entgegen, die

> –es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;
>
> –zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;
>
> –zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und

unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

–zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

–es zur Bekämpfung schwerer Kriminalität und, a fortiori, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen

gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

2. Art. 15 I RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, zum einen eine automatisierte Analyse sowie eine Erhebung in Echtzeit insbesondere von Verkehrs- und Standortdaten und zum anderen eine Erhebung in Echtzeit der technischen Daten zum Standort der verwendeten Endgeräte vorzunehmen, sofern

–der Rückgriff auf die automatisierte Analyse auf Situationen beschränkt ist, in denen sich ein Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, und Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer die fragliche Maßnahme rechtfertigenden Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und

–der Rückgriff auf die Erhebung von Verkehrs- und Standortdaten in Echtzeit auf Personen beschränkt ist, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind, und einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, deren Entscheidung bindend ist, wobei dieses Gericht oder diese Stelle sich vergewissern muss, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen.

3. Die RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") ist dahin auszulegen, dass sie im Bereich des

Schutzes der Vertraulichkeit der Kommunikation sowie des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Dienste der Informationsgesellschaft nicht anwendbar ist; dieser Schutz ist entweder durch die RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung oder durch die VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung RL 95/46 geregelt. Art. 23 I der VO (EU) Nr. 2016/679 ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

4. Ein nationales Gericht darf eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste ua zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 I RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta der Grundrechte rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 I der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.

EuGH (Große Kammer), Urteil vom 6.10.2020 – C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua/Premier ministre ua)

Zum Sachverhalt:

Das Urteil betrifft die Auslegung von Art. 15 I RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002 L 201, 37; im Folgenden: RL 2002/58) in der durch die RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 (ABl. 2009 L 337, 11) geänderten Fassung (im Folgenden: RL 2009/136) sowie der Art. 12-15 RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. 2000 L 178, 1; im Folgenden: RL 2000/31) im Licht der Art.

4, 6-8 und 11 sowie von Art. 52 I der Charta der Grundrechte der Europäischen Union (im Folgenden: GRCh) und von Art. 4 II EUV.

Die Ersuchen in den Rechtssachen sind im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 2-4.

Rechtssache C-511/18

Mit Klageschriften, die am 30.11.2015 und am 16.3.2016 eingingen und im Ausgangsverfahren verbunden wurden, haben La Quadrature du Net, das French Data Network und die Fédération des fournisseurs d'accès à Internet associatifs sowie Igwan.net beim *Conseil d'État* (Staatsrat, Frankreich) Klagen auf Nichtigerklärung der Dekrete Nr. 2015-1185, 2015-1211, 2015-1639 und 2016-67 erhoben. (Die Begründung der Klage ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 56-57.)

In Bezug auf den Klagegrund des Verstoßes gegen die RL 2002/58 führt das vorlegende Gericht aus, wie insbesondere aus den Bestimmungen dieser Richtlinie und aus dem Urteil v. 21.12.2016 (*EuGH* ECLI:EU:C:2016:970 = NJW 2017, 717 – Tele2 Sverige und Watson ua [C-203/15 u. C-698/15]; im Folgenden: Urteil Tele2) hervorgehe, dass nationale Bestimmungen, die den Betreibern elektronischer Kommunikationsdienste Pflichten wie die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten ihrer Nutzer und Teilnehmer zu den in Art. 15 I der Richtlinie genannten Zwecken, zu denen der Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit gehöre, auferlegten, in den Geltungsbereich der Richtlinie fielen, soweit diese Regelungen die Tätigkeit der genannten Betreiber regelten. Das Gleiche gelte für Regelungen des Zugangs nationaler Behörden zu diesen Daten und ihrer Nutzung. Folglich fielen in den Geltungsbereich RL 2002/58 sowohl die Speicherungspflicht, die sich aus Art. L. 851-1 des CSI ergebe, als auch der in den Art. L. 851-1, L. 851-2 und L. 851-4 des CSI vorgesehene behördliche Zugang zu den Daten, einschließlich des Echtzeit-Zugangs. Das Gleiche gelte für die Bestimmungen von Art. L. 851-3 des CSI, die den Betreibern zwar keine allgemeine Speicherungspflicht auferlegten, sie aber verpflichte-

ten, in ihren Netzen automatisierte Verarbeitungen vorzunehmen, die dazu dienten, Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen könnten. Die in den Nichtigkeitsklagen angeführten Bestimmungen des CSI über Techniken zur Sammlung von Informationen, die unmittelbar vom Staat umgesetzt würden, ohne die Tätigkeiten der Betreiber elektronischer Kommunikationsdienste zu regeln und ihnen spezielle Pflichten aufzuerlegen, fielen dagegen nicht in den Geltungsbereich RL 2002/58. In ihnen könne keine Umsetzung des Unionsrechts gesehen werden, so dass nicht mit Erfolg gerügt werden könne, dass sie gegen diese Richtlinie verstießen. (Die Einschätzung des Gerichts betreffend die Rechtmäßigkeit der Dekrete Nr. 2015-1185, 2015-1211, 2015-1639 und 2016-67 ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 61-66.)

Die Ausführungen zu den Verfahrensgarantien sind im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 67.

Unter diesen Umständen hat der *Conseil d'État* (Staatsrat) das Verfahren ausgesetzt und dem *EuGH* seine Fragen zur Vorabentscheidung vorgelegt.

Rechtssache C-512/18

Mit Klageschrift, die am 1.9.2015 einging, haben das French Data Network, La Quadrature du Net und die Fédération des fournisseurs d'accès à Internet associatifs beim *Conseil d'État* Klage auf Nichtigerklärung der aus dem Schweigen des Premierministers auf ihren Antrag, Art. Rn. 10-13 des CPCE und das Dekret Nr. 2011-219 ua wegen Verstoßes gegen Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 der GRCh aufzuheben, resultierenden stillschweigenden ablehnenden Entscheidung für nichtig zu erklären, erhoben. Privacy International und das Center for Democracy and Technology sind im Ausgangsverfahren als Streithelfer zugelassen worden. Zu Art. Rn. 10-13 des CPCE und der darin vorgesehenen Pflicht zur allgemeinen und unterschiedslosen Speicherung von Kommunikationsdaten führt das vorlegende Gericht mit ähnlichen Erwägungen wie in der Rs. C-511/18 aus, eine solche Speicherung verschaffe der Justizbehörde Zugriff auf Daten über Kommunikationen, die ein Einzelner getätigt habe, bevor er in den Verdacht geraten sei, eine Straftat begangen zu haben; sie biete daher einen einzigartigen Nutzen für die Ermittlung, Feststellung und Verfolgung von Straftaten.

Zum Dekret Nr. 2011-219 stellt das vorlegende Gericht fest, Abschn. II von Art. 6 der LCEN, der eine Pflicht zur Erhebung und Speicherung allein der die Schaffung von Inhalten betreffenden Daten vorsehe, falle nicht in den Geltungsbereich RL 2002/58, der sich nach deren Art. 3 I auf die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union beschränke, sondern in den Geltungsbereich RL 2000/31. Wie sich aus Art. 15 I und 2 RL 2000/31 ergebe, enthalte sie aber kein grundsätzliches Verbot, die Schaffung von Inhalten betreffende Daten zu speichern, von dem nur ausnahmsweise abgewichen werden könnte. Somit stelle sich die Frage, ob die Art. 12, 14 und 15 dieser Richtlinie im Licht der Art. 6-8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen seien, dass sie es einem Mitgliedstaat gestatteten, eine nationale Regelung wie Art. 6 Abschn. II der LCEN einzuführen, mit der die Betroffenen verpflichtet würden, Daten so zu speichern, dass jede Person, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen habe, identifiziert werden könne, damit die Justizbehörde gegebenenfalls ihre Übermittlung verlangen könne, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen. Unter diesen Umständen hat der *Conseil d'État* das Verfahren ausgesetzt und dem *EuGH* seine Fragen zur Vorabentscheidung vorgelegt.

Rechtssache C-520/18

Mit Klageschriften, die am 10., 16., 17. und 18.1.2017 eingingen und im Ausgangsverfahren verbunden wurden, haben der Ordre des barreaux francophones et germanophone, die Académie Fiscale ASBL, UA, die Liga voor Mensenrechten ASBL und die Ligue des Droits de l'Homme ASBL sowie *VZ*, *WY* und *XX* bei der *Cour constitutionnelle* (Verfassungsgerichtshof, Belgien) Klagen auf Nichtigerklärung des Gesetzes vom 29.5.2016 wegen Verstoßes gegen die Art. 10 und 11 der belgischen Verfassung iVm den Art. 5, 6-11, 14, 15, 17 und 18 der EMRK, den Art. 7, 8, 11 und 47 sowie von Art. 52 I der GRCh Art. 17 des von der Generalversammlung der Vereinten Nationen am 16.12.1966 angenommenen und am 23.3.1976 in Kraft getretenen Internationalen Pakts über bürgerliche und politische Rechte, der

allgemeinen Grundsätze der Rechtssicherheit, der Verhältnismäßigkeit und der informationellen Selbstbestimmung sowie von Art. 5 IV EUV erhoben.

Der Vortrag der Kl. des Ausgangsverfahrens ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 75-79.

Unter diesen Umständen hat der *Verfassungsgerichtshof* das Verfahren ausgesetzt und dem *EuGH* seine Fragen zur Vorabentscheidung vorgelegt.

Der *EuGH* hat nach Anhörung des Generalanwalts *Campos Sánchez-Bordona* (ECLI:EU:C:2020:6 = BeckRS 2020, 56) wie aus dem Tenor ersichtlich entschieden.

Aus den Gründen:

Zu den Vorlagefragen

Zur ersten Frage in den Rs. C-511/18 und C-512/18 sowie zur ersten und zur zweiten Frage in der Rs. C-520/18

81Mit der ersten Frage in den Rs. C-511/18 u. C-512/18 sowie der ersten und der zweiten Frage in der Rs. C-520/18, die zusammen zu prüfen sind, möchten die vorlegenden Gerichte wissen, ob Art. 15 I RL 2002/58 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die die Betreiber elektronischer Kommunikationsdienste zu den in Art. 15 I genannten Zwecken zur allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet.

Vorbemerkungen

82– 86(*Die Vorbemerkungen sind im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 82-86.*)

Zum Geltungsbereich RL 2002/58

87La Quadrature du Net, die Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International und das Center for Democracy and Technology tragen im Wesentlichen, insoweit gestützt auf die Rechtsprechung des *EuGH* zum Geltungsbereich der RL 2002/58, vor, sowohl die Vorratsspeicherung der Daten als auch der Zugang zu den gespeicherten Daten fielen in den Geltungsbereich der Richtlinie, unabhängig davon, ob der Zugang in Echtzeit erfolge oder nicht. Da das Ziel des Schutzes der nationalen Sicherheit in Art. 15 I der Richtlinie ausdrücklich erwähnt werde, führe seine Verfolgung nämlich nicht zu ihrer Unanwendbarkeit. Der von den vorlegenden Gerichten angesprochene Art. 4 II EUV ändere daran nichts.

88Zu den nachrichtendienstlichen Maßnahmen, die von den zuständigen französischen Behörden unmittelbar umgesetzt werden, ohne die Tätigkeit der Betreiber elektronischer Kommunikationsdienste durch die Auferlegung spezifischer Verpflichtungen zu regeln, führt das Center for Democracy and Technology aus, diese Maßnahmen fielen notwendigerweise in den Geltungsbereich der RL 2002/58 und der Charta, da sie Ausnahmen von dem durch Art. 5 der Richtlinie garantierten Grundsatz der Vertraulichkeit darstellten. Derartige Maßnahmen müssten somit den Anforderungen von Art. 15 I der Richtlinie genügen.

89Die französische, die tschechische und die estnische Regierung, Irland, die zyprische, die ungarische, die polnische und die schwedische Regierung sowie die Regierung des Vereinigten Königreichs machen hingegen im Wesentlichen geltend, die RL 2002/58 gelte nicht für nationale Regelungen wie die in den Ausgangsverfahren in Rede

stehenden, da sie auf den Schutz der nationalen Sicherheit abzielten. Die zur Aufrechterhaltung der öffentlichen Ordnung sowie zum Schutz der inneren Sicherheit und der Integrität des Hoheitsgebiets dienenden Tätigkeiten der Nachrichtendienste gehörten zu den grundlegenden Funktionen der Mitgliedstaaten und fielen deshalb in ihre alleinige Zuständigkeit, wie insbesondere Art. 4 II 3 EUV zeige.

90 Diese Regierungen sowie Irland verweisen überdies auf Art. 1 III der RL 2002/58, wonach Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates von ihrem Geltungsbereich ausgeschlossen seien, wie es bereits bei der RL 95/46 nach deren Art. 3 II erster Gedankenstrich der Fall gewesen sei. Sie stützen sich dabei auf die Auslegung der letztgenannten Bestimmung im Urteil vom 30.5.2006 (*EuGH* ECLI:EU:C:2006:346 = EuZW 2006, 403 – Parlament ua/Rat und Kommission ua. [C-317/04, C-318/04]).

EuGH: Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage(EuZW 2021, 209) 212

91 Hierzu ist festzustellen, dass die RL 2002/58 nach ihrem Art. 1 I ua eine Harmonisierung der Vorschriften der Mitgliedstaaten vorsieht, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation zu gewährleisten.

92 Nach Art. 1 III der RL 2002/58 sind von ihrem Geltungsbereich die „Tätigkeiten des Staates" in den dort vorgesehenen Bereichen ausgeschlossen, zu denen die Tätigkeiten des Staates im strafrechtlichen Bereich sowie die Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt, gehören. Die dort beispielhaft aufgeführten Tätigkeiten sind allesamt spezifische Tätigkeiten der Staaten oder staatlicher Stellen, die nichts mit den Tätigkeitsbereichen von Privatpersonen zu tun haben (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 32 mwN – Ministerio Fiscal [C-207/16]).

93 Nach Art. 3 der RL 2002/58 gilt sie für die Verarbeitung personenbezogener Daten iVm der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen (im Folgenden: elektronische Kommunikationsdienste). Folglich ist davon auszugehen, dass diese Richtlinie die Tätigkeiten der Betreiber solcher Dienste regelt (*EuGH* EGLI:EU:C:2018:788 = NJW 2019, 655 Rn. 33 mwN – Ministerio Fiscal).

94 In diesem Rahmen können die Mitgliedstaaten nach Art. 15 I der RL 2002/58 unter den dort angegebenen Voraussetzungen „Rechtsvorschriften erlassen, die die Rechte und Pflichten gem. Art. 5, 6, 8 I-IV sowie Art. 9 dieser Richtlinie beschränken" (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 71 – Tele2 [C-203/15, C-698/15]).

95 Art. 15 I der RL 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Rechtsvorschriften in den Geltungsbereich der Richtlinie fallen, da sie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die in dieser Bestimmung vorgesehenen Voraussetzungen eingehalten werden. Außerdem regeln diese Rechtsvorschriften – zu den in dieser Bestimmung genannten

Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 34 – Ministerio Fiscal).

96 Vor allem anhand dieser Erwägungen ist der *EuGH* zu dem Schluss gelangt, dass Art. 15 I der RL 2002/58 in Verbindung mit ihrem Art. 3 dahin auszulegen ist, dass in den Geltungsbereich der Richtlinie nicht nur eine Rechtsvorschrift fällt, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, die Verkehrs- und Standortdaten zu speichern, sondern auch eine Rechtsvorschrift, die ihnen vorschreibt, den zuständigen nationalen Behörden Zugang zu diesen Daten zu gewähren. Solche Vorschriften haben nämlich zwangsläufig eine Verarbeitung der betreffenden Daten durch die Betreiber zur Folge und können, da sie die Tätigkeiten dieser Betreiber regeln, den in Art. 1 III der Richtlinie genannten spezifischen Tätigkeiten der Staaten nicht gleichgestellt werden (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 37 mwN – Ministerio Fiscal).

97 Außerdem würde in Anbetracht der Erwägungen in Rn. 95 des vorliegenden Urteils und der Systematik der RL 2002/58 eine Auslegung, wonach die Rechtsvorschriften, auf die sich ihr Art. 15 I bezieht, von ihrem Geltungsbereich ausgeschlossen sind, weil sich die Zweckbestimmungen, denen solche Rechtsvorschriften entsprechen müssen, im Wesentlichen mit den Zielen decken, die mit den in Art. 1 III der Richtlinie genannten Tätigkeiten verfolgt werden, Art. 15 I jede praktische Wirksamkeit nehmen (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 72 u. 73 – Tele2).

98 Der Begriff „Tätigkeiten" in Art. 1 III der RL 2002/58 kann daher, wie der Generalanwalt in Rn. 75 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net ua (*EuGH* ECLI:EU:C:2020:6 = BeckRS 2020, 25511 – La Quadrature du Net ua [C-511/18 u. C-512/18]) im Wesentlichen ausgeführt hat, nicht so ausgelegt werden, dass er sich auf die Rechtsvorschriften iSv Art. 15 I der Richtlinie erstreckt.

99 Die Bestimmungen von Art. 4 II EUV, auf die die in Rn. 89 des vorliegenden Urteils genannten Regierungen Bezug nehmen, können diese Auslegung nicht in Frage stellen. Denn nach ständiger Rechtsprechung des *EuGH* ist es zwar Sache der Mitgliedstaaten, ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um ihre innere und äußere Sicherheit zu gewährleisten, doch kann die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht zur Unanwendbarkeit des Unionsrechts führen und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbinden (*EuGH* ECLI:EU:C:2013:363 = NVwZ 2013, 3807 Rn. 38 – ZZ [C-300/11], *EuGH* ECLI:EU:C:2018:194 = NZBau 2018, 478 Rn. 75 u. 76 – Kommission/Österreich [Staatsdruckerei] [C-187/16], sowie *EuGH* ECLI:EU:C:2020:257 = NJW 2020,1729 Rn. 143 u. 170 – Kommission/Republik Polen ua [C-715/17 ua]).

100 Es trifft zu, dass der *EuGH* im Urteil vom 30.5.2006 (*EuGH* ECLI:EU:C:2006:346 = EuZW 2006, 403 Rn. 56-59 – Parlament ua/Rat und Kommission ua) entschieden hat, dass die Übermittlung personenbezogener Daten durch Fluggesellschaften an die Behörden eines Drittstaats zur Verhütung und Bekämpfung des Terrorismus und anderer schwerer Straftaten nach Art. 3 II erster Gedankenstrich der RL 95/46 nicht in deren Anwendungsbereich fiel, weil sie in einem von staatlichen Stellen geschaffenen Rahmen stattfand und der öffentlichen Sicherheit diente.

101 Angesichts der Erwägungen in den Rn. 93, 95 und 96 des vorliegenden Urteils ist diese Rechtsprechung jedoch nicht auf die Auslegung von Art. 1 III der RL 2002/58 übertragbar. Wie der Generalanwalt in den Rn. 70-72 seiner Schlussanträge in den verbundenen Rechtssachen La Quadrature du Net ua (GA *Campos Sánchez-Bordona* Schlussanträge v. 15.01.2020, ECLI:EU:C:2020:6 = BeckRS 2020, 56) im Wesentlichen ausgeführt hat, nahm Art. 3 II erster Gedankenstrich der RL 95/46, auf den sich die genannte Rechtsprechung bezieht, nämlich „Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung [und] die Sicherheit des Staates" generell vom Anwendungsbereich dieser Richtlinie aus, ohne anhand des Urhebers der betreffenden Verarbeitung von Daten zu unterscheiden. Dagegen erweist sich eine solche Unterscheidung im Rahmen der Auslegung von Art. 1 III der RL 2002/58 als erforderlich. Wie aus den Rn. 94 bis 97 des vorliegenden Urteils hervorgeht, fallen alle Verarbeitungen personenbezogener Daten durch Betreiber elektronischer Kommunikationsdienste nämlich in ihren Geltungsbereich, einschließlich Verarbeitungen aufgrund von Verpflichtungen, die ihnen von den Behörden auferlegt wurden. Die letztgenannten Verarbeitungen konnten hingegen gegebenenfalls unter die in Art. 3 II erster Gedankenstrich der RL 95/46 vorgesehene Ausnahme fallen, da diese Bestimmung weiter gefasst ist und sich auf alle die öffentliche Sicherheit, die Landesverteidigung oder die Sicherheit des Staates betreffenden Verarbeitungen erstreckt, unabhängig von ihrem Urheber.

102 Überdies ist festzustellen, dass die RL 95/46, um die es in der Rechtssache ging, in der das Urteil vom 30.5.2006 (*EuGH* ECLI:EU:C:2006:346-

= EuZW 2006, 403 – Parlament ua/Rat und Kommission ua) ergangen ist, gem. Art. 94 I der VO 2016/679 mit Wirkung vom 25.5.2018 durch diese aufgehoben und ersetzt wurde. Die Verordnung findet zwar nach ihrem Art. 2 II Buchst. d keine Anwendung auf Verarbeitungen „durch die zuständigen Behörden" ua zum Zweck der Verhütung und Feststellung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Wie aus Art. 23 I Buchst. d und h der Verordnung hervorgeht, fallen aber Verarbeitungen personenbezogener Daten, die zu diesem Zweck von Privatpersonen vorgenommen werden, in ihren Anwendungsbereich. Daraus folgt, dass die vorstehende Auslegung von Art. 1 III, Art. 3 und Art. 15 I der RL 2002/58 im Einklang mit der Abgrenzung des Anwendungsbereichs der VO Nr. 2016/679 steht, die diese Richtlinie ergänzt und präzisiert.

103 Wenn die Mitgliedstaaten unmittelbar Maßnahmen umsetzen, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen, fällt der Schutz der Daten der Betroffenen hingegen nicht unter die RL 2002/58, sondern allein unter das nationale Recht, vorbehaltlich der Anwendung der RL (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 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), so

dass die fraglichen Maßnahmen insbesondere mit nationalem Recht von Verfassungsrang und den Anforderungen der EMRK im Einklang stehen müssen.

104 Aus den vorstehenden Erwägungen folgt, dass eine nationale Regelung, die wie die in den Ausgangsverfahren in Rede stehenden die Betreiber elektronischer Kommunikationsdienste zum Schutz der nationalen Sicherheit und zur Bekämpfung der Kriminalität zur Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet, in den Geltungsbereich der RL 2002/58 fällt.

Zur Auslegung von Art. 15 I RL 2002/58

105 Einleitend ist darauf hinzuweisen, dass nach ständiger Rechtsprechung bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen ist, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und insbesondere deren Entstehungsgeschichte (*EuGH* ECLI:EU:C:2018:257 = EuZW 2018, 381 Rn. 44 – Egenberger [C-414/16]).

106 Die RL 2002/58 soll, wie sich ua aus ihren Erwägungsgründen 6 u. 7 ergibt, die Nutzer elektronischer Kommunikationsdienste vor den Risiken für ihre personenbezogenen Daten und ihre Privatsphäre schützen, die sich aus den neuen Technologien und vor allem den zunehmenden Fähigkeiten zur automatisierten Speicherung und Verarbeitung von Daten ergeben. Insbesondere soll mit der Richtlinie nach ihrem zweiten Erwägungsgrund gewährleistet werden, dass die in den Art. 7 und 8 der GRCh niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM[2000] 385 endg.), aus dem die RL 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber sicherstellen wollte, „dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt".

107 Zu diesem Zweck wird in Art. 5 I RL 2002/58 der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt, der ua das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert.

108 Insbesondere ergibt sich hinsichtlich der Verarbeitung und Speicherung von Verkehrsdaten durch die Betreiber elektronischer Kommunikationsdienste aus Art. 6 sowie den Erwägungsgründen 22 u. 26 RL 2002/58, dass eine solche Verarbeitung nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums zulässig ist. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 I der Richtlinie nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 86 mwN – Tele2 [C-203/15, C-698/15]).

109 Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der GRCh verankerten Rechte konkretisiert, so dass die Nutzer elektronischer

Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt.

110 Art. 15 I RL 2002/58 gestattet es den Mitgliedstaaten jedoch, Ausnahmen von der in Art. 5 I der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, ua in den Art. 6 und 9 der Richtlinie genannten Pflichten zu schaffen, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten ua durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden.

111 Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 RL 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (vgl. idS *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 89 u. 104 – Tele2).

112 Hinsichtlich der Zwecke, die eine Beschränkung der insbesondere in den Art. 5, 6 und 9 RL 2002/58 vorgesehenen Rechte und Pflichten rechtfertigen können, hat der *EuGH* bereits entschieden, dass die Aufzählung der in Art. 15 I 1 der Richtlinie genannten Zwecke abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 52 mwN – Ministerio Fiscal).

EuGH: Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage(EuZW 2021, 209) 214

113 Außerdem geht aus Art. 15 I 3 RL 2002/58 hervor, dass die Mitgliedstaaten Rechtsvorschriften, die die Tragweite der Rechte und Pflichten gemäß den Art. 5, 6 und 9 dieser Richtlinie beschränken sollen, nur unter Beachtung der allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und der durch die Charta garantierten Grundrechte erlassen dürfen. Hierzu hat der *EuGH* bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der GRCh betreffen, sondern auch der in Art. 11 der GRCh gewährleisteten Freiheit der Meinungsäußerung (*EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 25 u. 70 – Digital Rights [C-293/12, C-594/12], sowie *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 91 u. 92 mwN – Tele2).

114 Bei der Auslegung von Art. 15 I RL 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der GRCh gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten,

wie sie sich aus der Rechtsprechung des *EuGH* ergibt, berücksichtigt werden sowie das in Art. 11 der GRCh gewährleistete Recht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (*EuGH* ECLI:EU:C:2001:127 = BeckRS 2001, 31031657 Rn. 39 – Connolly/Kommission [C-274/99], und *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 93 mwN – Tele2).

115 Insoweit ist darauf hinzuweisen, dass die Speicherung der Verkehrs- und Standortdaten als solche zum einen eine Abweichung von dem nach Art. 5 I RL 2002/58 für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten darstellt und zum anderen einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Art. 7 und 8 der GRCh verankert sind; dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben (vgl. idS *EuGH* ECLI:EU:C:2017:592 = BeckRS 2017, 123252 = ZD 2018, 23 Rn. 124 u. 126 mwN – Gutachten 1/15 [PNR-Abkommen EU-Kanada]; vgl. entspr., in Bezug auf Art. 8 der EMRK, *EGMR*, 30.1.2020, Breyer gegen Deutschland, ECLI:CE:ECHR:2020:0130JUD005000112 = ZD 2020, 250, § 81).

116 Irrelevant ist auch, ob die gespeicherten Daten in der Folge verwendet werden (vgl. entspr., in Bezug auf Art. 8 der EMRK, *EGMR*, 16.2.2000, Amann gegen Schweiz, ECLI:CE:ECHR:2000:0216JUD002779895, § 69, sowie 13.2.2020, Trjakovski und Chipovski gegen Nordmazedonien, ECLI:CE:ECHR:2020:0213JUD005320513 = BeckRS 2020, 1448, § 51), da der Zugriff auf solche Daten, unabhängig von ihrer späteren Verwendung, einen gesonderten Eingriff in die in der vorstehenden Rn. genannten Grundrechte darstellt (vgl. idS *EuGH* ECLI:EU:C:2017:592 = BeckRS 2017, 123252 = ZD 2018, 23 Rn. 124 u. 126 – Gutachten 1/15 [PNR-Abkommen EU-Kanada]).

117 Dieser Schluss erscheint umso gerechtfertigter, als die Verkehrs- und Standortdaten Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten können, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand, wobei solche Daten im Übrigen im Unionsrecht besonderen Schutz genießen. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren. Diese Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst (*EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 27 – Digital Rights, und *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 99 – Tele2).

118 Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken zum einen für sich genommen das in Art. 7 der GRCh verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der GRCh gewährleisteten Freiheit der Meinungsäußerung abhalten (*EuGH* ECLI:EU:C:2014:238 Rn. 28 – Digital

Rights, und *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 101 – Tele2). Solche abschreckenden Wirkungen können in besonderem Maß Personen treffen, deren Kommunikationen nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen, sowie Whistleblower, deren Aktivitäten durch die RL 2019/1937/EU des Europäischen Parlaments und des Rates vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. 2019 L 305, 17), geschützt werden. Außerdem sind diese Wirkungen umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind.

119 Zum anderen birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, Gefahren des Missbrauchs und des rechtswidrigen Zugangs.

120 In Art. 15 I RL 2002/58, der es den Mitgliedstaaten gestattet, die in Rn. 110 des vorliegenden Urteils angesprochenen Ausnahmen vorzusehen, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der GRCh verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen (*EuGH* ECLI:EU:C:2020:559 = EuZW 2020, 941 Rn. 172 mwN – Facebook Ireland und Schrems [C-311/18]).

121- 129 (*Weitere Ausführungen zu der Auslegung des Art. 15 I der RL 2002/58 im Zuge der GRCh sind im Volltext abrufbar unter BeckRS 2020, 2511 Rn. 121-129.*)

130 Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des *EuGH* verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Au-

ßerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird (*EuGH* ECLI:EU:C:2008:727 = EuZW 2009, 108 Rn. 56 – Satakunnan Markkinapörssi und Satamedia [C-73/07]; *EuGH* ECLI:EU:C:2010:662 = BeckRS 2010, 91284 Rn. 76, 77 u. 86 – Volker und Markus Schecke und Eifert [C-92/09, C-93/09], sowie *EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 52 – Digital Rights; *EuGH* ECLI:EU:C:2017:592 = BeckRS 2017, 123252 = ZD 2018, 23 Rn. 140 – Gutachten 1/15 [PNR-Abkommen EU-Kanada]).

131 Insbesondere geht aus der Rechtsprechung des *EuGH* hervor, dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der ua in den Art. 5, 6 und 9 RL 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, zu beurteilen ist, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 55 mwN – Ministerio Fiscal).

132 Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (*EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 54 u. 55 – Digital Rights, sowie *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2; *EuGH* ECLI:EU:C:2017:592 = ZD 2018, 23 Rn. 141 – Gutachten 1/15 [PNR-Abkommen EU-Kanada]).

133 Eine Regelung, die eine Vorratsspeicherung personenbezogener Daten vorsieht, muss daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (vgl. idS *EuGH* ECLI:EU:C:2017:592 = BeckRS 2017, 123252 = ZD 2018, 23 Rn. 191 mwN – Gutachten 1/15 [PNR-Abkommen EU-Kanada], sowie *EuGH* ECLI:EU:C:2019:823 = NVwZ-RR 2019, 1066 = BeckRS 2019, 23100 Rn. 63 – A ua [C-302/18]).

Zu den Rechtsvorschriften, die zum Schutz der nationalen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

134 Das von den vorlegenden Gerichten und den Regierungen, die Erklärungen abgegeben haben, angesprochene Ziel des Schutzes der nationalen Sicherheit ist vom *EuGH* in seinen Urteilen zur Auslegung RL 2002/58 noch nicht spezifisch geprüft worden.

135 Insoweit ist zunächst festzustellen, dass nach Art. 4 II EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.

136 Die Bedeutung des Ziels des Schutzes der nationalen Sicherheit übersteigt im Licht von Art. 4 II EUV die der übrigen von Art. 15 I RL 2002/58 erfassten Ziele, insbesondere der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen. Bedrohungen wie die in der vorstehenden Rn. genannten unterscheiden sich nämlich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 I der GRCh ist das Ziel des Schutzes der nationalen

Sicherheit daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten.

137 Somit steht Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh in Situationen wie den in den Rn. 135 u. 136 des vorliegenden Urteils beschriebenen einer Rechtsvorschrift, mit der den zuständigen Behörden gestattet wird, den Betreibern elektronischer Kommunikationsdienste aufzugeben, die Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel für begrenzte Zeit zu speichern, grundsätzlich nicht entgegen, sofern hinreichend konkrete Umstände die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit iSd Rn. 135 u. 136 des vorliegenden Urteils gegenübersieht. Auch wenn eine solche Maßnahme unterschiedslos alle Nutzer elektronischer Kommunikationsmittel erfasst, ohne dass *prima facie* ein Zusammenhang im Sinne der in Rn. 133 des vorliegenden Urteils angeführten Rechtsprechung zwischen ihnen und einer Bedrohung der nationalen Sicherheit dieses Mitgliedstaats zu bestehen scheint, ist gleichwohl davon auszugehen, dass das Vorliegen einer derartigen Bedrohung als solches geeignet ist, diesen Zusammenhang herzustellen.

138 Die Anordnung, die Daten aller Nutzer elektronischer Kommunikationsmittel präventiv auf Vorrat zu speichern, muss jedoch in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden. Zwar kann nicht ausgeschlossen werden, dass die an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung, Daten auf Vorrat zu speichern, wegen des Fortbestands einer solchen Bedrohung verlängert werden kann, doch darf die Laufzeit jeder Anordnung einen absehbaren Zeitraum nicht überschreiten. Überdies muss eine solche Vorratsdatenspeicherung Beschränkungen unterliegen und mit strengen Garantien verbunden sein, die einen wirksamen Schutz der personenbezogenen Daten der Betroffenen vor Missbrauchsrisi-

ken ermöglichen. Die Speicherung darf somit keinen systematischen Charakter haben.

139 Angesichts der Schwere des aus einer solchen allgemeinen und unterschiedslosen Speicherung resultierenden Eingriffs in die Grundrechte, die in den Art. 7 und 8 der GRCh verankert sind, muss gewährleistet sein, dass darauf tatsächlich nur in Situationen wie den in den Rn. 135 und 136 des vorliegenden Urteils angesprochenen zurückgegriffen wird, in denen eine ernste Bedrohung für die nationale Sicherheit besteht. Dabei ist es unabdingbar, dass eine an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung einer solchen Vorratsdatenspeicherung Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist, sein kann, mit der das Vorliegen einer dieser Situationen sowie die Beachtung der vorzusehenden Bedingungen und Garantien geprüft werden.

Zu den Rechtsvorschriften, die zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

140 Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, sind im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte, die in den Art. 7 und 8 der GRCh verankert sind, zu rechtfertigen. Daher können nur Eingriffe in die genannten Grundrechte, die nicht schwer sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 102 – Tele2; *EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 56 u. 57 – Ministerio Fiscal; *EuGH* ECLI:EU:C:2017:592 = BeckRS 2017, 123252 = ZD 2018, 23 Rn. 149 – Gutachten 1/15 [PNR-Abkommen EU-Kanada]).

141 Eine nationale Regelung, die zur Bekämpfung schwerer Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, überschreitet die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh verlangt (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 107 – Tele2).

142 Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 118 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in den Art. 7 und 11 der GRCh verankerten Grundrechte haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in einer demokratischen Gesellschaft, wie es das durch die RL 2002/58 geschaffene System vorsieht, die Ausnahme und nicht die Regel sein, und solche Daten dürfen nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein. Dies gilt auch in Anbetracht der Ziele der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit sowie der Bedeutung, die ihnen beizumessen ist.

143 Außerdem hat der *EuGH* hervorgehoben, dass eine Regelung, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, die elektronischen Kommunikationen fast der gesamten Bevölkerung erfasst, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels. Eine solche Regelung betrifft entgegen dem in Rn. 133 des vorliegenden Urteils angesprochenen Erfordernis pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit voraus (*EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 57 u. 58 – Digital Rights, sowie *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 105 – Tele2).

144 Insbesondere beschränkt eine solche Regelung, wie der *EuGH* bereits entschieden hat, die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung schwerer Kriminalität beitragen könnten (*EuGH* ECLI:EU:C:2014:238 = BeckRS 2014, 80686 Rn. 59 – Digital Rights und *EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 106 – Tele2).

145 Selbst die positiven Verpflichtungen, die sich, je nach Fall, für die Mitgliedstaaten aus den Art. 3, 4 und 7 der GRCh ergeben können und, wie in den Rn. 126 u. 128 des vorliegenden Urteils ausgeführt worden ist, die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen, können aber keine so schwerwiegenden Eingriffe rechtfertigen, wie sie mit einer Regelung, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, für die in den Art. 7 und 8 der GRCh verankerten Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen.

146 Hingegen können nach den Ausführungen in den Rn. 142-144 des vorliegenden Urteils und angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, die Ziele der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Beeinträchtigungen der öffentlichen Sicherheit und erst recht des Schutzes der nationalen Sicherheit in Anbetracht ihrer Bedeutung im Hinblick auf die in der vorstehenden Rn. angesprochenen positiven Verpflichtungen, auf die insbesondere der Verfassungsgerichtshof abgestellt hat, den mit einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten verbundenen besonders schwerwiegenden Eingriff rechtfertigen.

147 Wie der *EuGH* bereits entschieden hat, untersagt Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh es einem Mitgliedstaat somit nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sowie zum Schutz der nationalen Sicherheit präventiv eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern ihre Speiche-

rung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 108 – Tele2).

148 Die erforderliche Begrenzung einer solchen Vorratsdatenspeicherung kann insbesondere anhand der Kategorien betroffener Personen vorgenommen werden, da Art. 15 I RL 2002/58 einer auf objektiven Kriterien beruhenden Regelung nicht entgegensteht, mit der Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 111 – Tele2).

149– 157(*Die Ausführungen des EuGH bzgl. der Kriterien für die zu erfassenden Personen, sowie die Begrenzung der Vorratsdatenspeicherung unter Zugrundelegung des Grundsatzes der Verhältnismäßigkeit sind im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 149-157.*)

158 Daraus ergibt sich im Einklang mit den Ausführungen in Rn. 140 des vorliegenden Urteils, dass Rechtsvorschriften, die auf die Verarbeitung dieser Daten als solcher, insbesondere auf ihre Speicherung und den Zugang zu ihnen zum alleinigen Zweck der Identifizierung des betreffenden Nutzers abzielen, ohne dass die Daten mit Informationen über die erfolgten Kommunikationen in Verbindung gebracht werden können, durch den in Art. 15 I 1 RL 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein können (*EuGH* ECLI:EU:C:2018:788 = NJW 2019, 655 Rn. 62 – Ministerio Fiscal).

159 Unter diesen Umständen ist angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, aus den in den Rn. 131 u. 158 des vorliegenden Urteils genannten Gründen davon auszugehen, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh, auch wenn es keine Verbindung zwischen der Gesamtheit der Nutzer elektronischer Kommunikationsmittel und den verfolgten Zielen gibt, einer Rechtsvorschrift nicht entgegensteht, die den Betreibern elektronischer Kommunikationsdienste ohne besondere Frist auferlegt, zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der öffentlichen Sicherheit Daten über die Identität aller Nutzer elektronischer Kommunikationsmittel auf Vorrat zu speichern, ohne dass es sich um schwere Straftaten, Bedrohungen oder Beeinträchtigungen der öffentlichen Sicherheit handeln muss.

Zu den Rechtsvorschriften, die zur Bekämpfung schwerer Kriminalität eine umgehende Sicherung von Verkehrs- und Standortdaten vorsehen

160 Die von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 RL 2002/58 oder auf der Grundlage von Rechtsvorschriften der in den Rn. 134-159 des vorliegenden Urteils beschriebenen Art, die gem. Art. 15 I der Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten müssen grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, entweder gelöscht oder anonymisiert werden.

161Während dieser Verarbeitung und Speicherung können jedoch Situationen auftreten, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über diese Fristen hinaus zu speichern, und zwar sowohl dann, wenn die Taten oder Beeinträchtigungen bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht besteht, dass sie vorliegen.

162 Insoweit ist darauf hinzuweisen, dass das von den 27 Mitgliedstaaten unterzeichnete und von 25 von ihnen ratifizierte Übereinkommen des Europarats vom 23.11.2001 über Computerkriminalität (Sammlung Europäischer Verträge – Nr. 185), das die Bekämpfung von Straftaten, die mittels Rechnernetzen begangen wurden, erleichtern soll, in Art. 14 vorsieht, dass die Vertragsstaaten für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren bestimmte Maßnahmen hinsichtlich

bereits gespeicherter Verkehrsdaten treffen, zu denen die umgehende Sicherung dieser Daten gehört. Dazu heißt es in Art. 16 I des Übereinkommens insbesondere, dass die Vertragsparteien die erforderlichen gesetzgeberischen Maßnahmen treffen, damit ihre zuständigen Behörden die umgehende Sicherung von Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass diese Daten verloren gehen oder verändert werden könnten.

163 In einer Situation wie der in Rn. 161 des vorliegenden Urteils beschriebenen steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in Rn. 130 des vorliegenden Urteils die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, frei, in Rechtsvorschriften, die sie gem. Art. 15 I RL 2002/58 erlassen, vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben wird, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

164 Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspricht, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Art. 8 II der GRCh jede Datenverarbeitung für festgelegte Zwecke zu erfolgen hat, müssen die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden kann. Angesichts der Schwere des Eingriffs in die Grundrechte der Art. 7 und 8 der GRCh, der mit einer solchen Speicherung verbunden sein kann, sind nur die Bekämpfung schwerer Kriminalität und, a fortiori, der Schutz der nationalen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Um sicherzustellen, dass der mit einer derartigen Maßnahme verbundene Eingriff auf das absolut Notwendige beschränkt bleibt, darf sich die Speicherungspflicht zudem zum einen nur auf Verkehrs- und Standortdaten erstrecken, die zur Aufdeckung der schweren Straftat oder der Beeinträchtigung der nationalen Sicherheit beitragen können. Zum anderen muss die Speicherungsdauer der Daten auf das absolut Notwendige beschränkt bleiben, kann allerdings verlängert werden, wenn die Umstände und das mit der fraglichen Maßnahme verfolgte Ziel es rechtfertigen.

165 Insoweit ist hinzuzufügen, dass sich eine solche umgehende Sicherung nicht auf die Daten der Personen beschränken muss, die konkret im Verdacht stehen, eine Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben. Unter Beachtung des durch Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh vorgegebenen Rahmens und angesichts der Erwägungen in Rn. 133 des vorliegenden Urteils kann eine solche Maßnahme nach Wahl des Gesetzgebers, unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat oder eine Beeinträchtigung der nationalen Sicherheit geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers, seines sozialen oder beruflichen Umfelds oder bestimmter geografischer Zonen, etwa der Orte, an denen die fragliche Straftat oder Beeinträchtigung der nationalen

Sicherheit begangen oder vorbereitet wurde. Außerdem müssen beim Zugang der zuständigen Behörden zu den gespeicherten Daten die Voraussetzungen eingehalten werden, die sich aus der Rechtsprechung zur Auslegung RL 2002/58 ergeben (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 118-121 mwN – Tele2).

166 Ferner ist hinzuzufügen, dass – wie sich insbesondere aus den Rn. 115 u. 133 des vorliegenden Urteils ergibt – der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste in Anwendung einer gem. Art. 15 I RL 2002/58 erlassenen Rechtsvorschrift gespeicherten Verkehrs- und Standortdaten grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung den Betreibern auferlegt wurde. Daraus folgt insbesondere, dass keinesfalls ein Zugang zu solchen Daten zwecks Verfolgung und Ahndung einer gewöhnlichen Straftat gewährt werden kann, wenn ihre Speicherung mit dem Ziel der Bekämpfung schwerer Kriminalität oder gar dem Schutz der nationalen Sicherheit gerechtfertigt wurde. Dagegen kann, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach seiner Auslegung in Rn. 131 des vorliegenden Urteils, ein Zugang zu Daten, die im Hinblick auf die Bekämpfung schwerer Kriminalität gespeichert wurden, mit dem Ziel des Schutzes der nationalen Sicherheit gerechtfertigt werden, sofern die in der vorstehenden Rn. genannten materiellen und prozeduralen Voraussetzungen für einen solchen Zugang eingehalten werden.

167 Insoweit steht es den Mitgliedstaaten frei, in ihren Rechtsvorschriften vorzusehen, dass ein Zugang zu Verkehrs- und Standortdaten bei Einhaltung der fraglichen materiellen und prozeduralen Voraussetzungen zur Bekämpfung schwerer Kriminalität oder zum Schutz der nationalen Sicherheit erfolgen kann, wenn diese Daten von einem Betreiber in einer mit den Art. 5, 6 und 9 oder mit Art. 15 I RL 2002/58 im Einklang stehenden Weise gespeichert wurden.

168 Nach alledem ist auf die erste Frage in den Rs. C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rs. C-520/18 zu antworten, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen ist, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 I genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 I der Richtlinie im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh Rechtsvorschriften nicht entgegen, die

> –es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

–zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

–zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

–zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

–es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

Zur zweiten und zur dritten Frage in der Rs. C-511/18

169 Mit seiner zweiten und seiner dritten Frage in der Rs. C-511/18 möchte das vorlegende Gericht wissen, ob Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste aufgegeben wird, in ihren Netzen Maßnahmen umzusetzen, die es ermöglichen, zum einen Verkehrs- und Standortdaten automatisiert zu analysieren und in Echtzeit zu erheben und zum anderen die technischen Daten zum Standort der verwendeten Endgeräte in Echtzeit zu erheben, ohne dass die Unterrichtung der Betroffenen von diesen Verarbeitungen und Datenerhebungen vorgesehen ist.

170 (*Das Vorbringen des vorlegenden Gerichts ist im Volltext abrufbar unter BeckRS 2020,25511 Rn. 170.*)

171 Zunächst ist darauf hinzuweisen, dass der Umstand, dass nach Art. L. 851-3 des CSI die dort vorgesehene automatisierte Analyse es als solche nicht ermöglicht, die Nutzer zu identifizieren, deren Daten dieser Analyse unterzogen werden, der Einstufung solcher Daten als „personenbezogene Daten" nicht entgegensteht. Da das in Abschnitt IV dieser Bestimmung vorgesehene Verfahren es gestattet, die Personen, bei denen die automatisierte Analyse ihrer Daten ergeben hat, dass eine terroristische Bedrohung vorliegen kann, später zu identifizieren, bleiben nämlich alle Personen, deren Daten Gegenstand der automatisierten Analyse waren, anhand dieser Daten identifizierbar.

Nach der Definition in Art. 4 Nr. 1 der VO Nr. 2016/679 sind aber ua Informationen, die sich auf eine identifizierbare Person beziehen, personenbezogene Daten.

Zur automatisierten Analyse von Verkehrs- und Standortdaten

172– 182(*Die umfassenden Ausführungen zur automatisierten Analyse von Verkehrs- und Standortdaten ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 172-182.*)

Zur Erhebung von Verkehrs- und Standortdaten in Echtzeit

183– 191(*Die rechtliche Würdigung betreffend die Erhebung von Verkehrs- und Standortdaten in Echtzeit, sowie die Unterrichtung der von der Datenerhebung betroffener Personen ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 183-191.*)

192 Nach alledem ist auf die zweite und die dritte Frage in der Rs. C-511/18 zu antworten, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen ist, dass er einer nationalen Regelung nicht entgegensteht, mit der den Betreibern elektronischer Kommunikationsdienste auferlegt wird, zum einen eine

automatisierte Analyse sowie eine Erhebung in Echtzeit insbesondere von Verkehrs- und Standortdaten und zum anderen eine Erhebung in Echtzeit der technischen Daten zum Standort der verwendeten Endgeräte vorzunehmen, sofern

> –der Rückgriff auf die automatisierte Analyse auf Situationen beschränkt ist, in denen sich ein Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, und Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer die fragliche Maßnahme rechtfertigenden Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und
>
> –der Rückgriff auf die Erhebung von Verkehrs- und Standortdaten in Echtzeit auf Personen beschränkt ist, bei denen ein triftiger Grund für den Verdacht besteht, dass sie auf irgendeine Weise in terroristische Aktivitäten verwickelt sind, und einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, deren Entscheidung bindend ist, wobei dieses Gericht oder diese Stelle sich vergewissern muss, dass eine solche Erhebung in Echtzeit nur in den Grenzen des absolut Notwendigen gestattet wird. In hinreichend begründeten Eilfällen muss die Kontrolle kurzfristig erfolgen.

Zur zweiten Frage in der Rs. C-512/18

193 Mit der zweiten Frage in der Rs. C-512/18 möchte das vorlegende Gericht wissen, ob die Bestimmungen RL 2000/31 im Licht der Art. 6-8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

194– 195(*Das Vorbringen des vorlegenden Gerichts ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 194 u 195.*)

196 Desgleichen erstreckten sich die von der Pflicht zur Vorratsspeicherung erfassten Daten auf die Kennungen der Teilnehmer, der Verbindungen und der verwendeten Endgeräte, die den Inhalten zugewiesenen Kennungen Datum und Uhrzeit von Beginn und Ende der Verbindungen und Vorgänge sowie die Arten der für die Verbindung zum Dienst und für die Übertragung der Inhalte verwendeten Protokolle. Der Zugang zu diesen Daten, die ein Jahr lang zu speichern seien, könne im Rahmen von Straf- und Zivilverfahren beantragt werden, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen, sowie im Rahmen von Maßnahmen zur Sammlung nachrichtendienstlicher Erkenntnisse, für die Art. L. 851-1 des CSI gelte.

197– 204(*Zur Abgrenzung der Dienste der Informationsgesellschaft iSd RL 2000/31 und 95/46 sowie RL 2002/58 ist im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 197-204.*)

205 Die Internetzugangsdienste, die offenbar von der in Rn. 195 des vorliegenden Urteils angesprochenen nationalen Regelung erfasst werden, stellen somit, wie der zehnte Erwägungsgrund RL 2002/21 bestätigt, elektronische Kommunikationsdienste im Sinne dieser Richtlinie dar (*EuGH* ECLI:EU:C:2019:460 = EuZW 2019, 576 Rn. 37 – Skype Communications). Dies gilt auch für die möglicherweise ebenfalls unter diese nationale Regelung fallenden internetbasierten E-Mail-Dienste, wenn sie in technischer Hinsicht ganz oder überwiegend die Übertragung von Signalen über elektronische Kommunikationsnetze implizieren (vgl. idS *EuGH* ECLI:EU:C:2019:498 = EuZW 2019, 572 Rn. 35 u. 38 – Google [C-193/18]).

206 Hinsichtlich der Erfordernisse, die sich aus Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh ergeben, ist auf die gesamten Feststellungen und Erwägungen im Rahmen der Antwort auf die erste Frage in den Rs. C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rs. C-520/18 zu verweisen.

207 In Bezug auf die Erfordernisse, die sich aus der VO Nr. 2016/679 ergeben, ist darauf hinzuweisen, dass sie, wie sich aus ihrem zehnten Erwägungsgrund ergibt, namentlich darauf abzielt, innerhalb der Union ein hohes Datenschutzniveau für natürliche Personen zu gewährleisten und zu diesem Zweck für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung personenbezogener Daten zu sorgen (*EuGH* ECLI:EU:C:2020:559 = EuZW 2020, 941 Rn. 101 – Facebook Ireland und Schrems).

208 Zu diesem Zweck müssen bei jeder Verarbeitung personenbezogener Daten, vorbehaltlich der nach Art. 23 der VO Nr. 2016/679 zulässigen Ausnahmen, die in ihrem Kapitel II aufgestellten Grundsätze für die Verarbeitung personenbezogener Daten sowie die in ihrem Kapitel III geregelten Rechte der betroffenen Person beachtet werden. Insbesondere muss jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 der Verordnung aufgestellten Grundsätzen im Einklang stehen und zum anderen die in Art. 6 der Verordnung aufgezählten Rechtmäßigkeitsvoraussetzungen erfüllen (vgl. entspr., in Bezug auf die RL 95/46, *EuGH* ECLI:EU:C:2013:355 = NZA 2013, 723 Rn. 33 mwN – Worten [C-342/12]).

209 Speziell zu Art. 23 I der VO Nr. 2016/679 ist festzustellen, dass er es, wie Art. 15 I RL 2002/58, den Mitgliedstaaten gestattet, im Hinblick auf die Ziele, die er vorsieht, und mittels Gesetzgebungsmaßnahmen die dort genannten Pflichten und Rechte zu beschränken, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte

und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die [das verfolgte Ziel] sicherstellt". Jede auf dieser Grundlage getroffene Gesetzgebungsmaßnahme muss insbesondere den in Art. 23 II der Verordnung aufgestellten spezifischen Anforderungen genügen.

210 Art. 23 I und II der VO Nr. 2016/679 kann somit nicht dahin ausgelegt werden, dass er den Mitgliedstaaten die Befugnis zu einer Beeinträchtigung der Achtung des Privatlebens, unter Verstoß gegen Art. 7 der GRCh, oder der übrigen in der GRCh vorgesehenen Garantien verleihen kann (vgl. entspr., in Bezug auf die RL 95/46, *EuGH* ECLI:EU:C:2003:294 = BeckRS 2004, 77378 Rn. 91 – Österreichischer Rundfunk ua [C-465/00 ua]). Insbesondere darf, ebenso wie bei Art. 15 I RL 2002/58, die den Mitgliedstaaten durch Art. 23 I der VO Nr. 2016/679 verliehene Befugnis nur unter Wahrung des Erfordernisses der Verhältnismäßigkeit ausgeübt werden, wonach Ausnahmen vom Schutz personenbezogener Daten und dessen Beschränkungen nicht über das absolut Notwendige hinausgehen dürfen (vgl. entspr., in Bezug auf die RL 95/46, *EuGH* ECLI:EU:C:2013:715 = BeckRS 2013, 82121 Rn. 39 mwN – IPI [C-473/12]).

211 Folglich gelten die Feststellungen und Erwägungen im Rahmen der Antwort auf die erste Frage in den Rs. C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rs. C-520/18 mutatis mutandis auch für Art. 23 der VO Nr. 2016/679.

EuGH: Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage(EuZW 2021, 209)	220

212 Nach alledem ist auf die zweite Frage in der Rs. C-512/18 zu antworten, dass die RL 2000/31 dahin auszulegen ist, dass sie im Bereich des Schutzes der Vertraulichkeit der Kommunikation sowie des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Dienste der Informationsgesellschaft nicht anwendbar ist; dieser Schutz ist entweder durch die RL 2002/58 oder durch die VO Nr. 2016/679 geregelt. Art. 23 I der VO Nr. 2016/679 ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh dahin auszulegen, dass er einer nationalen Regelung entgegensteht, mit der den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird.

Zur dritten Frage in der Rs. C-520/18

213 Mit der dritten Frage in der Rs. C-520/18 möchte das vorlegende Gericht wissen, ob ein nationales Gericht eine Bestimmung seines nationalen Rechts anwenden darf, aufgrund deren es, wenn es im Einklang mit seinem nationalen Recht eine nationale Rechtsvorschrift, mit der den Betreibern elektronischer Kommunikationsdienste ua zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh für rechtswidrig erklärt, zu einer Beschränkung der zeitlichen Wirkungen dieser Erklärung befugt ist.

214– 218(*Die Ausführungen zum Anwendungsvorrang sind im Volltext abrufbar unter BeckRS 2020, 25511 Rn. 214-218.*)

219 Im Gegensatz zu dem Versäumnis, einer prozeduralen Pflicht wie der vorherigen Prüfung der Auswirkungen eines Projekts im speziellen Bereich des Umweltschutzes nachzukommen, kann ein Verstoß gegen Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh aber nicht durch ein Verfahren wie das in der vorstehenden Rn. erwähnte geheilt werden. Würden die Wirkungen nationaler Rechtsvorschriften wie der im Ausgangsverfahren in Rede stehenden aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Betreibern elektronischer Kommunikationsdienste weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten gespeichert wurden.

220 Das vorlegende Gericht darf somit eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung der Rechtswidrigkeit der im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften in ihren zeitlichen Wirkungen zu beschränken.

221 *VZ*, *WY* und *XX* machen in ihren beim *EuGH* eingereichten Erklärungen geltend, die dritte Frage werfe implizit, aber zwangsläufig die Frage auf, ob das Unionsrecht dem entgegenstehe, dass im Rahmen eines Strafverfahrens Informationen und Beweise verwertet würden, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt worden seien.

222 Insoweit ist, um dem vorlegenden Gericht eine sachgerechte Antwort zu geben, darauf hinzuweisen, dass es beim gegenwärtigen Stand des Unionsrechts grundsätzlich allein Sache des nationalen Rechts ist, die Vorschriften für die Zulässigkeit und die Würdigung der durch eine solche unionsrechtswidrige Vorratsdatenspeicherung erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, schwere Straftaten begangen zu haben, festzulegen.

223 Nach ständiger Rechtsprechung ist es mangels einschlägiger unionsrechtlicher Vorschriften nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats, die Verfahrensmodalitäten für Klagen, die den Schutz der den Einzelnen aus dem Unionsrecht erwachsenden Rechte gewährleisten sollen, zu regeln, wobei sie jedoch nicht ungünstiger sein dürfen als diejenigen, die gleichartige, dem innerstaatlichen Recht unterliegende Sachverhalte regeln (Äquivalenzgrundsatz), und die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren dürfen (Effektivitätsgrundsatz) (*EuGH* ECLI:EU:C:2015:662 = EuZW 2015, 917 Rn. 26 u. 27 – Târşia [C-69/14]; *EuGH* ECLI:EU:C:2018:853 = EuZW 2019, 82 Rn. 21 u. 22 mwN – XC ua [C-234/17], und *EuGH* ECLI:EU:C:2019:1114 = EuZW 2020, 189 Rn. 33 – Deutsche Umwelthilfe [C-752/18]).

224 Was den Äquivalenzgrundsatz anbelangt, obliegt es dem nationalen Gericht, das mit einem Strafverfahren aufgrund von Informationen oder Beweisen befasst ist, die unter Verstoß gegen die Anforderungen aus RL 2002/58 erlangt wurden, zu prüfen, ob das für dieses Verfahren geltende nationale Recht Vorschriften vorsieht, die in Bezug auf die Zulässigkeit und die Verwertung solcher Informationen und Beweise ungünstiger sind als die Vorschriften für Informationen und Beweise, die unter Verstoß gegen innerstaatliches Recht erlangt wurden.

225 Zum Effektivitätsgrundsatz ist festzustellen, dass die nationalen Vorschriften über die Zulässigkeit und die Verwertung von Informationen und Beweisen darauf abzielen, nach Maßgabe der im nationalen Recht getroffenen Entscheidungen zu verhindern, dass rechtswidrig erlangte Informationen und Beweise einer Person, die im Verdacht steht, Straftaten begangen zu haben, unangemessene Nachteile zufügen. Dieses Ziel kann aber im nationalen Recht nicht nur durch ein Verbot der Verwertung solcher Informationen und Beweise erreicht werden, sondern auch durch nationale Vorschriften und Praktiken für die Würdigung und Gewichtung der Informationen und Beweise oder durch eine Berücksichtigung ihrer Rechtswidrigkeit im Rahmen der Strafzumessung.

226 Nach der Rechtsprechung des *EuGH* ist das Erfordernis, Informationen und Beweise auszuschließen, die unter Verstoß gegen unionsrechtliche Vorschriften erlangt wurden, insbesondere anhand der Gefahr zu beurteilen, die mit der Zulässigkeit solcher Informationen und Beweise für die Wahrung des Grundsatzes des kontradiktorischen Verfahrens und damit für das Recht auf ein faires Verfahren verbunden ist (*EuGH* ECLI:EU:C:2003:228 = EuZW 2003, 666 Rn. 76 u. 77 – Steffensen [C-276/01]). Kommt ein Gericht zu dem Ergebnis, dass eine Partei nicht in der Lage ist, sachgerecht zu einem Beweismittel Stellung zu nehmen, das einem Bereich entstammt, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet ist, die Würdigung der Tatsachen maßgeblich zu beeinflussen, muss es eine Verletzung des Rechts auf ein faires Verfahren feststellen und dieses Beweismittel ausschließen, um eine solche Verletzung zu verhindern (*EuGH* ECLI:EU:C:2003:228 = EuZW 2003, 666 Rn. 78 u. 79 – Steffensen).

227 Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht somit dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfah-

EuGH: Datenschutzrecht: Anlassbezogene Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage(EuZW 2021, 209) 221

rens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.

228 Nach alledem ist auf die dritte Frage in der Rs. C-520/18 zu antworten, dass ein nationales Gericht eine Bestimmung seines nationalen Rechts nicht anwenden darf, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste ua zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der GRCh rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 I der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht

stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.

Anmerkung von Akad. Rätin a.Z. Aqilah Sandhu*

I. Hintergrund

Nachdem der *EuGH* mit der Tele2-Entscheidung 2016 die anlass- und unterschiedslose Speicherung von Verkehrs- und Standortdaten der Nutzer elektronischer Kommunikation (Vorratsspeicherung) für weitestgehend unvereinbar mit Art. 7, 8 und 11 iVm Art. 52 I GRCh erklärt hatte (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 [C-203/15]), sorgten sich viele Mitgliedstaaten um die Zukunft dieses aus ihrer Sicht unverzichtbaren Instruments. Da nach der Tele2-Entscheidung praktisch kein Raum mehr für eine anlasslose, flächendeckende Vorratsspeicherung verblieb, war es nur eine Frage der Zeit, bis der *EuGH* zur Konkretisierung seiner sehr grundrechtsfreundlichen Maßstäbe aufgefordert werden würde (so schon *Sandhu* EuR 2017, 453 [467 f.]). Dem hier zu besprechenden Urteil lagen drei Vorabentscheidungsersuchen aus Frankreich und Belgien zugrunde. Über ein viertes Vorabentscheidungsersuchen aus dem Vereinigten Königreich erging eine Parallelentscheidung (*EuGH* ECLI:EU:C:2020:790 = BeckRS 2020, 25341 – Privacy International [C-623/17]) vom selben Tage.

II. Bewertung

Zentral stellte sich die Frage der Anwendbarkeit RL 2002/58 auf die mitgliedstaatlichen Vorschriften (Rn. 81-104). Zudem ist auf die Frage der Echtzeiterhebung von Verkehrs- und Standortdaten einzugehen.

Die Vorlagefragen betrafen jeweils nationale Regelungen zur Vorratsspeicherung zum Zweck des Schutzes der nationalen Sicherheit (Art. 4 II EUV). Das französische Gesetzbuch über innere Sicherheit verpflichtet die Betreiber elektronischer Kommunikationsdienste zur Vorratsspeicherung und zur Ermöglichung des Zugangs durch Nachrichten- und Sicherheitsdienste zum Schutz der nationalen Sicherheit. Die belgische Regelung wurde insbesondere mit der positiven Verpflichtung zur wirksamen strafrechtlichen Verfolgung sexuellen Missbrauchs von Minderjährigen begründet. Da gem. Art. 4 II 3 EUV die nationale Sicherheit ausdrücklich in die ausschließliche Kompetenz der Mitgliedstaaten fällt, lag die Anwendbarkeit der RL 2002/58 bzw. der Unionsgrundrechte nicht nahe. Das Sekundärrecht nimmt deklaratorisch „Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates […] und Tätigkeiten des Staates im strafrechtlichen Bereich" aus dem Anwendungsbereich heraus (Art. 1 III RL 2002/58; ähnlich Art. 3 II RL 95/46; etwas allgemeiner Art. 2 II Buchst. a DSGVO). Angesichts dessen ist die Bedeutung von Art. 15 I RL 2002/58, der die mitgliedstaatliche Abweichung vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation und dem grundsätzlichen Speicherverbot von Verkehrsdaten zum Zwecke der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit sowie zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zulässt, seit Jahren umstritten. Der *EuGH* legt ihr als permissive Bestimmung und Grundrechtsschranke ein restriktives

Verständnis zugrunde: Im Sinne des *effet utile* beurteile sich die Anwendbarkeit nicht nach dem Zweck einer Maßnahme, sondern nach den Akteuren. Tätigkeiten Privater, also auch der Betreiber elektronischer Kommunikationsdienste, unterfallen danach ungeachtet dessen, dass sie den Schutz der nationalen Sicherheit bezwecken, der RL 2002/58. Nur „spezifische Tätigkeiten der Staaten oder der staatlichen Stellen" sind ausgenommen (*EuGH* ECLI:EU:C:2016:970 = EuZW 2017, 153 Rn. 72 – Tele2). Argumentativ bedient sich der *EuGH* der teleologischen Auslegung im Lichte des Sekundärrechtsziels, das sich auf den Schutz personenbezogener Daten und der Privatsphäre bei der Nutzung elektronischer Kommunikationsdienste beschränkt: Weil Art. 15 I RL 2002/58 die Abweichung vom Grundsatz der Vertraulichkeit der Kommunikation an bestimmte Voraussetzungen knüpfe – sie muss verhältnismäßig sein, insbesondere ist die Speicherung nur für eine begrenzte Zeit zulässig – müsse die Richtlinie „zwangsläufig" auch auf die dort in Bezug genommenen mitgliedstaatlichen Rechtsvorschriften anwendbar sein (Rn. 95, 110 ff.). Die Rechtmäßigkeit der Speicherpflicht für die Betreiber elektronischer Kommunikationsdienste sowie die Übermittlung an die zuständigen mitgliedstaatlichen Behörden beurteile sich deshalb nach dem Unionsrecht. Erstmals äußert sich der *EuGH* aber zur divergierenden PNR-Entscheidung (*EuGH* ECLI:EU:C:2006:346 = EuZW 2006, 403 – Parlament ua/Rat und Kommission ua [C-317/04, C-318/04]), in der er noch davon ausging, dass die Übermittlung personenbezogener Daten durch Fluggesellschaften an die Behörden eines Drittstaats aus Gründen der nationalen Sicherheit wegen Art. 3 II RL 95/46 nicht dem Sekundärrecht unterfalle. Schon bei der Entscheidung über die Unionskompetenz für die Vorratsspeicherungs-RL, die im Unterschied zur Fluggastdatenspeicherung sehr wohl auf die Binnenmarktkompetenz gestützt werden konnte, wurde dieser Widerspruch kritisiert (vgl. *Rossi* ZJS 2009, 298 [299]). Zwar werden Private tätig, allerdings – so der *EuGH* – auf behördliche Anordnung, mithin „in einem von staatlichen Stellen geschaffenen Rahmen" (Rn. 100). Anders als die Bereichsausnahme der ehemaligen RL 95/46, die Tätigkeiten zum Zweck der nationalen Sicherheit „generell" ausgeschlossen habe, stelle Art. 1 III RL 2002/58 auf den Urheber der Verarbeitung ab (Rn. 101). Überzeugend ist dies nicht. Denn die genannten Bereichsausnahmen spiegeln nur die Grenzen des Primär-

rechts und das Prinzip der begrenzten Einzelermächtigung wider, so dass ihnen nicht zwei verschiedene Verständnisse zugrunde gelegt werden können. Es bedarf vielmehr einer einheitlichen Antwort. Deutlich wird dies mit Blick auf Art. 2 II Buchst. a DSGVO, der die nationale Sicherheit gerade nicht mehr explizit als Ausnahme vom Anwendungsbereich erwähnt (siehe aber EG 16 DSGVO). Dies wird vielmehr mit Blick auf Art. 4 II 3 EUV vorausgesetzt. Der *EuGH* legt Öffnungsklauseln zugunsten mitgliedstaatlicher Kompetenzreservate (auch Art. 23 I Buchst. d und h DSGVO) anwendungserweiternd aus und verkennt dadurch ihren nur klarstellenden Charakter (vgl. bereits *Wollenschläger* NJW 2016, 906 [908]; *Sandhu* Grundrechtsunitarisierung durch Sekundärrecht, Manuskript, 145 ff.).

Den Prüfungsmaßstab bilden das in Art. 5 I RL 2002/58 konkretisierte Grundrecht auf den Schutz der Vertraulichkeit der elektronischen Kommunikation sowie Art. 7, 8 und 11 iVm Art. 52 I GRCh. Angesichts der abschreckenden Wirkungen, der

Missbrauchsgefahren sowie der hohen Streubreite und Sensibilität der betroffenen Daten sind die Speicherung und der behördliche Zugriff jeweils zwei schwerwiegende Eingriffe, die einem strikten Verhältnismäßigkeitserfordernis unterliegen. Nicht mehr auf das absolut Notwendige beschränkt ist eine unterschiedslose Vorratsspeicherung, wenn sie zur Abwehr gewöhnlicher Straftaten erfolgt. Für die Bekämpfung schwerer Straftaten ist sie nur zulässig, wenn der Kreis der Betroffenen auf solche Personen (bspw. geografisch) begrenzt wird, die zumindest mittelbar in einem Zusammenhang mit den schweren Straftaten stehen. Zu Recht lässt der *EuGH* mit Blick auf die Schwere des Eingriffs weiterhin nur die gezielte Vorratsspeicherung zur Bekämpfung schwerer Straftaten zu (s. Rn. 146).

Diese Grundsätze sollen nun aber dann nicht mehr gelten, wenn hinreichend konkrete Umstände für die Annahme vorliegen, dass sich ein Mitgliedstaat in einer „real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit" befindet (Rn. 137). Hierin liegt die zentrale Neuerung der Entscheidung: Allein, dass eine solche nationale Bedrohungslage vorliegt, rechtfertigt die unterschiedslose Vorratsspeicherung der Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel, ohne dass es eines Zusammenhangs mit einer schweren Straftat bedarf. Diese general-präventive Vorratsspeicherung muss in zeitlicher Hinsicht auf das absolut Notwendige beschränkt sein (wobei eine Verlängerung möglich ist) und darf „keinen systematischen Charakter" haben (Rn. 138). Der Grundrechtsschutz der Nutzer elektronischer Kommunikation wird damit in einer nationalen terroristischen Bedrohungslage faktisch ausgesetzt. Dies zeigt erneut eindrücklich, wie sich die extensiv verstandene Grundrechtskompetenz des *EuGH* zulasten des effektiven Grundrechtsschutzes im Mehrebenensystem auswirken kann. Denn anstatt die RL 2002/58 und gem. Art. 51 I GRCh die Unionsgrundrechte für unanwendbar zu erklären, weil die betreffenden Tätigkeiten eine den Mitgliedstaaten vorbehaltene und unionsrechtlich nur schwach determinierte Domäne betreffen, bildet der *EuGH* – wohl mit Blick auf die Kompetenzsensitivität – einen grundrechtlichen Minimalstandard, sobald die Verarbeitung zum Schutz der nationalen Sicherheit erfolgt. Unionsrechtlicher Grundrechtsschutz ist in diesen Fällen gerade kein Mehrwert (zum Ganzen *Sandhu* Grundrechtsunitarisierung durch Sekundärrecht, Manuskript, 151 ff.).

Auch die vom *EuGH* als besonders schwerwiegender Eingriff qualifizierte automatisierte Analyse der Vorratsdaten und ihre Echtzeiterhebung ist in einer real und aktuell „oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit" verhältnismäßig, wenn die Speicherdauer auf das absolut Notwendige beschränkt ist (Rn. 177). Bei der Erhebung in Echtzeit können Nachrichtendienste die Kommunikationspartner, -mittel, -dauer und den Ort kontinuierlich überwachen und sehr detaillierte Persönlichkeitsprofile erstellen. Dies erachtet der *EuGH* im Fall der terroristischen Bedrohungslage für zulässig. Einschränkend darf sich die Maßnahme nur auf Personen erstrecken, gegen die ein „begründeter Verdacht" der Beteiligung an terroristischen Straftaten besteht. Die Überwachungskriterien müssen objektiv nachvollziehbar sein und dürfen insbesondere nicht allein an die in Art. 21 GRCh aufgezählten verbotenen Diskriminierungsmerkmale anknüpfen.

III. Praxisfolgen

Die in § 113 b TKG vorgesehene deutsche Vorratsspeicherung wurde in einer Eilrechtsentscheidung des *OVG Münster* für einen klagenden Internetzugangsdienstleister einstweilig ausgesetzt (*OVG Münster* NVwZ-RR 2018, 43) und seither nicht mehr durch die *BNetzA* durchgesetzt. Sie liegt derzeit dem *EuGH* zur Vorabentscheidung vor (*BVwerG,* NVwZ 2020, 1108 = ZD 2020, 167). Als anlasslose und generelle Vorratsspeicherung ist sie schon im Lichte der bisherigen *EuGH*-Entscheidungen unionsrechtswidrig und nur bei Vorliegen einer ernstlichen terroristischen Gefahr mit Art. 15 I RL 2002/58 vereinbar. Doch selbst dann darf der behördliche Zugang nicht für gewöhnliche Straftaten gewährt werden. Indes ermöglicht § 100 g II StPO den Abruf auch zur Bekämpfung des Einbruchsdiebstahls oder der einfachen Brandstiftung. Ausgeweitet wurde der Kreis der abrufberechtigten Behörden. In Bayern sind dies auch die Polizei zur Abwehr dringender Gefahren für den Bestand des Bundes, eines Landes oder für Leib und Leben (Art. 43 II 2 BayPAG) sowie seit 2018 der Verfassungsschutz (Art. 15 III BayVSG). Ihre Tätigkeiten unterliegen als spezifische Tätigkeiten der Sicherheitsbehörden nicht dem Anwendungsbereich des Unionsrechts. Jenseits der Kompetenzfrage führt das Verständnis des *EuGH* zu einer künstlichen Aufspaltung einer einheitlich zu beurteilenden Maßnahme. Die den Unionsrechtgrundrechten unterfallende Vorratsspeicherungspflicht ist untrennbar mit der Frage des behördlichen Umgangs mit diesen Daten verbunden, der aber dem nationalen Grundrechtsschutz unterfällt. Auch eine gezielte und eingegrenzte Vorratsspeicherung kann in der Gesamtbetrachtung unverhältnismäßig werden, wenn zu viele Behörden Zugriff auf die Daten erhalten.

---

* Die Autorin ist Akademische Rätin a.Z. am Lehrstuhl für Staats- und Verwaltungsrecht, Europarecht sowie Gesetzgebungslehre von *Prof. Dr. Matthias Rossi*, Universität Augsburg.