Datenschutz: Deutsche Vorratsdatenspeicherung verstößt gegen Unionsrecht

RL 2002/58/EG (DatenschutzRL für elektronische Kommunikation) Art. 15 I; GRCh Art. 7, 8, 11, 52 I

Mit dem vorliegenden Urteil stellt der EuGH klar, dass Kommunikationsdaten von Bürgerinnen und Bürgern innerhalb der EU ohne konkreten Anlass nicht gespeichert werden dürfen. Ein begrenztes Speichern dieser Daten ist vielmehr nur unter klar definierten, engen Voraussetzungen zulässig. Im Ausgangsverfahren hatten Telekom und Spacenet gegen die deutschen Vorschriften betreffend die anlasslose Vorratsdatenspeicherung geklagt.

Tenor des Gerichts:

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 nationalen Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

er nationalen Rechtsvorschriften nicht entgegensteht, 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 der 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.

EuGH (Große Kammer), Urteil vom 20.9.2022 – C-793/19, C-794/19 (Bundesrepublik Deutschland/SpaceNet AG 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) 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 2002/58) im Licht der Art. 6-8 und 11 sowie von Art. 52 I der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) und von Art. 4 II EUV. Es ergeht im Rahmen von Rechtsstreitigkeiten zwischen der Bundesrepublik Deutschland, vertreten durch die BNetzA für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, auf der einen Seite und der SpaceNet AG (Rechtssache C-793/19) sowie der Telekom Deutschland GmbH (Rechtssache C-794/19) auf der anderen Seite wegen der den Letztgenannten auferlegten Verpflichtung, Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden auf Vorrat zu speichern.

SpaceNet und Telekom Deutschland erbringen in Deutschland öffentlich zugängliche Internetzugangsdienste. Telekom Deutschland erbringt darüber hinaus, ebenfalls in Deutschland, öffentlich zugängliche Telefondienste. Diese Diensteanbieter fochten vor dem VG Köln die ihnen durch § 113a I iVm § 113b TKG auferlegte Pflicht an, ab dem 1.7. 2017 Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden auf Vorrat zu speichern.

Mit Urteilen vom 20.4.2018 entschied das VG Köln (9 K 3859/16, BeckRS 2018, 9168), dass SpaceNet und Telekom Deutschland nicht verpflichtet seien, die in § 113b III TKG genannten Verkehrsdaten in Bezug auf die Telekommunikation der Kunden, denen sie einen Internetzugang zur Verfügung stellten, auf Vorrat zu speichern, und dass Telekom Deutschland ferner nicht verpflichtet sei, die in § 113b II 1 und 2 TKG genannten Verkehrsdaten in Bezug auf die Telekommunikation der Kunden, denen sie einen Zugang zu öffentlichen Telefondiensten zur Verfügung stelle, auf Vorrat zu speichern. Dieses Gericht war nämlich im Licht des Urteils vom 21.12.2016 (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua (C-203/15)) der Auffassung, dass diese Pflicht zur Vorratsspeicherung gegen das Unionsrecht verstoße.

Die Bundesrepublik Deutschland legte beim BVerwG, dem vorlegenden Gericht, Revision gegen diese Urteile ein.

Das BVerwG ist der Ansicht, dass die Frage, ob die durch § 113a I iVm § 113b TKG auferlegte Pflicht zur Vorratsspeicherung gegen das Unionsrecht verstoße, von der Auslegung der RL 2002/58 abhänge.

Insoweit weist das vorlegende Gericht darauf hin, dass der EuGH bereits im Urteil vom 21.12.2016 (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua) abschließend geklärt habe, dass Regelungen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie über den Zugang der nationalen Behörden zu diesen Daten grundsätzlich in den Geltungsbereich der RL 2002/58 fielen. Außerdem könne die in den Ausgangsverfahren in Rede stehende Pflicht zur Vorratsspeicherung, soweit sie die Rechte aus Art. 5 I, Art. 6 I und Art. 9 I RL 2002/58 beschränke, nur auf der Grundlage von Art. 15 I dieser Richtlinie gerechtfertigt werden.

Insoweit gehe aus dem Urteil vom 21.12.2016 (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua) hervor, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 I der Charta dahin auszulegen sei, dass er einer nationalen Regelung entgegenstehe, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe.

Nach Ansicht des vorlegenden Gerichts verlangt die in den Ausgangsverfahren in Rede stehende nationale Regelung jedoch wie die nationalen Regelungen, um die es in den Rechtssachen ging, in denen das genannte Urteil ergangen ist, weder einen Anlass für die Speicherung der Daten noch irgendeinen Zusammenhang zwischen den gespeicherten Daten und einer Straftat oder einer Gefahr für die öffentliche Sicherheit. Diese nationale Regelung schreibe nämlich eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung eines Großteils der relevanten Telekommunikations-Verkehrsdaten vor.

Das vorlegende Gericht ist allerdings der Auffassung, dass nicht ausgeschlossen sei, dass die in den Ausgangsverfahren in Rede stehende Pflicht zur Vorratsspeicherung nach Art. 15 I RL 2002/58 gerechtfertigt sein könne.

Erstens verlange die in den Ausgangsverfahren in Rede stehende nationale Regelung im Gegensatz zu den nationalen Regelungen, um die es in den Rechtssachen gegangen sei, in denen das Urteil vom 21.12.2016 (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua) ergangen sei, nicht die Vorratsspeicherung sämtlicher Verkehrsdaten bezüglich der Telekommunikation aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel. Von der Speicherpflicht ausgenommen sei nicht nur der Inhalt der Kommunikation, sondern es dürften auch Daten über aufgerufene Internetseiten, Daten von E-Mail-Diensten sowie Daten, die den Verbindungen zu oder von bestimmten Anschlüssen in sozialen oder kirchlichen Bereichen zugrunde lägen, nicht gespeichert werden, wie aus § 113b V und VI TKG hervorgehe.

Zweitens weist das vorlegende Gericht darauf hin, dass § 113b I TKG eine Speicherungsfrist von vier Wochen für Standortdaten und von zehn Wochen für Verkehrsdaten vorsehe, während die RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der RL 2002/58/EG (ABl. 2006 L 105, 54), die den nationalen Regelungen zugrunde gelegen habe, um die es in den Rechtssachen gegangen sei, in denen das Urteil vom 21.12.2016 (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua) ergangen sei, eine Speicherungsfrist zwischen sechs Monaten und zwei Jahren vorgesehen habe.

Zwar genügten die Ausnahme bestimmter Kommunikationsmittel oder Datenkategorien und die Begrenzung der Speicherungsfrist nicht, um jede Gefahr der Erstellung eines umfassenden Profils der betroffenen Personen zu beseitigen, jedoch sei diese Gefahr im Rahmen der Anwendung der in den Ausgangsverfahren in Rede stehenden nationalen Regelung zumindest erheblich verringert.

Drittens enthalte diese Regelung strenge Beschränkungen in Bezug auf den Schutz der gespeicherten Daten und den Zugang hierzu. Somit gewährleiste sie zum einen einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang. Zum anderen dürften die auf Vorrat gespeicherten Daten nur zur Bekämpfung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes verwendet werden.

Viertens könnte nach Ansicht des vorlegenden Gerichts der Auslegung von Art. 15 I RL 2002/58 dahin, dass jede anlasslose Vorratsdatenspeicherung mit dem Unionsrecht allgemein unvereinbar wäre, die

Handlungspflicht der Mitgliedstaaten entgegenstehen, die sich aus dem in Art. 6 der Charta verankerten Recht auf Sicherheit ergebe.

Fünftens würde nach Auffassung des vorlegenden Gerichts eine Auslegung von Art. 15 RL 2002/58 dahin, dass er einer allgemeinen Vorratsspeicherung der Daten entgegensteht, den Handlungsspielraum des nationalen Gesetzgebers in einem Bereich der Strafverfolgung und der öffentlichen Sicherheit, der nach Art. 4 II EUV weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, erheblich einschränken.

Sechstens ist das vorlegende Gericht der Ansicht, dass die Rechtsprechung des EGMR zu berücksichtigen sei und weist darauf hin, dass dieser entschieden habe, dass Art. 8 Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) nationalen Bestimmungen, die eine Massenüberwachung des grenzüberschreitenden Datenverkehrs vorsähen, angesichts der Bedrohungen, denen zahlreiche Staaten derzeit ausgesetzt seien, und den technologischen Instrumenten, auf die sich Terroristen und Kriminelle nunmehr zur Begehung strafbarer Handlungen stützen könnten, nicht entgegenstehe. Vor diesem Hintergrund hat das BVerwG die Verfahren ausgesetzt und dem EuGH seine Frage zur Vorabentscheidung vorgelegt (BVerwG NVwZ 2020, 1108).

Der EuGH hat nach Anhörung des Generalanwalts Campos Sánchez-Bordona (ECLI:EU:C:2021:939 = BeckRS 2021, 35300) wie aus dem Tenor ersichtlich entschieden.

Aus den Gründen: *Verfahren vor dem EuGH*

[40] Mit Beschluss des Präsidenten des EuGH vom 3.12. 2019 sind die Rechtssachen C-793/19 und C-794/19 zu gemeinsamem schriftlichen und mündlichen Verfahren sowie zu gemeinsamer Entscheidung verbunden worden.

[41] Mit Beschluss des Präsidenten des EuGH vom 14.7. 2020 ist das Verfahren in den verbundenen Rechtssachen C-793/19 und C-794/19 gem. Art. 55 I Buchst. b der Verfahrensordnung des EuGH bis zur Verkündung des Urteils in der Rechtssache La Quadrature du Net ua (C-511/18, C-512/18 und C-520/18) ausgesetzt worden.

[42] Nachdem der EuGH am 6.10.2020 sein Urteil in der Rechtssache La Quadrature du Net ua (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua – (C-511/18 ua)) erlassen hatte, hat der Präsident des EuGH am 8.10.2020 die Fortsetzung des Verfahrens in den verbundenen Rechtssachen C-793/19 und C-794/19 angeordnet.

[43] Das vorlegende Gericht, dem die Kanzlei dieses Urteil übermittelt hatte, hat mitgeteilt, dass es sein Vorabentscheidungsersuchen aufrechterhalte.

[44] Insoweit hat das vorlegende Gericht zunächst darauf hingewiesen, dass die in der in den Ausgangsverfahren in Rede stehenden Regelung vorgesehene Speicherpflicht weniger Daten und eine kürzere Speicherungsfrist betreffe, als sie die nationalen Regelungen vorgesehen hätten, um die es in den Rechtssachen gegangen sei, in denen das Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) ergangen sei. Diese Besonderheiten verringerten die Möglichkeit, dass aus den gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert worden seien, gezogen würden.

[45] Sodann hat das vorlegende Gericht erneut darauf hingewiesen, dass die in den Ausgangsverfahren in Rede stehende nationale Regelung gewährleiste, dass die auf Vorrat gespeicherten Daten wirksam vor den Risiken eines Missbrauchs und eines unberechtigten Zugangs geschützt seien.

[46] Schließlich hat es hervorgehoben, dass weiterhin Unsicherheiten hinsichtlich der Frage bestünden, ob die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Speicherung der IP-Adressen mit dem Unionsrecht vereinbar sei, weil zwischen den Rn. 155 u. 168 des Urteils vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) eine Inkohärenz bestehe. So ergebe sich aus diesem Urteil eine Unsicherheit hinsichtlich der Frage, ob der EuGH für die Vorratsspeicherung der IP-Adressen einen mit dem Ziel des Schutzes der nationalen Sicherheit, der Bekämpfung schwerer Kriminalität oder der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zusammenhängenden Anlass verlange, wie sich aus Rn. 168 des genannten Urteils ergebe, oder ob die Vorratsspeicherung der IP-Adressen auch bei Fehlen eines konkreten Anlasses zulässig sei und lediglich die Verwendung der gespeicherten Daten durch diese Ziele begrenzt werde, wie sich aus Rn. 155 des genannten Urteils ergebe.

Zur Vorlagefrage

[47] Mit seiner Vorlagefrage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 I RL 2002/58 im Licht der Art. 6-8 und 11 sowie des Art. 52 I der Charta und des Art. 4 II EUV dahin auszulegen ist, dass er einer nationalen Rechtsvorschrift entgegensteht, die – von bestimmten Ausnahmen abgesehen – die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste für die in Art. 15 I der genannten Richtlinie aufgeführten Zwecke, insbesondere zur Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für die nationale Sicherheit, zu einer allgemeinen und unterschiedslosen Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste verpflichtet und eine Speicherungsfrist von mehreren Wochen sowie Regeln vorsieht, die einen wirksamen Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleisten sollen.

Zur Anwendbarkeit der RL 2002/58

[48] Was das Vorbringen Irlands sowie der französischen, der niederländischen, der polnischen und der schwedischen Regierung anbelangt, die in den Ausgangsverfahren in Rede stehende nationale Regelung falle nicht in den Geltungsbereich der RL 2002/58, da sie insbesondere zum Schutz der nationalen Sicherheit erlassen worden sei, genügt der Hinweis, dass eine nationale Regelung, die wie die in den Ausgangsverfahren in Rede stehende die Betreiber elektronischer Kommunikationsdienste insbesondere 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 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 104 – La Quadrature du Net ua).

Zur Auslegung von Art. 15 I RL 2002/58

Hinweis auf die sich aus der Rechtsprechung des EuGH ergebenden Grundsätze

[49] Nach stRspr. ist bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen, 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:2022:258 = BeckRS 2022, 6441 Rn. 32 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua (C-140/20)).

[50] Bereits aus dem Wortlaut von Art. 15 I RL 2002/58 geht hervor, dass die Rechtsvorschriften, zu deren Erlass die Richtlinie die Mitgliedstaaten unter den in der Richtlinie festgelegten Voraussetzungen ermächtigt, lediglich darauf abzielen können, die ua in den Art. 5, 6 und 9 RL 2002/58 vorgesehenen Rechte und Pflichten zu „beschränken" (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 33 = EuZW 2022, 536 Ls.– Commissioner of An Garda Síochána ua).

[51] Was das durch diese Richtlinie eingeführte System betrifft, in das sich ihr Art. 15 I einfügt, ist darauf hinzuweisen, dass die Mitgliedstaaten nach Art. 5 I 1 und 2 der Richtlinie verpflichtet sind, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen. Sie sind insbesondere verpflichtet, das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer zu untersagen, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gem. Art. 15 I der Richtlinie gesetzlich dazu ermächtigt sind (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 34 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[52] Insoweit hat der EuGH bereits entschieden, dass in Art. 5 I RL 2002/58 der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt wird, der ua das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 107 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 35 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[53] Diese Bestimmung spiegelt das vom Unionsgesetzgeber beim Erlass der RL 2002/58 verfolgte Ziel wider. 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, ergibt sich nämlich, 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". Die genannte Richtlinie soll somit, wie sich ua aus ihren Erwgr. 6 und 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 ist es, wie im zweiten Erwägungsgrund der Richtlinie zum Ausdruck kommt, der Wille des Unionsgesetzgebers, die uneingeschränkte Achtung der in den die Achtung des Privatlebens bzw. den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta niedergelegten Rechte zu gewährleisten (vgl. idS EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 36 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[54] Durch den Erlass der RL 2002/58 hat der Unionsgesetzgeber somit diese 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 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 109 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 37 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[55] Was die Verarbeitung und Speicherung von sich auf Teilnehmer und Nutzer beziehenden Verkehrsdaten durch die Betreiber elektronischer Kommunikationsdienste anbelangt, sieht Art. 6 RL 2002/58 in Abs. 1 vor, dass diese Daten zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden, und stellt in Abs. 2 klar, dass Verkehrsdaten, die zum Zweck der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, nur bis zum Ablauf der Frist verarbeitet werden dürfen, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. 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.

[56] Folglich beschränkt sich die RL 2002/58 nicht darauf, den Zugang zu solchen Daten durch Garantien zu regeln, die Missbrauch verhindern sollen, sondern sie regelt insbesondere auch den Grundsatz des Verbots der Speicherung dieser Daten durch Dritte (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 39 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[57] Indem Art. 15 I RL 2002/58 den Mitgliedstaaten gestattet, Rechtsvorschriften zu erlassen, die die Rechte und Pflichten gemäß ua den Art. 5, 6 und 9 dieser Richtlinie – wie sie sich aus den in Rn. 52 des vorliegenden Urteils angeführten Grundsätzen der Vertraulichkeit der Kommunikation und dem Verbot der Speicherung der damit verbundenen Daten ergeben – „beschränken", sieht diese Bestimmung eine Ausnahme von der allgemeinen Regel vor, die ua in den Art. 5, 6 und 9 vorgesehen ist, und ist daher nach ständiger Rechtsprechung eng auszulegen. Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die Ausnahme von der grundsätzlichen Verpflichtung, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen, und insbesondere von dem in Art. 5 RL 2002/58 vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 40 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[58] 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:2022:258 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[59] Außerdem geht aus Art. 15 I 3 RL 2002/58 hervor, dass die nach dieser Vorschrift von den Mitgliedstaaten erlassenen Vorschriften die allgemeinen Grundsätze des Uni-

onsrechts beachten müssen, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die Achtung der durch die Charta garantierten Grundrechte gewährleisten müssen. Hierzu hat der EuGH bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch nationale Rechtsvorschriften 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 Art. 7 und 8 der Charta betreffen, sondern auch die in Art. 11 der Charta gewährleistete Freiheit der Meinungsäußerung, und dass diese Freiheit eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Europäische Union nach Art. 2 EUV gründet (vgl. idS EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 42 u. 43 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[60] 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 Charta 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 oder ob die gespeicherten Daten in der Folge verwendet werden oder nicht (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 44 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[61] 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:2022:258 = BeckRS 2022, 6441 Rn. 45 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[62] Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken zum einen das in Art. 7 der Charta verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung abhalten; diese Wirkungen sind umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind. 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 (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 46 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[63] In Art. 15 I RL 2002/58, der es den Mitgliedstaaten gestattet, die in den Rn. 51-54 des vorliegenden Urteils angesprochenen Rechte und Pflichten zu beschränken, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen. Nach Art. 52 I der Charta sind nämlich Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Bei der Auslegung von Art. 15 I RL 2002/58 im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den in den Art. 3, 4, 6 und 7 der Charta verankerten Rechten und den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer zukommt (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 48 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[64] Somit ist in Bezug insbesondere auf die wirksame Bekämpfung von Straftaten, deren Opfer ua Minderjährige und andere schutzbedürftige Personen sind, zu berücksichtigen, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens ergeben können. Solche Verpflichtungen können sich aus Art. 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 49 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[65] Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen berechtigten Interessen und Rechte somit miteinander in Einklang gebracht werden, und es ist ein rechtlicher Rahmen zu schaffen, der diesen Einklang ermöglicht (vgl. idS EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 50 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[66] In diesem Rahmen ergibt sich bereits aus dem Wortlaut von Art. 15 I 1 RL 2002/58, dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem in Rn. 52 des vorliegenden Urteils genannten Grundsatz der Vertraulichkeit abweicht, wenn eine solche Vorschrift „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig" ist, wobei es im elften Erwägungsgrund der Richtlinie heißt, dass eine derartige Maßnahme in einem „strikt" angemessenen Verhältnis zum intendierten Zweck stehen muss.

[67] Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach stRspr. des EuGH verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem 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:2022:258 = BeckRS 2022, 6441 Rn. 52 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[68] Insbesondere geht aus der Rspr. 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:2022:258 = BeckRS 2022, 6441 Rn. 53 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[69] Um dem Erfordernis der Verhältnismäßigkeit zu genügen, müssen nationale Rechtsvorschriften 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. Diese Rechtsvorschriften müssen 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:2022:258 = = BeckRS 2022, 6441 Rn. 54 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[70] Nationale Rechtsvorschriften, die eine Vorratsspeicherung personenbezogener Daten vorsehen, müssen daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 55 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[71] Was die dem Gemeinwohl dienenden Ziele anbelangt, die eine nach Art. 15 I RL 2002/58 erlassene Vorschrift rechtfertigen können, geht aus der Rspr. des EuGH, insbesondere aus dem Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) hervor, dass nach dem Grundsatz der Verhältnismäßigkeit eine Hierarchie zwischen diesen Zielen entsprechend ihrer jeweiligen Bedeutung besteht und dass die Bedeutung des mit einer solchen Vorschrift verfolgten Ziels im Verhältnis zur Schwere des daraus resultierenden Eingriffs stehen muss (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 56 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[72] Daher hat der EuGH, was den Schutz der nationalen Sicherheit anbelangt, dessen Bedeutung die der übrigen von Art. 15 I RL 2002/58 erfassten Ziele übersteigt, festgestellt, dass diese Bestimmung im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta Rechtsvorschriften nicht entgegensteht, 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 (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 58 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[73] Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, hat der EuGH festgestellt, dass im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet sind, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte, die in den Art. 7 und 8 der Charta 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:2022:258 BeckRS 2022, 6441 Rn. 59 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[74] Was das Ziel der Bekämpfung schwerer Kriminalität anbelangt, hat der EuGH entschieden, dass nationale Rechtsvorschriften, die zu diesem Zweck die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, die Grenzen des absolut Notwendigen überschreiten und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden können. 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. 62 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in den Art. 7 und 11 der Charta 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 (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 65

mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[75] Dagegen hat der EuGH klargestellt, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta Rechtsvorschriften nicht entgegensteht, die 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;
- für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
- eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
- vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze).

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 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 168 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 67 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

Zu einer Maßnahme, die für eine Dauer von mehreren Wochen eine allgemeine und unterschiedslose Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vorsieht

[76] Anhand dieser grundsätzlichen Erwägungen sind die vom vorlegenden Gericht hervorgehobenen Merkmale der in den Ausgangsverfahren in Rede stehenden nationalen Regelung zu prüfen.

[77] Was erstens den Umfang der auf Vorrat gespeicherten Daten anbelangt, geht aus der Vorlageentscheidung hervor, dass im Rahmen der Erbringung von Telefondiensten die durch diese Regelung auferlegte Pflicht zur Vorratsspeicherung insbesondere die Daten betrifft, die erforderlich sind, um die Quelle und den Adressaten einer Nachricht, Datum und Uhrzeit von Beginn und Ende der Verbindung oder – im Fall der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten – die Zeitpunkte der Versendung und des Empfangs der Nachricht sowie, im Fall der mobilen Nutzung, die Bezeichnung der Funkzellen, die vom Anrufer und vom Angerufenen bei Beginn der Verbindung genutzt wurden, zu identifizieren. Im Rahmen der Bereitstellung von Internetzugangsdiensten bezieht sich die Pflicht zur Vorratsspeicherung ua auf die dem Teilnehmer zugewiesene IP-Adresse, Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse und, im Fall der mobilen Nutzung, die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle. Die Daten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben, werden ebenfalls gespeichert.

[78] Zwar nimmt die in den Ausgangsverfahren in Rede stehende nationale Regelung den Inhalt der Kommunikation sowie die Daten über aufgerufene Internetseiten von der Speicherpflicht aus und schreibt die Speicherung der Funkzellenkennung lediglich zu Beginn der Kommunikation vor, jedoch ist darauf hinzuweisen, dass dies im Wesentlichen auch für die nationalen Regelungen zur Umsetzung der RL 2006/24 galt, um die es in den Rechtssachen ging, in denen das Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) ergangen ist. Trotz dieser Beschränkungen hat der EuGH in diesem Urteil aber entschieden, dass die Kategorien der nach der genannten Richtlinie und diesen nationalen Regelungen auf Vorrat gespeicherten Daten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen – 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 – und insbesondere die Erstellung eines Profils dieser Personen ermöglichen konnten.

[79] Darüber hinaus ist festzustellen, dass die in den Ausgangsverfahren in Rede stehende Regelung zwar nicht die Daten über die aufgerufenen Internetseiten erfasst, wohl aber die Speicherung der IP-Adressen vorsieht. Diese Adressen können jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und in Folge dessen seiner Online-Aktivität genutzt werden, so dass diese Daten die Erstellung eines detaillierten Profils dieses Nutzers ermöglichen. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar (vgl. idS Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 153 – La Quadrature du Net ua).

[80] Außerdem stellen, wie SpaceNet in ihren schriftlichen Erklärungen ausgeführt hat, die Daten betreffend E-Mail-Dienste, auch wenn sie nicht von der in der in den Ausgangsverfahren in Rede stehenden Regelung vorgesehenen Pflicht zur Vorratsspeicherung erfasst werden, nur einen Bruchteil der in Rede stehenden Daten dar.

[81] Wie der Generalanwalt in Rn. 60 seiner Schlussanträge (Campos Sánchez-Bordona ECLI:EU:C:2021:939 = BeckRS 2021, 35300) im Kern ausgeführt hat, erstreckt sich die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Pflicht zur Vorratsspeicherung somit auf einen umfangreichen Satz von Verkehrs- und Standortdaten, der im Wesentlichen denjenigen entspricht, die zu der ständigen Rechtsprechung geführt haben, auf die in Rn. 78 des vorliegenden Urteils hingewiesen worden ist.

[82] Des Weiteren hat die deutsche Regierung in Beantwortung einer in der mündlichen Verhandlung gestellten Frage ausgeführt, dass in der Liste der Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen lediglich 1.300 Stellen aufgeführt seien, deren Daten betreffend die elektronische Kommunikation nicht nach § 99 II und § 113b VI TKG auf Vorrat gespeichert würden, was offensichtlich einen geringen Teil aller Nutzer von Telekommunikationsdiensten in Deutschland darstellt, deren Daten unter die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehene Pflicht zur Vorratsspeicherung fallen. So werden ua Daten von Nutzern gespeichert,

die dem Berufsgeheimnis unterliegen, wie beispielsweise Rechtsanwälte, Ärzte und Journalisten.

[83] Aus der Vorlageentscheidung geht somit hervor, dass die in dieser nationalen Regelung vorgesehene Vorratsspeicherung von Verkehrs- und Standortdaten nahezu alle die Bevölkerung bildenden Personen betrifft, ohne dass diese sich auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte. Ebenso schreibt sie die anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vor, deren Umfang im Wesentlichen dem der Daten entspricht, die in den Rechtssachen gespeichert wurden, die zu der in Rn. 78 des vorliegenden Urteils angeführten Rechtsprechung geführt haben.

[84] In Anbetracht der in Rn. 75 des vorliegenden Urteils angeführten Rechtsprechung kann daher eine Verpflichtung zur Vorratsdatenspeicherung wie die in den Ausgangsverfahren in Rede stehende entgegen dem Vorbringen der deutschen Regierung nicht als gezielte Vorratsdatenspeicherung angesehen werden.

[85] Zweitens ergibt sich, was die Vorratsspeicherungsfrist anbelangt, aus Art. 15 I 2 RL 2002/58, dass die Vorratsspeicherungsfrist, die eine nationale Maßnahme vorsieht, die eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorschreibt, zwar ein relevanter Faktor unter anderen ist, um zu bestimmen, ob das Unionsrecht einer solchen Maßnahme entgegensteht, wobei der genannte S. 2 verlangt, dass diese Frist „begrenzt" sein muss.

[86] Im vorliegenden Fall sind diese Fristen, die gem. § 113 b I TKG vier Wochen für Standortdaten und zehn Wochen für sonstige Daten betragen, zwar deutlich kürzer als die Fristen, die in den nationalen Regelungen, die eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung vorschreiben, vorgesehen sind, die der EuGH in seinen Urteilen (EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 Sverige und Watson ua; EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = EuZW 2022, 536 Ls. = BeckRS 2022, 6441 – Commissioner of An Garda Síochána ua) geprüft hat.

[87] Wie aus der in Rn. 61 des vorliegenden Urteils angeführten Rechtsprechung hervorgeht, ergibt sich die Schwere des Eingriffs jedoch aus der Gefahr, dass die auf Vorrat gespeicherten Daten insbesondere in Anbetracht ihrer Menge und Vielfalt es in ihrer Gesamtheit ermöglichen, sehr genaue Schlüsse auf das Privatleben der Person bzw. der Personen zu ziehen, deren Daten gespeichert wurden, und insbesondere die Erstellung eines Profils der betroffenen Person bzw. der betroffenen Personen ermöglichen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

[88] Folglich ist die Speicherung von Verkehrs- oder Standortdaten, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte liefern können, in jedem Fall schwerwiegend, unabhängig von der Länge des Speicherzeitraums und von der Menge oder Art der gespeicherten Daten, sofern der Datensatz geeignet ist, sehr genaue Schlüsse auf das Privatleben der betroffenen Person bzw. der betroffenen Personen zuzulassen (vgl. zum Zugang zu solchen Daten EuGH ECLI:EU:C:2021:152 = EuZW 2021, 316 Rn. 39 – Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation] (C-746/18)).

[89] Insoweit können selbst die Speicherung einer begrenzten Menge von Verkehrs- oder Standortdaten oder die Speicherung dieser Daten über einen kurzen Zeitraum geeignet sein, sehr genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern. Außerdem können die Menge der verfügbaren Daten und die daraus resultierenden sehr genauen Informationen über das Privatleben des Betroffenen erst nach Konsultation der fraglichen Daten beurteilt werden. Der sich aus der Speicherung der genannten Daten ergebende Eingriff erfolgt aber notwendigerweise, bevor die Daten und die daraus resultierenden Informationen konsultiert werden können. Somit erfolgt die Beurteilung der Schwere des in der Speicherung bestehenden Eingriffs notwendigerweise anhand der mit der Kategorie gespeicherter Daten allgemein verbundenen Gefahr für das Privatleben der Betroffenen, ohne dass es überdies darauf ankommt, ob die daraus resultierenden Informationen über das Privatleben im konkreten Fall sensiblen Charakter haben (vgl. idS EuGH ECLI:EU:C:2021:152 = EuZW 2021, 316 Rn. 40 – Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation]).

[90] Im vorliegenden Fall kann, wie aus Rn. 77 des vorliegenden Urteils hervorgeht und in der mündlichen Verhandlung bestätigt worden ist, ein Satz von Verkehrs- und Standortdaten, die zehn Wochen bzw. vier Wochen lang gespeichert werden, sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden – 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-, und insbesondere die Erstellung eines Profils dieser Personen ermöglichen.

[91] Drittens ist in Bezug auf die in der in den Ausgangsverfahren in Rede stehenden nationalen Regelung vorgesehenen Garantien, die die gespeicherten Daten gegen Missbrauchsrisiken und vor jedem unberechtigten Zugang schützen sollen, festzustellen, dass die Vorratsspeicherung dieser Daten und der Zugang zu ihnen, wie sich aus der in Rn. 60 des vorliegenden Urteils angeführten Rechtsprechung ergibt, unterschiedliche Eingriffe in die in den Art. 7 und 11 der Charta garantierten Grundrechte darstellen, die eine gesonderte Rechtfertigung nach Art. 52 I der Charta erfordern. Daraus folgt, dass nationale Rechtsvorschriften, die die vollständige Einhaltung der Voraussetzungen gewährleisten, die sich im Bereich des Zugangs zu auf Vorrat gespeicherten Daten aus der Rechtsprechung zur Auslegung RL 2002/58 ergeben, naturgemäß den schwerwiegenden Eingriff weder beschränken noch beseitigen können, der sich aus der nach diesen nationalen Rechtsvorschriften vorgesehenen allgemeinen Vorratsspeicherung dieser Daten in die Rechte ergeben würde, die in den Art. 5 und 6 dieser Richtlinie und in den durch diese Vorschriften konkretisierten Grundrechten garantiert werden (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 47 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[92] Viertens und letztens hat der EuGH, was das Vorbringen der Europäischen Kommission anbelangt, wonach besonders schwere Kriminalität einer Bedrohung der nationalen Sicherheit gleichgestellt werden könne, bereits ent-

schieden, dass das Ziel der Wahrung der nationalen Sicherheit dem zentralen Anliegen entspricht, die wesentlichen Funktionen des Staats und die grundlegenden Interessen der Gesellschaft durch die Verhütung und Repression von Tätigkeiten zu schützen, 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 etwa terroristische Aktivitäten (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 61 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[93] Im Unterschied zur Kriminalität – auch besonders schwerer Kriminalität – muss eine Bedrohung für die nationale Sicherheit real und aktuell, zumindest aber vorhersehbar sein, was das Eintreten hinreichend konkreter Umstände voraussetzt, um eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung von Verkehrs- und Standortdaten für einen begrenzten Zeitraum rechtfertigen zu können. Eine solche Bedrohung unterscheidet sich somit ihrer Art, ihrer Schwere und der Besonderheit der sie begründenden Umstände nach von der allgemeinen und ständigen Gefahr, dass – auch schwere – Spannungen oder Störungen der öffentlichen Sicherheit auftreten, oder schwerer Straftaten (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 62 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[94] Somit kann Kriminalität – auch besonders schwere Kriminalität – nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden. Eine solche Gleichstellung könnte nämlich eine Zwischenkategorie zwischen der nationalen Sicherheit und der öffentlichen Sicherheit einführen, um auf die zweite Kategorie die Voraussetzungen der ersten Kategorie anzuwenden (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 63 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

Zu den Maßnahmen, die eine gezielte Vorratsspeicherung, eine umgehende Sicherung oder eine Speicherung der IP-Adressen vorsehen

[95] Mehrere Regierungen, darunter die französische Regierung, betonen, dass nur eine allgemeine und unterschiedslose Vorratsspeicherung die wirksame Verwirklichung der mit den Speicherungsmaßnahmen verfolgten Ziele ermögliche; die deutsche Regierung führt im Wesentlichen aus, dass diese Schlussfolgerung nicht dadurch entkräftet werde, dass die Mitgliedstaaten auf die in Rn. 75 des vorliegenden Urteils genannten Maßnahmen der gezielten Vorratsspeicherung und umgehenden Sicherung zurückgreifen könnten.

[96] Hierzu ist erstens festzustellen, dass die Wirksamkeit der Strafverfolgung im Allgemeinen nicht von einem einzigen Ermittlungsinstrument abhängt, sondern von allen Ermittlungsinstrumenten, über die die zuständigen nationalen Behörden zu diesem Zweck verfügen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 69 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[97] Zweitens gestattet Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta in seiner Auslegung durch die in Rn. 75 des vorliegenden Urteils angeführte Rechtsprechung es den Mitgliedstaaten, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit nicht nur Rechtsvorschriften zur Einführung einer gezielten Vorratsspeicherung und einer umgehenden Sicherung zu erlassen, sondern auch Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratsspeicherung von zum einen der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten und zum anderen der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 70 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[98] Insoweit steht fest, dass die Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten zur Bekämpfung schwerer Kriminalität beitragen kann, sofern diese Daten es ermöglichen, die Personen zu identifizieren, die solche Kommunikationsmittel im Zusammenhang mit der Vorbereitung oder Begehung einer zur schweren Kriminalität zählenden Tat verwendet haben (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 71 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[99] Die RL 2002/58 steht aber einer allgemeinen Vorratsspeicherung der die Identität betreffenden Daten für die Zwecke der Bekämpfung der Kriminalität im Allgemeinen nicht entgegen. Unter diesen Umständen ist klarzustellen, dass weder diese Richtlinie noch irgendein anderer Unionsrechtsakt nationalen Rechtsvorschriften entgegenstehen, die die Bekämpfung schwerer Kriminalität zum Gegenstand haben und nach denen der Erwerb eines elektronischen Kommunikationsmittels wie einer vorausbezahlten SIM-Karte von der Überprüfung amtlicher Dokumente, die die Identität des Käufers belegen, und der Erfassung der sich daraus ergebenden Informationen durch den Verkäufer abhängig ist, wobei der Verkäufer gegebenenfalls verpflichtet ist, den zuständigen nationalen Behörden Zugang zu diesen Informationen zu gewähren (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 72 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[100] Außerdem ist darauf hinzuweisen, dass die allgemeine Speicherung der IP-Adressen der Quelle der Verbindung einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte darstellt, da diese IP-Adressen es ermöglichen können, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen, und abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 der Charta garantierten Freiheit der Meinungsäußerung haben kann. Allerdings hat der EuGH in Bezug auf eine solche Speicherung festgestellt, dass, um die widerstreitenden Rechte und berechtigten Interessen miteinander in Einklang zu bringen, wie es die in den Rn. 65-68 des vorliegenden Urteils angeführte Rechtsprechung verlangt, zu berücksichtigen ist, dass im Fall einer im Internet begangenen Straftat und insbesondere im Fall des Erwerbs, der Verbreitung, der Weitergabe oder der Bereitstellung im Internet von Kinderpornografie iSv Art. 2 Buchst. c RL 2011/93/EU des Europäischen Parlaments und des Rates vom 13.12.2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. 2011 L 335, 1, berichtigt in ABl. 2012 L 18, 7) die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 73 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[101] Unter diesen Umständen trifft es zwar zu, dass eine Rechtsvorschrift, die eine Vorratsspeicherung der IP-Adressen aller natürlichen Personen vorsieht, denen ein Endgerät gehört, von dem aus ein Internetzugang möglich ist, Personen erfassen würde, die prima facie keinen Zusammenhang mit den verfolgten Zielen im Sinne der in Rn. 70 des vorliegenden Urteils angeführten Rechtsprechung aufweisen, und dass die Internetnutzer nach der Feststellung in Rn. 54 des vorliegenden Urteils aufgrund der Art. 7 und 8 der Charta erwarten dürfen, dass ihre Identität grundsätzlich nicht preisgegeben wird. Gleichwohl verstößt eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 155 – La Quadrature du Net ua).

[102] Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, sind neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 156 – La Quadrature du Net ua).

[103] Entgegen den Ausführungen des vorlegenden Gerichts besteht somit kein Spannungsverhältnis zwischen den Rn. 155 u. 168 des Urteils vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua). Wie der Generalanwalt in den Rn. 81 und 82 seiner Schlussanträge (Campos Sánchez-Bordona ECLI:EU:C:2021:939 = BeckRS 2021, 35300) im Kern ausgeführt hat, geht nämlich aus dieser Rn. 155 iVm Rn. 156 und Rn. 168 dieses Urteils klar hervor, dass neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet sind, die allgemeine Vorratsspeicherung der der Quelle einer Verbindung zugewiesenen IP-Adressen zu rechtfertigen, unabhängig davon, ob die betroffenen Personen einen zumindest mittelbaren Zusammenhang mit den verfolgten Zielen aufweisen.

[104] Was drittens die Rechtsvorschriften betrifft, die eine gezielte Vorratsspeicherung und eine umgehende Sicherung der Verkehrs- und Standortdaten vorsehen, lassen bestimmte, von den Mitgliedstaaten in Bezug auf solche Maßnahmen dargelegte Erwägungen ein engeres Verständnis der Tragweite dieser Vorschriften erkennen als das, das der in Rn. 75 des vorliegenden Urteils angeführten Rechtsprechung zugrunde liegt. Denn auch wenn diese Maßnahmen der Speicherung, wie in Rn. 57 des vorliegenden Urteils ausgeführt worden ist, in dem durch die RL 2002/58 geschaffenen System Ausnahmecharakter haben müssen, so macht diese Richtlinie im Licht der in den Art. 7, 8 und 11 sowie in Art. 52 I der Charta verankerten Grundrechte die Möglichkeit, eine Anordnung zur gezielten Vorratsspeicherung zu erlassen, gleichwohl nicht von den Voraussetzungen abhängig, dass im Voraus bekannt ist, an welchen Orten eine schwere Straftat begangen werden könnte oder welche Personen verdächtigt werden, an einer solchen Tat beteiligt zu sein. Ebenso wenig verlangt die Richtlinie, dass die Anordnung, mit der eine umgehende Sicherung angeordnet wird, auf Verdächtige beschränkt wird, die vor einer solchen Anordnung identifiziert wurden (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 75 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[105] Was erstens die gezielte Vorratsspeicherung anbelangt, so hat der EuGH entschieden, dass Art. 15 I RL 2002/58 auf objektiven Kriterien beruhenden nationalen Rechtsvorschriften nicht entgegensteht, mit denen zum einen Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, 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:2022:258 = BeckRS 2022, 6441 Rn. 76 mwN = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[106] Der EuGH hat insoweit klargestellt, dass diese objektiven Kriterien zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterschiedlich sein können, zu den erfassten Personen aber insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver und nicht diskriminierender Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 77 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[107] Die Mitgliedstaaten haben somit ua die Möglichkeit, Maßnahmen zur Speicherung zu ergreifen, die Personen betreffen, die aufgrund einer solchen Einstufung Gegenstand aktueller Ermittlungen oder anderer Überwachungsmaßnahmen sind oder zu denen im nationalen Strafregister eine frühere Verurteilung wegen schwerer Straftaten vermerkt ist, die ein hohes Rückfallrisiko bedeuten können. Beruht eine solche Einstufung aber auf objektiven und nicht diskriminierenden Kriterien, die im nationalen Recht festgelegt sind, so ist die gezielte Vorratsspeicherung in Bezug auf so eingestufte Personen gerechtfertigt (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 78 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[108] Zum anderen kann eine Maßnahme gezielter Vorratsspeicherung von Verkehrs- und Standortdaten nach Wahl des nationalen Gesetzgebers und unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit auch auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nicht diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht. Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Seehäfen,

Bahnhöfe oder Mautstellen (EuGH ECLI:EU:C:2022:258 = EuZW 2022, 536 – Commissioner of An Garda Síochána ua Rn. 79 mwN).

[109] Es ist hervorzuheben, dass nach dieser Rspr. die zuständigen nationalen Behörden für die in der vorstehenden Rn. genannten Gebiete eine Maßnahme der gezielten Vorratsspeicherung auf der Grundlage eines geografischen Kriteriums wie ua der durchschnittlichen Kriminalitätsrate in einem geografischen Gebiet treffen können, ohne dass sie zwingend über konkrete Anhaltspunkte für die Vorbereitung oder die Begehung schwerer Straftaten in den betreffenden Gebieten verfügen müssten. Da eine gezielte Vorratsspeicherung, die auf einem solchen Kriterium beruht, je nach den betreffenden schweren Straftaten und der den jeweiligen Mitgliedstaaten eigenen Situation sowohl Orte betreffen kann, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, als auch Orte, die für die Begehung solcher Straftaten besonders anfällig sind, kann sie grundsätzlich auch nicht zu Diskriminierungen führen, da das Kriterium der durchschnittlichen Rate schwerer Straftaten als solches keine Verbindung zu potenziell diskriminierenden Elementen aufweist (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 80 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[110] Außerdem und va ermöglicht eine gezielte Vorratsspeicherung in Bezug auf Orte oder Infrastrukturen, die regelmäßig von einer sehr großen Zahl von Personen frequentiert werden, oder auf strategische Orte wie Flughäfen, Bahnhöfe, Seehäfen oder Mautstellen den zuständigen Behörden, Verkehrsdaten und insbesondere Standortdaten aller Personen zu sammeln, die zu einem bestimmten Zeitpunkt an einem dieser Orte ein elektronisches Kommunikationsmittel benutzen. Eine solche Maßnahme der gezielten Vorratsspeicherung kann es diesen Behörden somit ermöglichen, durch den Zugang zu den so gespeicherten Daten Informationen über die Anwesenheit dieser Personen an den Orten oder in den geografischen Gebieten, auf die sich diese Maßnahme bezieht, sowie über ihre Bewegungen zwischen oder innerhalb dieser Orte oder geografischen Gebiete zu erhalten und daraus zum Zweck der Bekämpfung schwerer Kriminalität Schlüsse über ihre Anwesenheit und ihre Tätigkeit an diesen Orten oder in diesen geografischen Gebieten zu einem bestimmten Zeitpunkt während des Speicherungszeitraums zu ziehen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 81 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[111] Ferner ist darauf hinzuweisen, dass die geografischen Gebiete, auf die sich eine solche gezielte Vorratsspeicherung bezieht, geändert werden können und gegebenenfalls müssen, wenn sich die Bedingungen, die ihre Auswahl gerechtfertigt haben, ändern, so dass insbesondere auf die Entwicklungen bei der Bekämpfung schwerer Kriminalität reagiert werden kann. Der EuGH hat nämlich bereits entschieden, dass die Dauer der in den Rn. 105-110 des vorliegenden Urteils beschriebenen Maßnahmen gezielter Speicherung das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige nicht überschreiten darf, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 151 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 82 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[112] Was die Möglichkeit betrifft, andere Unterscheidungskriterien als ein persönliches oder geografisches Kriterium für die Durchführung einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten vorzusehen, so kann nicht ausgeschlossen werden, dass andere objektive und nicht diskriminierende Kriterien in Betracht kommen, um sicherzustellen, dass der Umfang einer gezielten Vorratsspeicherung auf das absolut Notwendige beschränkt wird, und um eine zumindest indirekte Verbindung zwischen den schweren Straftaten und den Personen, deren Daten auf Vorrat gespeichert werden, herzustellen. Da sich Art. 15 I RL 2002/58 auf Rechtsvorschriften der Mitgliedstaaten bezieht, obliegt es allerdings diesen und nicht dem EuGH, solche Kriterien zu bestimmen, wobei es nicht darum gehen kann, auf diesem Weg wieder eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und Standortdaten einzuführen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 83 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[113] Wie der Generalanwalt in Rn. 50 seiner Schlussanträge (Campos Sánchez-Bordona ECLI:EU:C:2021:939 = BeckRS 2021, 35300) ausgeführt hat, kann jedenfalls das etwaige Bestehen von Schwierigkeiten bei der genauen Bestimmung der Fälle und Bedingungen, in bzw. unter denen eine gezielte Vorratsspeicherung durchgeführt werden kann, nicht rechtfertigen, dass Mitgliedstaaten, indem sie die Ausnahme zur Regel machen, eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten vorsehen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 84 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[114] Was zweitens die umgehende Sicherung der von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 RL 2002/58 oder auf der Grundlage von Rechtsvorschriften, die gem. Art. 15 I dieser Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten anbelangt, ist darauf hinzuweisen, dass solche Daten grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, je nach Fall, entweder gelöscht oder anonymisiert werden müssen. Allerdings hat der EuGH entschieden, dass während dieser Verarbeitung und Speicherung Situationen auftreten können, 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 (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 85 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[115] In einer solchen Situation steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in den Rn. 65-68 des vorliegenden Urteils die widerstreitenden Rechte und berechtigten 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 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209

Rn. 163 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 86 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[116] 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 Charta 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 in den Art. 7 und 8 der Charta verankerten Grundrechte, 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, sofern diese Maßnahme sowie der Zugang zu den auf Vorrat gespeicherten Daten die Grenzen des absolut Notwendigen, wie sie in den Rn. 164-167 des Urteils vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 163 – La Quadrature du Net ua) dargelegt sind, einhalten (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 87 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[117] Der EuGH hat klargestellt, dass sich eine derartige Maßnahme der Vorratsspeicherung nicht auf die Daten der Personen beschränken muss, die zuvor als Bedrohung für die öffentliche oder nationale Sicherheit des betreffenden Mitgliedstaats identifiziert wurden, oder von Personen, die konkret im Verdacht stehen, eine schwere Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben. Nach Auffassung des EuGH kann nämlich unter Beachtung des durch Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta vorgegebenen Rahmens und angesichts der Erwägungen in Rn. 70 des vorliegenden Urteils eine solche Maßnahme nach Wahl des nationalen 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 sowie seines sozialen oder beruflichen Umfelds (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 165 – La Quadrature du Net ua, sowie EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 88 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[118] Somit kann eine Rechtsvorschrift es gestatten, gegenüber den Betreibern elektronischer Kommunikationsdienste anzuordnen, die Verkehrs- und Standortdaten ua von Personen, mit denen ein Opfer vor dem Auftreten einer schweren Bedrohung der öffentlichen Sicherheit oder der Begehung einer schweren Straftat unter Verwendung seiner elektronischen Kommunikationsmittel in Kontakt gestanden hat, umgehend zu sichern (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 89 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[119] Eine solche umgehende Sicherung kann nach der in Rn. 117 des vorliegenden Urteils angeführten Rechtsprechung des EuGH unter den in dieser Rn. genannten Voraussetzungen auch auf bestimmte geografische Gebiete wie die Orte der Begehung und Vorbereitung der Straftat oder der betreffenden Beeinträchtigung der nationalen Sicherheit ausgedehnt werden. Es ist klarzustellen, dass Gegenstand einer solchen Maßnahme auch die Verkehrs- und Standortdaten sein können, die sich auf den Ort beziehen, an dem eine Person, die möglicherweise Opfer einer schweren Straftat ist, verschwunden ist, sofern diese Maßnahme sowie der Zugang zu den auf diese Weise auf Vorrat gespeicherten Daten die Grenzen des für die Bekämpfung schwerer Straftaten oder den Schutz der nationalen Sicherheit absolut Notwendigen, wie sie in den Rn. 164-167 des Urteils vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) dargelegt sind, einhalten (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 90 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[120] Außerdem ist klarzustellen, dass Art. 15 I RL 2002/58 die zuständigen nationalen Behörden nicht daran hindert, bereits im ersten Stadium der Ermittlungen bezüglich einer schweren Bedrohung der öffentlichen Sicherheit oder einer möglichen schweren Straftat, dh ab dem Zeitpunkt, zu dem diese Behörden nach den einschlägigen Bestimmungen des nationalen Rechts solche Ermittlungen einleiten können, eine umgehende Sicherung anzuordnen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 91 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[121] Was des Weiteren die Vielfalt der in Rn. 75 des vorliegenden Urteils genannten Maßnahmen der Vorratsspeicherung der Verkehrs- und Standortdaten betrifft, ist klarzustellen, dass diese verschiedenen Maßnahmen nach der Wahl des nationalen Gesetzgebers und unter Einhaltung der Grenzen des absolut Notwendigen zusammen Anwendung finden können. Unter diesen Umständen steht Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta in der Auslegung durch die auf das Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) zurückgehende Rechtsprechung einer Kombination dieser Maßnahmen nicht entgegen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 92 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[122] Viertens und letztens ist darauf hinzuweisen, dass, wie sich aus dem die stRspr des EuGH zusammenfassenden Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) ergibt, die Verhältnismäßigkeit der nach Art. 15 I RL 2002/58 getroffenen Maßnahmen die Einhaltung nicht nur der Erfordernisse der Geeignetheit und der Erforderlichkeit verlangt, sondern auch des Erfordernisses, dass diese Maßnahmen in einem angemessenen Verhältnis zum verfolgten Ziel stehen müssen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 93 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[123] In diesem Zusammenhang ist darauf hinzuweisen, dass der EuGH in Rn. 51 des Urteils vom 8.4.2014 (EuGH ECLI:EU:C:2014:238 = EuZW 2014, 459 – Digital Rights Ireland ua (C-293/12)) entschieden hat, dass zwar die Bekämpfung schwerer Kriminalität von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann; eine solche dem Gemeinwohl dienende Zielsetzung kann aber, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Maßnahme der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten – wie sie die RL 2006/24 vorsieht – nicht rechtfertigen (EuGH

ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 94 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[124] Im selben Sinne hat der EuGH in Rn. 145 des Urteils vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 – La Quadrature du Net ua) klargestellt, dass selbst die positiven Verpflichtungen der Mitgliedstaaten – die sich, je nach Fall, aus den Art. 3, 4 und 7 der Charta ergeben können und, wie in Rn. 64 des vorliegenden Urteils ausgeführt worden ist, die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen – keine so schwerwiegenden Eingriffe rechtfertigen können, wie sie mit nationalen Rechtsvorschriften, die eine Speicherung von Verkehrs- und Standortdaten vorsehen, für die in den Art. 7 und 8 der Charta verankerten Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 95 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[125] Im Übrigen sind die Urteile des EGMR vom 25.5.2021 – Big Brother Watch ua/Vereinigtes Königreich (EGMR ECLI:CE:ECHR:2021:0525JUD005817013 = BeckRS 2021, 11635) und vom 25.5.2021 – Centrum för Rättvisa/Schweden (EGMR ECLI:CE:ECHR:2021:0525JUD003525208 = BeckRS 2021, 11638), die von einigen Regierungen in der mündlichen Verhandlung angeführt worden sind, um geltend zu machen, dass die EMRK nationalen Regelungen, die im Wesentlichen eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsähen, nicht entgegenstehe, nicht geeignet, die Auslegung von Art. 15 I RL 2002/58, die sich aus den vorstehenden Ausführungen ergibt, infrage zu stellen. In diesen Urteilen ging es nämlich um das massenhafte Abfangen von Daten betreffend internationale Kommunikationen. Somit hat der EGMR, wie die Kommission in der mündlichen Verhandlung ausgeführt hat, in den genannten Urteilen weder über die Vereinbarkeit einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten im Inland noch auch nur über ein Abfangen dieser Daten in großem Umfang zur Verhütung, Feststellung und Ermittlung schwerer Straftaten mit der EMRK entschieden. Jedenfalls ist darauf hinzuweisen, dass mit Art. 52 III der Charta die notwendige Kohärenz zwischen den in der Charta enthaltenen Rechten und den entsprechenden durch die EMRK garantierten Rechten gewährleistet werden soll, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des EuGH berührt wird, so dass die entsprechenden Rechte der EMRK bei der Auslegung der Charta nur als Mindestschutzstandard zu berücksichtigen sind (EuGH ECLI:EU:C:2020:1031 = NVwZ 2021, 219 Rn. 56 – Centraal Israëlitisch Consistorie van België ua (C-336/19)).

Zum Zugang zu Daten, die allgemein und unterschiedslos auf Vorrat gespeichert wurden

[126] In der mündlichen Verhandlung hat die dänische Regierung vorgebracht, dass die zuständigen nationalen Behörden zum Zweck der Bekämpfung schwerer Kriminalität Zugang zu Verkehrs- und Standortdaten haben müssten, die gemäß der aus dem Urteil vom 6.10.2020 (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 Rn. 135-139 – La Quadrature du Net ua) hervorgegangenen Rechtsprechung allgemein und unterschiedslos auf Vorrat gespeichert worden seien, um einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit zu begegnen.

[127] Zunächst ist festzustellen, dass die Gestattung des Zugangs zu allgemein und unterschiedslos auf Vorrat gespeicherten Verkehrs- und Standortdaten zum Zweck der Bekämpfung schwerer Kriminalität diesen Zugang von Umständen abhängig machen würde, die mit diesem Ziel nichts zu tun haben – je nachdem, ob in dem betreffenden Mitgliedstaat eine ernste Bedrohung für die nationale Sicherheit im Sinne der vorstehenden Rn. besteht oder nicht –, während im Hinblick auf das alleinige Ziel der Bekämpfung schwerer Kriminalität, das die Speicherung dieser Daten und den Zugang zu ihnen rechtfertigen soll, nichts eine unterschiedliche Behandlung insbesondere zwischen den Mitgliedstaaten rechtfertigen würde (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 97 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[128] Wie der EuGH bereits entschieden hat, kann der Zugang zu von Betreibern elektronischer Kommunikationsdienste in Anwendung einer gem. Art. 15 I RL 2002/58 erlassenen Rechtsvorschrift auf Vorrat gespeicherten Verkehrs- und Standortdaten, der unter vollständiger Beachtung der sich aus der Rechtsprechung zur Auslegung dieser Richtlinie ergebenden Voraussetzungen zu erfolgen hat, grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden, zu dem die Speicherung den Betreibern auferlegt wurde. Etwas anderes gilt nur, wenn die Bedeutung des mit dem Zugang verfolgten Ziels die Bedeutung des Ziels, das die Speicherung gerechtfertigt hat, übersteigt (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 98 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[129] Das Vorbringen der dänischen Regierung bezieht sich aber auf eine Situation, in der das Ziel des beabsichtigten Zugangsersuchens, nämlich die Bekämpfung schwerer Kriminalität, in der Hierarchie der dem Gemeinwohl dienenden Ziele von geringerer Bedeutung ist als das Ziel, das die Speicherung rechtfertigte, nämlich der Schutz der nationalen Sicherheit. In einer solchen Situation Zugang zu den auf Vorrat gespeicherten Daten zu gewähren, würde gegen die Hierarchie der dem Gemeinwohl dienenden Ziele verstoßen, auf die in der vorstehenden Rn. sowie in den Rn. 68, 71, 72 und 73 dieses Urteils hingewiesen worden ist (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 99 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[130] Außerdem und va dürfen nach der in Rn. 74 des vorliegenden Urteils angeführten Rechtsprechung Verkehrs- und Standortdaten für die Zwecke der Bekämpfung schwerer Kriminalität nicht allgemein und unterschiedslos auf Vorrat gespeichert werden, so dass auch der Zugang zu diesen Daten zu diesen Zwecken nicht gerechtfertigt sein kann. Wenn diese Daten ausnahmsweise allgemein und unterschiedslos zum Schutz der nationalen Sicherheit vor einer Bedrohung, die als real und aktuell oder vorhersehbar einzustufen ist, unter den in Rn. 71 des vorliegenden Urteils genannten Voraussetzungen gespeichert wurden, dürfen die für strafrechtliche Ermittlungen zuständigen nationalen Behörden im Rahmen der Strafverfolgung nicht auf diese Daten zugreifen, da sonst das in Rn. 74 genannte Verbot einer solchen Speicherung zum Zweck der Bekämpfung schwerer Straftaten seine praktische Wirksamkeit verlieren würde (EuGH ECLI:EU:C:2022:258 = BeckRS 2022, 6441 Rn. 100 = EuZW 2022, 536 Ls. – Commissioner of An Garda Síochána ua).

[131] Nach alledem ist auf die Vorlagefrage zu antworten, dass Art. 15 I RL 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta dahin auszulegen ist, dass er nationalen Rechtsvorschriften

entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen ist der genannte Art. 15 I im Licht der Art. 7, 8 und 11 sowie von Art. 52 I der Charta dahin auszulegen, dass er nationalen Rechtsvorschriften nicht entgegensteht, 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 der 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.

Anmerkung von Akademische Rätin a.Z. Dr. Aqilah Sandhu*

I. Hintergrund

Nach der grundrechtsfreundlichen Rechtsprechung des EuGH (EuGH ECLI:EU:C:2014:238 = EuZW 2014, 459 – Digital Rights (C-594/12, C-293/12) und EuGH ECLI:EU:C:2016:970 = EuZW 2017, 153 – Tele2 (C-698/15)) hatten mehrere Fachgerichte die Pflicht zur Speicherung von Verkehrsdaten nach § 113a I iVm § 113b TKG für unionsrechtswidrig und unanwendbar erklärt (OVG Münster NVwZ-RR 2018, 43; VG Köln ZD 2019, 187) und die BNetzA die Speicherpflicht bis zur Hauptsacheentscheidung ausgesetzt. Ein acte clair lag auf der Hand, dennoch legte das im Fall des VG Köln im Wege der Sprungrevision angerufene BVerwG die Frage der Vereinbarkeit der deutschen Regelung mit RL 2002/58 dem EuGH vor (Vorlage v. 25.9.2019 BeckRS 2019, 26126). Die nun ergangene Antwort war schon zum Zeitpunkt ihrer Einlegung weitgehend vorhersehbar (vgl. nur Sandhu EuR 2017, 453). Wohl in der Erwartung, dass sich die deutsche Vorlage erledigen würde, hatte der EuGH zwischenzeitlich zur französischen, belgischen (EuGH ECLI:EU:C:2020:791 = EuZW 2021, 209 (mAnm Sandhu) – La Quadrature du Net ua (C-511/18, C-512/18)) und jüngst zur irischen Vorratsdatenspeicherung eindeutig entschieden (EuGH ECLI:EU:C:2022:258 = EuZW 2022, 536 – Commissioner of An Garda Síochána ua (C-140/20)), auf die er nun weitgehend verweist. Bemerkenswert ist die Entscheidung va, weil das BVerwG die Vorlage nicht spätestens nach der irischen Entscheidung zurückgenommen hat, was gem. Art. 100 I VerfO EuGH bis zur Bekanntgabe des Termins der Urteilsverkündung hätte erfolgen können. Eine Besprechung verdient diese Entscheidung aber dennoch: Zum einen, da sie neues Konfliktpontenzial im Verhältnis zum BVerfG birgt. Zum anderen, da die gezielte Vorratsdatenspeicherung auch Gleichheitsfragen aufwirft.

II. Bewertung

Es ist der Eigenheit grundrechtskonkretisierenden Sekundärrechts geschuldet, dass die grundrechtliche Vereinbarkeit maßgeblich am Maßstab einer Richtlinienbestimmung geprüft wird, um deren Umsetzung es gar nicht ging (vgl. schon Sandhu, Grundrechtskonkretisierung durch Sekundärrecht, 2021, 18 f.). So prüft der EuGH die TKG-Regelung am Maßstab des Art. 15 I RL 2002/58, der als Ausnahme von dem Grundsatz der Vertraulichkeit elektronischer Kommunikation restriktiv auszulegen ist (Rn. 57). Ergänzend rekurriert er auf Art. 52 I GRCh für den Grundsatz der Verhältnismäßigkeit. Eingegriffen wird nicht nur in Art. 8 GRCh, sondern auch in Art. 11 GRCh und Art. 7 GRCh, der eine positive Schutzpflicht enthält (Rn. 64). Die anlasslose und undifferenzierte Vorratsdatenspeicherung ist nur zum Schutz der nationalen Sicherheit zulässig, zur Bekämpfung schwerer Kriminalität muss sie gezielt bspw. in der Form des Quick Freeze erfolgen (Rn. 72 ff.).

Das BVerwG hatte an seiner Vorlage insbesondere deshalb festgehalten, weil die TKG-Regelungen den Inhalt der Kommunikation sowie Daten über aufgerufene Internetseiten von der Speicherpflicht ausnehmen. Doch darin hebt sich die deutsche Regelung nicht merklich von den anderen nationalen Regelungen ab. Der EuGH wiederholt seine damaligen Feststellungen, wonach auch Metadaten sehr genaue Rückschlüsse auf das Privatleben der betroffenen Personen zulassen und ein Profil über den Lebensalltag sowie soziale Beziehungen ergeben (Rn. 78). Die bloße Erfassung von Verkehrs- und Standortdaten ändert nichts an der Schwere des Grundrechtseingriffs.

Ein weiterer Unterschied zu den bisherigen Regelungen lag darin, dass Daten aus dem sozialen und kirchlichen Bereich gem. §§ 99 II, 113b VI TKG von der Speicherung ausgenommen wurden. Wie sich in der mündlichen Verhandlung ergab, handelt es sich dabei aber um nur 1.300 Stellen, die behördlich gelistet sind und von der Vorratsspeicherung nicht erfasst werden (Rn. 82). Dies vermag die Pauschalität und Intensität des Grundrechtseingriffs nicht zu relativieren. Insbesondere deshalb nicht, weil die elektronische Kommunikation von Berufsgeheimnisträgern uneingeschränkt der Speicherpflicht unterfällt (darauf schon hinweisend Sandhu EuR 2017, 453).

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

Schließlich hebt sich die deutsche Regelung hinsichtlich der kürzeren Speicherfristen von den anderen nationalen Bestimmungen, die dem EuGH vorlagen, ab. Die Speicherdauer ist aber nur einer von vielen Faktoren für die Verhältnismäßigkeit der Maßnahme. An dieser Stelle trifft der EuGH erstmals eine wirklich neue Aussage: Werden Verkehrs- und Standortdaten betreffend die elektronische Kommunikation massenhaft gespeichert, so dass sich genaue Schlüsse auf das Privatleben der Betroffenen ergeben, ist eine Speicherung „unabhängig von der Länge des Speicherzeitraums und von der Menge oder Art der gespeicherten Daten" ein schwerwiegender Eingriff (Rn. 88). Schon die Speicherung selbst ist ein gravierender Eingriff, unabhängig von der anschließenden Auswertung. Diesen schweren Eingriff auf der ersten Stufe können anschließende Garantien und Schutzvorkehrungen gegen Missbrauch nicht mehr beseitigen (Rn. 91). Damit hebt sich der EuGH vom BVerfG ab, das den Eingriff auf der Stufe der Speicherung noch marginalisierte. Nicht schon die Datensammlung sei schwerwiegend, erst der Abruf der Daten führe zu „konkreten Belastungen" und einer „möglicherweise irreparablen Beeinträchtigung" (BVerfG NVwZ 2016, 1240 Rn. 18). Es wird nun in der Hauptsacheentscheidung auf diese Belehrung durch den EuGH reagieren müssen. In einer der einstweiligen Anordnungen zu ebenjener TKG-Regelung folgte es jedenfalls dem Vorbringen der Antragssteller nicht, die Unionsrechtskonformität als „Vorfrage" der Verfassungsmäßigkeit zu beantworten (BVerfG 8.6.2016 – 1 BvR 229/16, BeckRS 2016, 48517 Rn. 9). Stattdessen behielt es sich schon die – längst durch den EuGH beantwortete – Frage, ob und wie die GRCh oder sonstiges Unionsrecht für die deutsche Vorratsdatenspeicherung von Bedeutung seien, für das Hauptsacheverfahren vor (ebda. Rn. 27). Die Anwendbarkeit des Unionsrechts bejahte der EuGH diesmal in nur einem Satz, auch wenn die Vorratsspeicherung dem Schutz der nationalen Sicherheit dient (Rn. 48; hierzu Gerhold DÖV 2022, 93). Der Datenschutz wird kaum das Feld sein, auf dem sich das Gericht durch Abhebung von der EuGH-Rechtsprechung im Verfassungsdialog noch profilieren könnte.

Konfliktstoff bergen die Ausführungen zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen, die der EuGH für zulässig erachtet, wenn sie auf die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit beschränkt ist (Rn. 97). Zwar handelt es sich auch dabei um einen schweren Eingriff in Art. 7, 8 und 11 GRCh, allerdings sei bei im Internet begangenen Straftaten die IP-Adresse oftmals der einzige Anhaltspunkt für die Ermittlungsbehörden (Rn. 100). Diese Vorratsdatenspeicherung dürfe nur zum Schutz der nationalen Sicherheit, der Bekämpfung schwerer Kriminalität und schwerer Bedrohungen der öffentlichen Ordnung erfolgen. Die Auswertung müsse strengen Garantien unterliegen und die Speicherdauer auf das absolut Notwendige beschränkt sein (Rn. 102).

Nur vermeintlich grundrechtsschonender sind schließlich die EuGH-Vorgaben zur gezielten Vorratsdatenspeicherung. In dem Bemühen, die Maßnahme möglichst restriktiv zu gestalten, wird einem Profiling das Wort geredet. Die Einschränkung der Speichermaßnahme auf einen bestimmten Personenkreis sowie bestimmte Orte muss zwar auf objektiven Kriterien beruhen (Rn. 105). Diese können sich je nach den zu verfolgenden schweren Straftaten unterscheiden. Sie kann sich insbesondere auf diejenigen Personen erstrecken, die zuvor „im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver und nicht diskriminierender Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden" (Rn. 106). So kann sich die Vorratsdatenspeicherung auf Personen beschränken, die „Gegenstand aktueller Ermittlungen oder anderer Überwachungsmaßnahmen sind" oder die bereits im Strafregister wegen schwerer Straftaten erfasst sind (Rn. 107). Ebenso problematisch erscheint die Beschränkung auf geografische Gebiete (Rn. 108), zumal bei der Bekämpfung von Straftaten, die mittels elektronischer Kommunikation begangen wurden. Der EuGH erwähnt strategische Orte, wie Flughäfen, Seehäfen oder Bahnhöfe (Rn. 108). Doch eine derart geografisch umgrenzte Vorratsdatenspeicherung steht hinsichtlich ihrer Streubreite der undifferenzierten in nichts nach, zumal der EuGH ja selbst betont, dass der Vorteil dieser Orte darin liege, dass sie von einer „sehr großen Zahl von Personen frequentiert werden" (Rn. 110). Ausreichend für die Speichermaßnahme an einem bestimmten Ort soll etwa die durchschnittliche Kriminalitätsrate sein, unabhängig davon, dass konkrete Anhaltspunkte für die Vorbereitung schwerer Straftaten in den betreffenden Gebieten bestehen müssen. Die hierin offenkundig liegende Gefahr von Diskriminierungen weist der EuGH pauschal zurück: Die Anknüpfung an die Kriminalitätsrate oder auch nur Anfälligkeit für Kriminalität sei per se ein objektives Kriterium (Rn. 109). Dies verkennt jedoch die Verknüpfung von Armut sowie ethnischer und sozialer Herkunft in urbanen Ballungsräumen, die zu rassistischer Diskriminierung einlädt. Als Paradebeispiel mag der Fall CHEZ Razpredelenie Bulgaria dienen, in dem ein Stadtviertel mit einer Bevölkerung von überwiegender Roma-Herkunft bei der Anbringung von Stromzählern benachteiligt wurde. Zum Schutz vor illegalen Stromentnahmen, Manipulationen und Betrug, wurden in diesem Stadtteil die Stromzähler höher angebracht als in den anderen Stadtteilen. Auf Statistiken konnte sich der Betreiber nicht berufen, vielmehr erfolgte die Benachteiligung mit dem Argument, es sei „bekannt", dass in diesem Stadtteil besondere Gefahren drohten (EuGH ECLI:EU:C:2015:480 = NZA 2015, 1247 Rn. 117 – CHEZ Razpredelenie Bulgaria (C-83/14)). Dass auch dem Anschein nach neutrale Kritierien eine Rasse oder ethnische Gruppe besonders benachteiligen können, ist die Quintessenz einer mittelbaren Diskriminierung iSv Art. 2 II Buchst. b RL 2000/43 und Art. 21 GRCh. Auch bei der Vorratsdatenspeicherung droht eine stigmatisierende Auswahl des zu überwachenden Personenkreises und der geografischen Orte. Dies zeigt die Erfahrung mit anderen Instrumenten. So richtete sich die Rasterfahndung in den Polizeigesetzen der Länder gezielt „gegen Ausländer bestimmter Herkunft und muslimischen Glaubens" (BVerfGE 115, 320 (323, 353) = NJW 2006, 1939). Die hierdurch bewirkte stigmatisierende Wirkung erhöht den – ohnehin schon schwerwiegende Grundrechtseingriff – nur für einen bestimmten Personenkreis, der dadurch zusätzlich von Ungleichheit betroffen ist.

III. Praxisfolgen

Das seit über 15 Jahre andauernde „Trial and Error" um die Vorratsdatenspeicherung (Rückschau bei Petri ZD 2021, 493) geht va zulasten der Betroffenen digitaler Gewalt, aber auch der Betreiber öffentlicher TK-Dienste, deren Klagen der Vorlageentscheidung zugrunde lagen. Die Vorratsdatenspeicherung ist nicht das einzige Ermittlungsmittel, es ist, wie regelmäßig statistisch belegt wird, auch nicht das entscheidende Instrument zur Strafverfolgung im digitalen Raum. Im Koalitionsvertrag spricht sich das Parteienbündnis für eine rechtssichere, anlassbezogene und einer richterlichen Anord-

nung unterliegende Speicherung aus (Mehr Fortschritt wagen, S. 87). Ergänzt werden sollte dies um den evidenzbasierten Ansatz. Bevor nun einem Quick Freeze das Wort geredet wird, wäre eine kriminologische Analyse der Notwendigkeit einer weiteren Datenakkumulation angebracht. Auf die Vorratsdatenspeicherung verzichten die Ermittlungsbehörden nun schon seit Jahren, womöglich ist sie vollständig verzichtbar (vgl. die empirische Analyse des MPI im Auftrag des Bundesamtes für Justiz, Schutzlücken durch den Wegfall der Vorratsdatenspeicherung?, 2011, https://grundrechte.ch/2013/MPI_VDS_Studie.pdf).