

DATENSCHUTZ & E-GOVERNMENT

RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU) • Salzburg

EuGH: Vorratsdatenspeicherung reloaded

» jusIT 2020/84

✦ Vorratsdatenspeicherung; Telekommunikationsrecht; Datenschutzrecht; Verfassungswidrigkeit; Grundrecht auf Datenschutz; Sicherheitsbehörde; Strafverfolgungsbehörde; Auskunftersuchen; Strafe, schwerere; Verhältnismäßigkeit, keine; Zweck, konkreter, keiner; Löschung; Datenlöschung

§ RL 2000/31/EG: Art 1, 2, 14, 15; RL 2002/58/EG: Art 1, 2, 3, 6, 9 Abs 1, Art 15; VO (EU) 2016/679: Art 2 Abs 2 lit d, Art 4 Z 1, 2, Art 5 Abs 1, Art 6 Abs 1 lit c, Abs 3, Art 23, 79 Abs 1, Art 94, 95; DSGVO: § 1; TKG 2003: §§ 93, 97 Abs 2 Satz 1, § 99 Abs 2, § 102a und 102b (aF)

Im Oktober 2020 hat der EuGH in drei verbundenen sowie einem weiteren Vorlageverfahren auf zusammen über 300 Randzahlen entschieden, erstmals Ausnahmen vom bisherigen Verbot des allgemeinen und unterschiedslosen Protokollierens von digitalen Nutzerspuren zuzulassen. Es bleibt zwar bei einem Verbot pauschaler Vorratsdatenspeicherung (VDS), doch räumt das Urteil den Ermittlern neue Befugnisse ein. Das könnte die Diskussion auch in Österreich wieder befeuern.¹ Der vorliegende Beitrag erörtert die Anlassfälle und mögliche Auswirkungen für ein künftiges Modell einer abgestuften Vorratsdatenspeicherung aus datenschutz- und telekommunikationsrechtlicher Perspektive.

1. Die Ausgangsfälle

Gleich mehrere besorgte BürgerInnen und Menschenrechtsorganisationen aus drei EU-Staaten, nämlich Frankreich, Belgien und Großbritannien, hatten sich gegen die jeweiligen Sicherheitsgesetze, Verordnungen und Polizeierlässe beschwert, die als Reaktion auf die blutigen Anschläge radikaler Islamisten in Kraft gesetzt worden waren. Diesen mitgliedstaatlichen Regelungen war gemeinsam, die Anbieter von Telekommunikationsdiensten mehr oder weniger zu bestimmten Formen der Vorratsdatenspeicherung (VDS), dh der anlasslosen bzw verdachtslosen Erfassung von Verkehrsdaten zu sicherheitsbehördlichen Zwecken, zu verpflichten. Im Einzelnen hatten die den insgesamt vier Vorlageverfahren zugrunde liegenden nationalen Regelungen Folgendes bestimmt:

- eine allgemeine VDS von Verkehrsdaten durch TK-Betreiber,
- eine Technik zu implementieren, durch die TK-Anbieter in ihren Netzen Vorkommnisse erkennen sollen, die eine terroristische Gefahr darstellen (Netzfilter),

- die generelle und dauerhafte Speicherung von IP-Adressen,
- die generelle Speicherung von Bestandsdaten über einen längeren Zeitraum,
- das Sammeln von Kommunikationsdaten (Bestands- und Verkehrsdaten) samt Herausgabe dieser Daten an Nachrichtendienste.

Der EuGH hatte sich daher insb mit der Frage auseinanderzusetzen, ob einzelne EU-Staaten den Betreibern elektronischer Kommunikationsdienste allgemeine Pflichten zur Datenspeicherung auferlegen dürfen, um etwa schwere Kriminalität oder den konkreten Fall einer Bedrohung der nationalen Sicherheit bekämpfen zu können.

2. Die Entscheidung des Gerichts

Die Große Kammer² beantwortete die Vorlagefragen jeweils dahin gehend, dass eine anlasslose Speicherung und/oder Weitergabe von Verbindungsdaten zu präventiven Zwecken unzulässig wäre. Es handelte sich um einen schweren Eingriff in die Grundrechte. Die Regelungen – gleich welcher Stufe – unterfielen auch dem Unionsrecht. Der Argumentation zahlreicher Mitgliedstaaten, die auf ihre alleinige Zuständigkeit für Fragen der nationalen Sicherheit hinauslief, erteilten die RichterInnen eine klare Absage.

In der tieferen Analyse offenbart der Richterspruch aus Luxemburg allerdings etwas Ambivalenz, die den Datenschützern ein gewisses Unbehagen verursacht und Sicherheitspolitiker Morgenluft wittern lässt.

Der EuGH betont zunächst, dass Art 15 Abs 1 ePrivacy-RL³ grundsätzlich die Vorratsdatenspeicherung von Verkehrsdaten nicht ausschließt. Die Mitgliedstaaten können daher *inter alia*

¹ Vgl statt vieler Seiser, Zur (neuerlichen) Speicherung von Daten auf Vorrat – alles auf Anfang?, ZIIR 2016, 18 mwH zur bisherigen Rsp.

² EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 (La Quadrature du Net ua), ECLI:EU:C:2020:791, und EuGH 6. 10. 2020, C-623/17 (Privacy International), ECLI:EU:C:2020:790.

³ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Daten-

gesetzliche Maßnahmen erlassen, die eine elektronische Aufbewahrung von Daten für einen begrenzten Zeitraum vorsehen, den ein in Art 15 Abs 1 leg cit taxativ genannter Grund rechtfertigt.⁴ Diese Möglichkeit darf aber nicht dazu führen, eine Vorratsdatenspeicherung als Abweichung des Begrenzungsgrundsatzes bzw der Löschpflichten nach Art 5, 6 und 9 ePrivacy-RL zur Grundregel werden zu lassen. Die Speicherung von Verkehrsdaten hat demzufolge die Ausnahme zu bleiben. Sowohl das Speichern als auch das Herausgeben der gespeicherten Daten sind nach Art 15 Abs 1 iVm Art 3 ePrivacy-RL zu beurteilen.⁵ Denn in den Anlassfällen sind die Pflichten der Internet Service Provider (ISP) betroffen, nicht eine Tätigkeit des Staates. Ob die auf Vorrat gespeicherten Daten tatsächlich von Behörden genutzt würden, ist irrelevant.⁶

Trotz dieser Einschränkungen schließt die Große Kammer eine anlasslose Speicherung von elektronischen Verkehrsdaten aller Kunden eines Netzbetreibers nicht aus.⁷ Die Begründung dafür liegt in der nationalen Sicherheit, die zwar ohnehin in Art 15 Abs 1 Satz 1 ePrivacy-RL als Zweckbestimmung grundgelegt, aber nur zur Erreichung überragend wichtiger Ziele heranzuziehen ist. Hierbei geht die Erhaltung der nationalen Sicherheit iSv Art 4 Abs 2 Satz 2 EUV von ihrer Bedeutung her über die in Art 15 Abs 1 ePrivacy-RL genannten Ziele hinaus. Die so (weit) verstandene Sicherheit des Staates erlaubt daher auch stärkere Eingriffe in die Rechte der Bürger. Vorbehaltlich der Erfüllung der anderen in Art 52 Abs 1 GRC festgelegten Voraussetzungen ist das Ziel der Wahrung der nationalen Sicherheit daher geeignet, Maßnahmen zu rechtfertigen, die schwerwiegendere Eingriffe in die Grundrechte nach sich ziehen als diejenigen, die durch andere als die in Art 15 Abs 1 ePrivacy-RL genannten Ziele gerechtfertigt werden könnten.⁸

Eine solche auf Gründen der nationalen Sicherheit beruhende Vorratsdatenspeicherung ist aber nur so lange möglich, wie begründet angenommen werden kann, dass der Staat (aktuellen) terroristischen Gefahren ausgesetzt ist und bleibt. Die terroristische Gefahr muss sich konkretisiert haben, dh ernstlich bestehen, gegenwärtig und vorhersehbar sein. Eine auf terroristischer Gefahr beruhende Vorratsdatenspeicherung darf insgesamt nur zu einer Speicherung über einen überschaubaren Zeitraum führen. Sie hat durch strikte Sicherungsmaßnahmen gegen den Missbrauch der gespeicherten Daten abgesichert zu sein.⁹

3. Datenschutzrechtliche Anmerkungen

Das vorliegende Urteil bestätigt einmal mehr, dass eine anlasslose Vorratsdatenspeicherung sämtlicher Telekommunikations- und Internetverbindungsdaten der Nutzer aus Gründen der Verhältnismäßigkeit in Abwägung der Rechte aus Art 7, 8 GRC selbst zur Bekämpfung schwerer Verbrechen und Gefahren für die öffentliche Sicherheit unmöglich bleibt.¹⁰ Insoweit hat sich nichts an der bisher äußerst restriktiven VDS-Rsp des Europäischen Höchstgerichts geändert.¹¹

Dankenswerterweise stellt der EuGH klar fest, dass eine allgemein verpflichtende Regelung zur Vorratsdatenspeicherung durch Anbieter von Telekommunikationsdiensten nicht auf Art 23 Abs 1 DSGVO gestützt werden kann.¹²

Gleichermaßen kommt ein „Aushebeln“ des elektronischen Datenschutzes nicht in Betracht. Dies macht der EuGH im Privacy International-Urteil ganz besonders deutlich: Dem Umgehungsversuch, die Speicherung der Kommunikationsdaten der britischen BürgerInnen erst bei den Geheimdiensten anstatt bei den Providern vorzunehmen, sodass der Anwendungsbereich nach Art 3 Abs 1 ePrivacy-RL mangels (privater) TK-Betreiber gar nicht eröffnet wäre, erteilt die Große Kammer eine klare Absage. Der Effekt ist nämlich derselbe, „dass die Offenlegung personenbezogener Daten durch Übermittlung ebenso wie die Speicherung oder sonstige Bereitstellung von Daten eine Verarbeitung iSv Art 3 ePrivacy-RL darstellt und daher in den Anwendungsbereich dieser Richtlinie fällt“.¹³

Lediglich eine exakt zielgerichtete Regelung kann demnach eine (maßhaltende) VDS ermöglichen. Allein das herausragende Allgemeininteresse der nationalen Sicherheit iSv Art 4 Abs 2 EUV könnte eine Speicherung der Verkehrsdaten¹⁴ sämtlicher Betroffener rechtfertigen.

Eine gewissermaßen „VDS light“, also eine zielgerichtete, aber eingegrenzte Speicherung von Verkehrs- und Standortdaten zur Bekämpfung schwerer Verbrechen, um ernste Angriffe auf die öffentliche Sicherheit abzuwenden und zum Schutz der nationalen Sicherheit ist für die Große Kammer durchaus denkbar.¹⁵ Näher aufgeschlüsselt bedeutet dies:

- Eine zielgerichtete Datenspeicherung bzgl solcher Personen oder Personengruppen, die vor Veranlassung der Speicherung

schutzrichtlinie für elektronische Kommunikation – ePrivacy-RL), ABl L 2002/201, 37.

⁴ EuGH 6. 10. 2020 C-511/18, C-512/18 und C-520/186 Rz 110.

⁵ So bereits EuGH 2. 10. 2018, C-207/16 (Ministerio Fiscal) Rz 35 (37), ECLI:EU:C:2018:788, ZIIR 2019, 59 (Seiser).

⁶ Deutlich EuGH 26. 7. 2017, Gutachten 1/15 (Fluggastdatenabkommen Kanada) Rz 124 (126), ECLI:EU:C:2017:592, jusIT 2018/27, 77 (Jahnel); jüngst zu Art 8 EMRK ebenfalls EGMR 13. 2. 2020, 53205/13 (Trajkovski und Chipovski/Nordmazedonien) Rz 51.

⁷ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 137.

⁸ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 136.

⁹ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 138: Daher kann diese Aufbewahrung nicht systematischer Natur sein.

¹⁰ Deutlich EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 141.

¹¹ EuGH 21. 12. 2016, C-203/15, C-698/15 (Tele 2 Sverige) Rz 107, ECLI:EU:C:2016:970, jusIT 2017/10, 31 (Jahnel) = ÖJZ 2017/37, 281 (Lehofer); dazu Milicevic, EuGH setzt klare Vorgaben zur Vorratsdatenspeicherung, AnwBl 2017/93, 579.

¹² Deutlich Bärcker in Kühling/Buchner, DS-GVO³ (2020) Art 23 Rz 13.

¹³ Vgl EuGH 6. 10. 2020, C-623/17 (Privacy International/Secretary of State) Rz 41 (Übersetzung des Verfassers).

¹⁴ Darunter versteht etwa § 92 Abs 3 Z 4 TKG 2003 alle Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

¹⁵ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 146 zum Belgischen Ausgangsfall.

als Gefahr für die öffentliche Sicherheit identifiziert wurden, dh ohne bestimmte Personen zu diskriminieren.¹⁶

- Ebenfalls kann eine VDS-light für bestimmte geografische Orte bzw Plätze angeordnet werden. Dies soll dann möglich sein, wenn an diesem geografischen Ort eine Situation entsteht, die ein hohes Risiko für die Begehung von schweren Straftaten mit sich bringt. Typischerweise umfassen diese räumlichen Begrenzungen solche mit hoher Kriminalitätsrate oder solche, die anfällig für schwere Straftaten sind, wie besondere Infrastruktureinrichtungen oder Orte mit vielen Besuchern wie Flughäfen, Bahnhöfe und Stadien, dh bestimmte abgegrenzte Örtlichkeiten auf der Grundlage objektiver und nichtdiskriminierender Faktoren.¹⁷
- Die personen- und die ortsbezogene Vorratsdatenspeicherung muss stets zeitlich begrenzt sein. Sie darf nur so lange erfolgen, wie dies erforderlich ist. Auch die beschränkte und verhältnismäßige Dauer darf nicht auf diskriminierenden Kriterien beruhen.¹⁸

Durchaus bemerkenswert hat sich die Große Kammer auch zur Verwendung von Vorratsdaten als Beweismittel geäußert. Es ist zwar Sache der Mitgliedstaaten in ihren nationalen Prozessordnungen, die Zulässigkeit von Beweismitteln in Strafverfahren zu regeln. Nationale Strafgerichte sind aber verpflichtet, Beweismittel, die durch eine unionsrechtswidrige Vorratsdatenspeicherung erlangt worden seien, bei ihrer Entscheidung unberücksichtigt zu lassen. Dies jedenfalls dann, wenn die Betroffenen sich zu diesen Beweismitteln nicht effektiv äußern konnten.¹⁹

Der EuGH hat die Fälle an die nationalen Gerichte zurückverwiesen. Die endgültigen Entscheidungen der mitgliedstaatlichen Tribunale stehen noch aus. Im Ergebnis müssen aber die am Maßstab des Unionsrechts gemessenen Regelwerke einer Vorratsdatenspeicherung den aufgezeigten Erfordernissen entsprechen. Vor allem kommt es auf die Schutzmaßnahmen an, um ein angemessenes Gleichgewicht zwischen der Privatsphäre des Einzelnen und dem Schutz der Öffentlichkeit zu erzielen.

4. Telekommunikationsrechtliche Anmerkungen

Aus telekommunikationsrechtlicher Sicht verbleibt aus dem *La Quadrature du Net* ua-Urteil eine mögliche Verpflichtung der Provider zur gezielten Speicherung von Verbindungs- und Standortdaten zu resümieren:

Für eine *IP-Adressen-Speicherung* bleibt es beim bisherigen Grundsatz, dass die anlasslose Aufbewahrung bei sämtlichen

Nutzern zur Bekämpfung von schwerer Kriminalität und ernstlichen Gefahren für die öffentliche Sicherheit möglich ist. Dies umfasst aber jedenfalls nur die IP-Adressen des jeweiligen TK-Anschlusses und nicht die Adressen der besuchten Internetseiten.²⁰

Eine *Speicherung von Stammdaten*, die für sich keine Auskunft über einen Kommunikationsvorgang geben,²¹ ist grundsätzlich anlasslos auf Vorrat zulässig. Darin besteht keine ernstliche Beeinträchtigung der durch Art 7, 8 GRC geschützten Grundrechte. Nach dem Vorrang genießenden Sonderdatenschutz des Telekommunikationsrechts gelten folgende Löschfristen für den TK-Betreiber: für Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer nach § 97 Abs 2 Satz 1 TKG 2003. Eine Speicherung ist nur „soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen“. Damit ist grundsätzlich deren Aufbewahrung mit der Vertragsdauer des Teilnehmers verknüpft. Als „sonstige gesetzliche Verpflichtung“ sieht die DSB ausschließlich steuerliche Aufbewahrungsfristen (§ 132 BAO), nicht aber die bloße Festsetzungsverjährung des § 207 Abs 2 BAO an. Dieser Ansatz scheint durchaus kritikwürdig in Anbetracht der Judikatur des EuGH, wonach eine Speicherung für die Dauer einer Verjährungsfrist zulässig sein kann, da sich nach den Verjährungsfristen, die in den einzelnen Mitgliedstaaten gelten, auch nach mehreren Jahren Fragen ergeben können, die einen Rückgriff auf diese Daten erfordern.²² Zur Rechtfertigung der (weiteren) Speicherung dieser Daten können schon Strafverfolgungsinteressen dienen; diese sind nicht auf schwere Straftaten beschränkt.

Beim sogenannten „*Quick Freeze*“, dh einem Verfahren, mit dem Verkehrsdaten für Zwecke der Strafverfolgung vorübergehend gesichert werden können (Anlassdatenspeicherung), verbleibt es ebenfalls beim Grundsatz: Verbindungs- oder Verkehrsdaten sind nach § 99 Abs 2 Satz 2 TKG 2003 „zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beansprucht wurden“. Dabei handelt es sich um eine standardmäßige „Default-Frist“, die nur durch einen konkreten Einspruch des Teilnehmers und ein anschließendes Schlichtungs- oder Gerichtsverfahren verlängert werden kann.²³ Das bedeutet im Ergebnis, dass die ISP verpflichtet sind, Verbindungs-

¹⁶ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 149: Es muss klar gestellt werden, dass es sich bei den Personen, gegen die sich diese Maßnahme richtet, insbesondere um Personen handeln kann, die zuvor im Rahmen der geltenden nationalen Verfahren und auf der Grundlage objektiver Beweise als eine Gefahr für die öffentliche oder nationale Sicherheit in dem betreffenden Mitgliedstaat identifiziert wurden.

¹⁷ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 150.

¹⁸ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 151.

¹⁹ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 227.

²⁰ EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 156 ff.

²¹ Vgl § 93 Abs 3 Z 3 TKG 2003.

²² EuGH 9. 3. 2017, C-398/15 (Mani) Rz 54 ff, ÖJZ 2017/67, 481 (Lehofer) = ZIIR 2017, 166 (Thiele); dazu Jähnel, Kein allgemeines Recht auf Datenlöschung aus einem Gesellschaftsregister, jusIT 2017/37, 79.

²³ Vgl § 99 Abs 2 Satz 3 Z 1–4 TKG 2003; vgl auch DSB 28. 5. 2018, DSB-D216.471/0001-DSB/2018 (Löschfristen für Mobilfunkdaten), Dako 2018/53, 92 = jusIT 2018/72, 199 (Bergauer/Thiele) = ZIIR 2018, 370 (Thiele); dazu Gabauer, Zur Speicherfrist von Daten, ecolx 2018, 1038; Hötzendorfer/Kastelitz/Scheichenbauer/Tschohl, Erste Entscheidung der DSB zu Speicherfristen: Welche Rolle spielt die Interessenabwägung?, Dako 2018/66, 113; Knoll/Breuss, Die Aufbewahrung personenbezogener Daten für den Zweck der Rechtsverfolgung, jusIT 2019/11, 26.

daten unverzüglich zu löschen, die sie nicht zu Abrechnungszwecken benötigen.

Nach Ansicht des EuGH kann eine Behörde oder ein Gericht gegenüber einem TK-Anbieter durchaus anordnen, bestehende Verbindungsdaten nicht zu löschen, maW ein Löschesverbot durchsetzen.²⁴ Dieses Löschesverbot darf aber nur von relativ kurzer Dauer sein, muss sich auf bestimmte Personen beziehen und darf nur der Bekämpfung schwerer Kriminalität oder der Erhaltung der nationalen Sicherheit dienen.²⁵ Es kann aber auch (Verbindungs-)Daten von Personen umfassen, die in Bezug zu Personen stehen, die schwerer Straftaten verdächtig sind.²⁶

Kritisch sei angemerkt, dass die Große Kammer auch in hunderten Randzahlen keine Ausführungen dazu macht, wie mit den Verkehrsdaten von beruflichen Geheimnisträgern, wie zB Ärzten, Anwälten oder Geistlichen, verfahren werden darf.²⁷ Hier gilt nach wie vor ein absolutes Verbot: Die Verbindungsdaten dieser Berufsgruppen müssten von jeder Form der Vorratsdatenspeicherung ausgenommen werden.

Derzeit behängen weitere VDS-Verfahren beim EuGH. Das Deutsche Bundesverwaltungsgericht (BVwG) hat zusammengefasst die Frage vorgelegt, ob die anlasslose Speicherung von Verkehrs- und Standortdaten für eine Dauer von zehn bzw vier Wochen mit Art 15 Abs 1 ePrivacy-RL vereinbar ist.²⁸ Die Verfahren werden zur Rs C-793/19 (SpaceNet AG/Deutschland) geführt.

Darüber hinaus hat sich auf EU-Ebene unter der deutschen Ratspräsidentschaft eine neue Arbeitsgruppe gebildet, die eine harmonisierte Gesetzgebung zur Vorratsdatenspeicherung in der EU verfolgt.²⁹

5. Zusammenfassung

Zusammenfassend hat der EuGH jüngst in vier Fällen entschieden, dass eine anlass- und unterschiedslose Speicherung von Verkehrs- und Standortdaten („Kommunikationsdaten“) (weiterhin) nicht zulässig ist. In Situationen, in denen aber eine ernsthafte, konkretisierte Bedrohung der nationalen Sicherheit besteht, könnte von diesem Grundsatz abgewichen werden. Darunter ist kein Freibrief des Normgebers zur gesetzlichen Verpflichtung privater Telekommunikationsdienstleister zu verstehen, Telekommunikations- und Internetverbindungsdaten ihrer Nutzer für einen längeren Zeitraum zu speichern, damit Strafverfolgungsbehörden gegebenenfalls auf diese zugreifen können. Vielmehr entwickelt das Höchstgericht am Maßstab des Art 4 Abs 2 EUV iVm Art 15 Abs 1 ePrivacy-RL einerseits und Art 7, 8 und 52

Abs 1 EU-GRC andererseits seine bisherige Rsp³⁰ fort. Nach einem Teil der Lehre liefert der EuGH zugleich einen „Bauplan für den Gesetzgeber“,³¹ wie eine gerade noch unionsrechtskonforme Vorratsdatenspeicherung aussehen könnte. Eine VDS „reloaded“ wäre demnach zulässig, wenn

- sie der Aufrechterhaltung der nationalen Sicherheit, dem Kampf gegen schwere Kriminalität oder der Abwendung schwerer Bedrohungen der öffentlichen Sicherheit dient;
- sie auf der Basis objektiver und nicht diskriminierender Faktoren erfolgt, zB auf bestimmte Gruppen von betroffenen Personen beschränkt oder durch ein geografisches Kriterium begrenzt ist, und
- die Speicherdauer auf das absolut Notwendige begrenzt wird; was bei Fortbestehen der Gefahr aber verlängerbar sein darf.

Weitere Verfeinerungen aufgrund anhängiger Vorabentscheidungsverfahren sind zu erwarten.

30 Grundlegend EuGH 8. 4. 2014, C-293/12, C-594/12 (Digital Rights Ireland), MR-Int 2014, 17 (Otto/Seitlinger) = ÖJZ 2014/54, 337 (Lehofer); dazu Grabenwarter, Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, AnwBl 2015, 404; Schrott, EuGH erklärt Richtlinie zur Vorratsdatenspeicherung von Daten für ungültig, AnwBl 2014, 371; Wilhelm, EuGH Rs C-293/12 iVm C-594/12: Vorratsdatenspeicherung von Daten grundrechtswidrig, RL 2006/24/EG ex tunc ungültig, ecolex 2014, 397; Wolfgang Zankl, EuGH für Datenzugangssperre und gegen Datenvorratsdatenspeicherung, ecolex 2014, 576; Souhrada-Kirchmayer, Das Urteil des Europäischen Gerichtshofs zur „Vorratsdatenspeicherungs-Richtlinie“, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2014 (2014) 9; Klaushofer, Ungültigkeit der Vorratsdatenspeicherungsrichtlinie – oder: Die Geister, die man rief!, jusIT 2014/49, 96; Heißl, alea iacta est: Richtlinie über die Vorratsdatenspeicherung ist ungültig, NLMR 2014, 95; Seiser, ZIIR 2016, 18 (FN 1); Weh, Ende der Vorratsdatenspeicherung und andere Judikatur zum Grundrecht auf Datenschutz, ZVG 2014, 749; EuGH 21. 12. 2016, C-203/15, C-698/15 Rz 107.

31 Kiparski, EuGH – Bauplan einer neuen Vorratsdatenspeicherung, CR-Blog 14. 10. 2020, abrufbar unter <cr-online.de/blog/2020/10/14/eugh-bauplan-einer-neuen-vorratsdatenspeicherung/> (21. 10. 2020).

24 EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 161.

25 EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 162 ff.

26 EuGH 6. 10. 2020, C-511/18, C-512/18 und C-520/186 Rz 165.

27 Einzuräumen ist freilich, dass die Sachverhalte keinen Anlass boten, (auch) darauf einzugehen.

28 BVerwG 25. 9. 2019, 6 C 12.18 und 6 C 13.18 (Vorratsdatenspeicherung), K&R 2019, 819.

29 Council of Europe, „Ad-hoc Working Party on Data Retention“, 10772/20 vom 17. 9. 2020, abrufbar unter <statewatch.org/media/1382/eu-council-data-retention-working-party-10772-20.pdf> (22. 10. 2020).



Der Autor:

RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU) studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

Publikationen des Autors:

Standardkommentar zum RATG³ (2011); Mitherausgeber und Autor des Österreichischen und Europäischen Design- und Musterschutzrechts in zwei Bänden (2018 und 2020); Verfasser des Datenschutzstrafrechts in Pachinger (Hrsg.), Datenschutz. Recht und Praxis (2019); Mitautor des ZPO Taschenkommentars (2019); Mitherausgeber und Autor des führenden Praxiskommentars zum Österreichischen Datenschutzgesetz (2020); zahlreiche Beiträge in Fachzeitschriften zu Themen des IT-Rechts.

✉ Anwalt.Thiele@eurolawyer.at
http://www.eurolawyer.at

🌐 lesen.lexisnexis.at/autor/Thiele/Clemens

Foto: D. Wild