heitsmeldung (*data breach notification*) publik wurden. Nach Ansicht der ungarischen DSB hätte Digi diese Datenbank nach der Durchführung der notwendigen Tests und Fehlerbeseitigungen längst löschen müssen. Tatsächlich wurde die Testdatenbank noch 18 Monate lang weiterbetrieben. Vor dem Budapester Gerichtshof bekämpfte Digi die Geldbuße; schließlich legte das Gericht die Sache nach Luxemburg vor. Der EuGH hatte sich ua damit zu befassen, ob überhaupt und ggf wie lange wegen einer Serverstörung die Kund:innendaten in einer zusätzlichen Datenbank gespeichert werden dürfen.

Die Erste Kammer bejahte die Zulässigkeit des Überspielens der Datensätze in eine Testdatenbank aufgrund des technischen Defekts, maW das Sicherheits-Back-up, denn es war vom Zweckbindungsgrundsatz des Art 5 Abs 1 lit b DSGVO gedeckt. Dem Verantwortlichen war es gestattet, in einer zu Testzwecken und zur Behebung von Fehlern eingerichteten Datenbank personenbezogene Daten zu erfassen und zu speichern, die zuvor erhoben und in einer anderen Datenbank gespeichert wurden, wenn diese Weiterverarbeitung mit den konkreten Zwecken vereinbar ist, für die die personenbezogenen Daten ursprünglich erhoben worden waren, was anhand der in Art 6 Abs 4 DSGVO genannten Kriterien und sämtlicher Umstände fallkonkret zu beurteilen ist. Die konkrete Weiterverarbeitung zur Fehlerbehebung und zu Testzwecken erfüllte die Kriterien (Rz 43 und 44 des Urteils). Hingegen hielt der EuGH das Belassen der Datensätze nach Durchführung der Tests und der Fehlerbehebung für weder mit dem Grundsatz der Speicherbegrenzung noch der Datenminimierung für vereinbar. Ist nämlich der Zweck der Verarbeitung weggefallen, hat der Verantwortliche umgehend zu löschen (Rz 53 und 61 des Urteils).

Zuzustimmen ist dem vorliegenden Urteil zunächst darin, dass ein fehler- oder wartungsbedingtes Ausweichen auf eine Test- oder Sicherheitsdatenbank vom ursprünglichen Verarbeitungszweck der Datensätze umfasst ist. Die Durchführung von Tests und die Behebung von Fehlern, welche die Qualität der Abonnementkundendatenbank beeinträchtigen, weisen einen konkreten Zusammenhang mit der Erfüllung der mit den Fernseh- und Internetteilnehmenden abgeschlossenen Verträge auf. Denn solche Fehler können sich nachteilig auf die Erbringung der vertraglich abonnierten Dienstleistungen auswirken, für die die Daten ursprünglich erhoben wurden. Diese Verarbeitung weicht nicht von den legitimen Erwartungen der Abonnent:innen hinsichtlich der weiteren Verwendung ihrer Daten ab. Gleichermaßen erscheint die strikte Beschränkung der Speicherdauer zutreffend. Die Grundsätze der Zweckbindung und der Speicherbegrenzung gelten kumulativ, dh, die Speicherung personenbezogener Daten muss nicht nur dem Grundsatz der „*Zweckbindung*“, sondern auch dem Grundsatz der „*Speicherbegrenzung*“ genügen. Aus Letzterem folgt, dass selbst eine ursprünglich zulässige Verarbeitung von Daten im Laufe der Zeit mit der DSGVO unvereinbar werden kann, wenn diese Daten für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, nicht mehr erforderlich sind. Sobald also der Grund für das Ausweichen bzw der Sicherungszweck durch die erfolgreiche Wiederherstellung der ursprünglichen Datenbank weggefallen ist, müssen die Datensätze von der Testdatenbank gelöscht werden (so bereits EuGH 7. 5. 2009, C-553/07 [Rijkeboer] Rz 33, jusIT 2009/74, 151 [*Jahnel*]; EuGH 24. 9. 2019, C-136/17 [GC ua Auslistung sensibler Daten] Rz 74, Dako 2021/49, 90 [*Haidinger/Löffler*] = jusIT 2019/74, 210 [*Staudegger*] = jusIT 2019/91, 245 [*Thiele*] = ÖJZ 2019/130, 1102 [*Kumin/Maderbacher*]). Damit konkretisiert das Urteil zugleich die Anforderungen bei der Löschung von Daten und zeigt insb die Notwendigkeit des Führens eines Nachweises der erfüllten Löschpflicht auf (zur praktischen Umsetzung eines Löschkonzepts vgl *Thiele*, Datenschutz auf der Großbaustelle – Zur Teilnahme an Personaldokumentationssystemen aus Sicht der DSGVO, in Jahnel [Hrsg], Datenschutzrecht. Jahrbuch 2018 [2018] 151).

Ausblick: Das vorliegende Urteil erweitert sehr praxistauglich die Möglichkeiten der Wartung und (teilweisen) Wiederherstellung von Datenbanksystemen, die personenbezogene Daten enthalten, ebenso wie der kurzzeitigen Speicherung auf externen Servern zu Sicherungszwecken. Damit dürfte auch die Weiterverarbeitung zu Zwecken der Anonymisierung zulässig sein (instruktiv zum technischen Hintergrund *Sonntag*, Technische Grenzen der Anonymisierung, jusIT 2018/54, 137 mwH).

Zusammenfassend hat der EuGH entschieden, dass ein Internet- und Fernsehdiensteanbieter auch ohne die Einwilligung der Kund:innen bei einer Serverstörung deren Daten in einer externen Datenbank speichern darf, allerdings nur so lange, wie die Störung andauert. Ist der Zweck der Weiterverarbeitung und Speicherung weggefallen, muss unverzüglich gelöscht werden.

Bearbeiter: Clemens Thiele

EuGH: Zu Zulässigkeit und Grenzen der Vorratsdatenspeicherung

» jusIT 2022/93

§ GRC: Art 7, 8, 11, 52 Abs 1
EMRK: Art 8
RL 2002/58/EG: Art 15 Abs 1
RL 2003/6/EG: Art 12
VO (EU) 596/2014: Art 23
TKG (Deutschland): §§ 113a–113e
StPO (Deutschland): §§ 100g, 101a

EuGH 20. 9. 2022, C-793/19, C-794/19 (SpaceNet und Telekom Deutschland)
EuGH 20. 9. 2022, C-339/20, C-397/20 (VD und SR)

1. *Zu den verbundenen Rs C-793/19, C-794/19 (Deutschland):*
   a) Die verdachtsunabhängige Speicherung von IP-Adressen, Standort- und Verbindungsdaten aller Nutzerinnen und Nutzer, so wie sie im dTKG (in §§ 113a–113e idF dBGBl 2004 I, 1190) verankert wurde, widerspricht Art 15 Abs 1 ePrivacy-RL 2002/58/EG und ist insgesamt unionsrechtswidrig.

b) Demgegenüber steht Art 15 Abs 1 ePrivacy-RL iVm Art 7, 8, 11 und 52 Abs 1 GRC nationalen Rechtsvorschriften nicht entgegen, die es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersteht. Eine solche Anordnung muss dann aber durch ein Gericht oder eine unabhängige Verwaltungsstelle kontrolliert werden können und darf nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergehen (Bestätigung von EuGH C-140/20 [Commissioner of An Garda Síochána]).

2. *Zu den verbundenen Rs C-339/20, C-397/20 (Frankreich):*
   a) Art 15 Abs 1 ePrivacy-RL steht – auch unter Berücksichtigung der Unionsvorschriften RL 2003/6/EG über Insider-Geschäfte und Marktmanipulation und der Marktmissbrauchs-VO (EU) 596/2014 – nationalen Rechtsvorschriften entgegen, die zur Bekämpfung von Straftaten des Marktmissbrauchs, ua von Insidergeschäften, präventiv eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorsehen.
   b) Art 7, 8, 11 und 52 Abs 1 GRC verwehren es den nationalen Gerichten die festgestellte Unvereinbarkeit der nationalen Vorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Gericht oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, in ihren zeitlichen Wirkungen zu beschränken.
   c) Die Verwertbarkeit von Beweismitteln, die gemäß innerstaatlichen Rechtsvorschriften entgegen den unionsrechtlichen Vorratsdatenspeichergrundsätzen erlangt wurden, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung ua der Unionsgrundsätze von Äquivalenz und Effektivität – dem nationalen Recht.

Anmerkung des Bearbeiters:

Die beiden zu besprechenden Urteile zu Ausgangsfällen aus Frankreich und Deutschland behandeln die Thematik der Vorratsdatenspeicherung (VDS). Diese gehört – wie *Härting* (Entscheidungsanmerkung, CR 2022, 654) zutreffend bemerkt – „*seit 2010 zu den Untoten der Sicherheitspolitik*".

Im *deutschen Ausgangsfall* vor dem (letztlich zuständigen) Bundesverwaltungsgericht (BVerwG 25. 9. 2019, 6 C 12.18, 6 C 13.18 6, K&R 2019, 819 = NVwZ 2020, 1108) ging es darum, dass sich der Internetprovider SpaceNet – wie auch die Deutsche Telekom – weigerten, entsprechend ihren gesetzlichen Pflichten ab dem 1. Juli 2017 Verkehrs- und Standortdaten betreffend die Telekommunikation ihrer Kunden ohne konkreten Anlass, dh „*auf Vorrat*", zu speichern. Das erstinstanzliche Urteil (VG Köln 20. 4. 2018, 9 K 3859/16, openJur 2019, 21423) hatte bereits die Rechtmäßigkeit dieser Weigerung ausgesprochen. Im Revisionsverfahren legte das BVerwG dem EuGH zusammengefasst die Frage vor, ob die deutschen Regelungen zur anlasslosen VDS (§§ 113a–113e TKG aF und §§ 100g, 101a StPO aF), die eine Speicherung von Verkehrsdaten für zehn und von Standortdaten für vier Wochen vorsahen, mit dem Unionsrecht vereinbar sind.

Im *französischen Ausgangsfall* bildeten Strafverfahren, die wegen Insiderhandels, Hehlerei, Beihilfe zur Bestechung und Geldwäsche gegen zwei Privatpersonen (VD und SR) geführt wurden, den Ausgangspunkt. Im Zuge der Ermittlungen wurden im Rahmen der Bereitstellung von Diensten der elektronischen Kommunikation generierte personenbezogene Daten von den Behörden beansprucht. Die Vorlagefragen des Cour de Cassation betrafen innerstaatliche Rechtsvorschriften, nach denen die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten ab dem Zeitpunkt der Speicherung zur Bekämpfung von Straftaten des Marktmissbrauchs, ua von Insidergeschäften, präventiv ein Jahr lang allgemein und unterschiedslos auf Vorrat speichern durften. Als Folgefrage stellte sich die Verwertbarkeit von Erkenntnissen, die aus einer (unzulässigen) VDS gewonnen wurden.

In beiden Fällen (insgesamt also zu vier Vorlageverfahren) hielt die Große Kammer die jeweilige konkrete Ausgestaltung der Vorratsdatenspeicherung für *nicht* mit dem Unionsrecht vereinbar.

Im *deutschen Ausgangsfall*, den verbundenen Rs C-793/19, C-794/19 (SpaceNet und Telekom Deutschland) urteilte der Gerichtshof, dass nach Art 15 Abs 1 ePrivacy-RL iVm Art 7, 8, 11 und 52 Abs 1 GRC grundsätzlich eine Unzulässigkeit einer VDS bestünde. Diese Unzulässigkeit sei jedoch nicht absolut. So gäbe es Fälle, in denen eine Vorratsdatenspeicherung unter engen Voraussetzungen auch zulässig sein könnte. Maßgeblich sei am Ende insb die Verhältnismäßigkeit der Maßnahme (Rz 68 ff des SpaceNet-Urteils). Insoweit führte die Große Kammer aus, dass Tathandlungen im Rahmen schwerster Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit den Anwendungsbereich einer VDS eröffnen könnten. Dabei nennt der Gerichtshof einige Kriterien zur konkreten Ausgestaltung einer solchen – zulässigen – Speicherung:

- Verkehrs- und Standortdaten können allgemein und unterschiedslos auf Vorrat gespeichert werden, 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.

- IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, können allgemein und unterschiedslos auf Vorrat gespeichert werden, wenn dies zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit erforderlich und für einen auf das absolut Notwendige begrenzten Zeitraum beschränkt ist.

Derartige Überwachungsmaßnahmen müssen nach Ansicht des EuGH ihrerseits einer strengen Kontrolle unterliegen. Die Mitgliedstaaten haben insoweit durch klare und präzise Regeln sicherzustellen, 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 (Rz 75 ff des SpaceNet-Urteils).

Für den *französischen Sachverhalt* in den verbundenen Rs C-339/20, C-397/20 (VD und SR) kam der EuGH gleichermaßen zu dem Ergebnis der Unzulässigkeit einer VDS in der konkreten gesetzlichen Ausgestaltung. Insbesondere kann eine solche mit Blick auf Finanz- und Steuerkriminalität nicht aus den unionsrechtlichen Marktmissbrauchsregelungen von Art 23 Abs 2 lit g und h VO (EU) 596/2014 oder Art 12 Abs 2 lit a und d RL 2003/6/EG abgeleitet werden. Insgesamt war die anlasslose Speicherung nach den französischen Finanzmarktvorschriften unverhältnismäßig (Rz 90 ff des Urteils).

Die Große Kammer machte einmal mehr deutlich, dass die Verwertbarkeit von Beweismitteln, die aufgrund einer solchen Vorratsspeicherung von Daten erlangt wurden, nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten dem nationalen Recht unterliegt – vorbehaltlich der Beachtung ua der Grundsätze der Äquivalenz und der Effektivität. Letzterer verpflichte ein nationales Strafgericht jedoch dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung erlangt wurden, auszuschließen, sofern die betreffenden Personen nicht in der Lage seien, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über eigene Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen (Rz 105 ff des Urteils).

Der EuGH festigt mit beiden am selben Tag ergangenen Urteilen seine bisherige Entscheidungspraxis zur VDS weiter (zuletzt EuGH 5. 4. 2022, C-140/20 [Commissioner of An Garda Síochána], jusIT 2022/62, 155 [*Thiele*] = RZ 2022/9 [*Simma*]; dazu *Kreul*, Nein, aber ... Die Vorratsdatenspeicherung in Europa, MR-Int 2022, 60 mwN). Grundsätzlich beibehalten wurde auch die Zulässigkeit einer umgehenden Sicherung der Verkehrs- und Standortdaten (sog „*Quick Freeze*" – näher dazu bereits *Thiele*, EuGH: Vorratsdatenspeicherung reloaded, jusIT 2020/84, 224 [226]), auch wenn diese keinen gleichwertigen sicherheitstechnischen Ersatz bieten würde. In diesem Verfahren werden zwar auch Daten auf Vorrat erhoben, jedoch nur für einen erheblich kürzeren Zeitraum. Entsteht innerhalb dieses Zeitraums ein Verdacht auf eine Straftat, so werden nur die diese betreffenden Daten „*eingefroren*", während die restlichen Daten gelöscht werden. Die betroffenen Daten können sodann nach einer richterlichen Entscheidung entweder verwendet oder endgültig gelöscht werden.

Abschließend ist aus formaler Hinsicht anzumerken, dass sich die Urteile zur VDS zunehmend darauf beschränken, die in den vorhergehenden Entscheidungen entwickelten Grundsätze textbausteinartig (inkl Verweisen) aneinanderzureihen und damit zu wiederholen. Dies mag dem „*französischen Urteilsstil*" geschuldet sein, der am Gerichtshof gepflogen wird, macht aber die Entscheidungen immer umfangreicher, ohne dass dadurch eine verstärkte Überzeugungswirkung oder eine größere Schlüssigkeit erzielt wird.

Ausblick: Die Zulässigkeit von Beweismitteln, die durch eine – wie im Anlassfall – unzulässige VDS erlangt werden, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten dem nationalen Recht. Aus dem Datenschutzgrundrecht des § 1 DSG leitet die österreichische Rechtspraxis kein Beweismittelverwertungsverbot ab (*Thiele/Wagner*, DSG^2 § 1 Rz 196 mwN). In einer rezenten Entscheidung hat die zivile Rechtsprechung festgehalten, dass auch nach Inkrafttreten der DSGVO in Zivilverfahren kein generelles Verwertungsverbot für Beweismittel besteht, die entgegen den Datenschutzbestimmungen erlangt bzw angefertigt wurden. Die Verwertung einer rechtswidrig angefertigten Videoaufnahme in einem Zivilprozess hängt daher idR von einer Interessenabwägung im Einzelfall ab (OGH 24. 8. 2022, 7 Ob 121/22b, mwN).

Zusammenfassend hat der EuGH entschieden, dass Vorschriften der Mitgliedstaaten den Anbietern von Diensten der elektronischen Kommunikation nicht gestatten dürfen, die Verkehrsdaten ab dem Zeitpunkt der Speicherung zur Bekämpfung von Straftaten des Marktmissbrauchs, ua von Insidergeschäften, präventiv ein Jahr lang allgemein und unterschiedslos auf Vorrat zu speichern. Ein nationales Gericht kann die Feststellung, dass innerstaatliche Rechtsvorschriften, die eine solche Vorratsspeicherung der Verkehrsdaten vorsehen, ungültig sind, auch nicht in ihren zeitlichen Wirkungen beschränken. Weiters hat der EuGH neuerlich bestätigt, dass die ePrivacy-RL und die Unionsgrundrechte nach Art 7 und 8 GRC einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten entgegenstehen. Zulässig wäre eine VDS hingegen, wenn eine ernste Bedrohung für die nationale Sicherheit besteht und der Grundsatz der Verhältnismäßigkeit streng beachtet wird, maW ein exakt determinierter „*Quick Freeze*".

Bearbeiter: Clemens Thiele