

Grundsätze der Transparenz und der Verarbeitung nach Treu und Glauben gewährleistet. Weiters könnte eine Verletzung der Informationspflicht der Erteilung einer Einwilligung „in informierter Weise“ iSv Art 4 Z 11 DSGVO entgegenstehen, was diese Verarbeitung rechtswidrig iSv Art 5 Abs 1 DSGVO machen kann.

Da eine Verarbeitung personenbezogener Daten unter Verletzung des Informationsrechts, das der betroffenen Person aus Art 12 und 13 DSGVO zusteht, gegen die in Art 5 DSGVO festgelegten Anforderungen verstößt, ist die Verletzung dieses Rechts als ein Verstoß gegen die Rechte der betroffenen Person „infolge einer Verarbeitung“ iSv Art 80 Abs 2 DSGVO anzusehen. Das Informationsrecht stellt folglich ein Recht dar, bei dessen Verletzung von dem in Art 80 Abs 2 DSGVO vorgesehenen Verbandsklagemechanismus Gebrauch gemacht werden kann.

Ausblick: Dieses Urteil könnte in der Richtung verstanden werden, dass nach der erweiterten Prüfformel des EuGH nunmehr jede Missachtung der Betroffenenrechte eine Unzulässigkeit der Verarbeitung nach sich ziehen würde. Allerdings erfolgt in Rz 59 eine gewisse Einschränkung dahin gehend, dass von einer möglichen Rechtswidrigkeit der Verarbeitung nur im Zusammenhang mit der Nichterfüllung der Voraussetzungen für eine gültige Einwilligung gesprochen wird. Weiters ist zu beachten, dass es im konkreten Fall nicht um die Prüfung der Rechtmäßigkeit einer Datenverarbeitung ging, sondern um die Voraussetzungen für die Erhebung einer Verbandsklage. Insofern dürfte das Urteil eher so zu lesen sein, dass eine Verletzung des Transparenzgebotes (Art 5 Abs 1 lit a DSGVO) durch die Nichterfüllung der Informationspflicht eine Rechtswidrigkeit der Verarbeitung nach sich ziehen kann, nicht aber schon jede Verletzung eines der Betroffenenrechte der Art 12–22 DSGVO. Die weitere Entwicklung der Formel des EuGH für eine Rechtmäßigkeitsprüfung wird aber aufmerksam zu verfolgen sein.

Bearbeiter: Dietmar Jahnel

EuGH: Vorratsdatenspeicherung zur Verfolgung von Urheberrechtsverstößen (Plenum)

» jusIT 2024/107

§ GRC: Art 7, 8, 11, 52 Abs 1
RL 2002/58/EG: Art 5, 15
RL (EU) 2016/680: Art 1, 3

EuGH 30. 4. 2024, C-470/21 (La Quadrature du Net u.a. und Kampf gegen Fälschungen)

1. Die Mitgliedstaaten haben gem Art 15 Abs 1 RL 2002/58/EG (ePrivacy-RL) das Recht, unter bestimmten Bedingungen die Rechte und Pflichten im Bereich des elektronischen Datenschutzes, namentlich im Zusammenhang mit einer Vorratsdatenspeicherung, zu beschränken.

2. Nach Art 15 Abs 1 ePrivacy-RL ist der behördliche Zugang zu zeitlich begrenzt gespeicherten Identitätsdaten, die IP-Adressen zuzuordnen sind, die zuvor von Einrichtungen der Rechteinhaber gesammelt wurden, zur Verfolgung strafbarer Schutzrechtsverletzungen (hier: Urheberrechtsverstößen) unter Einhaltung enger (kumulativer) Voraussetzungen zulässig, nämlich dass

- die Speicherung getrennt nach Datenkategorien erfolgt, sodass keine Rückschlüsse auf das Privatleben möglich sind;
- der Zugang zu den Daten ausschließlich der Identifizierung von Verdächtigen dient und mit strengen Garantien versehen wird;
- die Verknüpfung der Daten zur Identifizierung nur unter gerichtlicher Kontrolle zulässig ist;
- das Datenverarbeitungssystem der Behörde regelmäßig durch unabhängige Stellen auf Missbrauch und Integrität überprüft wird.

Anmerkung des Bearbeiters:

Im aus Frankreich stammenden Ausgangsfall hatte ein gültiges Gesetz („Dekret“) zum Schutz von urheberrechtlich geschützten Werken vor Internetrechtsverletzungen zwei Verfahren zur Verarbeitung personenbezogener Daten vorgesehen. Das erste Verfahren erlaubte Rechteinhabern, IP-Adressen zu sammeln, die mutmaßlich in Peer-to-Peer-Netzen für Rechtsverletzungen genutzt wurden, und diese der Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet (kurz: „Hadopi“) zu übermitteln. Im zweiten Verfahren glichen Internetzugangsanbieter auf Ersuchen der Hadopi die IP-Adressen mit den Identitätsdaten der Inhaber ab. Diese Datenverarbeitungen ermöglichen es der Behörde, Verfahren gegen die identifizierten Personen einzuleiten, die sowohl erzieherische als auch repressive Maßnahmen umfassten und in schweren Fällen zur Weiterleitung an die Staatsanwaltschaft führen konnten, um allenfalls eine strafgerichtliche Verfolgung einzuleiten. Vier Vereinigungen zum Schutz der Rechte und Freiheiten im Internet haben den französischen Staatsrat („Conseil d'État“) auf Nichtigkeitklärung des Dekrets geklagt. Der Staatsrat ersuchte im Verfahren zur Überprüfung der abschlägigen Entscheidung des französischen Premierministers schließlich den EuGH um Klärung, ob diese Datenverarbeitungen mit dem Unionsrecht, insb mit dem Verbot der Vorratsdatenspeicherung nach Art 15 ePrivacy-RL (RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [Datenschutzrichtlinie für elektronische Kommunikation], ABl L 2002/201, 37), vereinbar sind. Die Vorlagefragen betrafen ausschließlich die zweite Verfahrensart, also die nachgelagerte Verarbeitung des Datenabgleichs (vgl Rz 58 und 64 des Urteils).

Das Plenum des EuGH entschied, dass eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen nicht zwangsläufig einen schwerwiegenden Eingriff in die Grundrechte



darstellt (Rz 79 des Urteils). Eine solche Vorratsspeicherung wäre dann zulässig, wenn nationale Regelungen sicherstellen, dass die verschiedenen Kategorien personenbezogener Daten wirksam und strikt getrennt werden, sodass keine präzisen Rückschlüsse auf das Privatleben der betroffenen Personen möglich wären (vgl Rz 82–84 des Urteils).

Das Europäische Höchstgericht ergänzte, dass das Unionsrecht einer nationalen Regelung nicht entgegensteht, die es ermöglicht, der zuständigen nationalen Behörde allein zum Zweck der Identifizierung einer Person, die einer Straftat verdächtigt wird, Zugang zu den von den Internetzugangsanbietern getrennt gespeicherten Identitätsdaten zu gewähren. Die Mitgliedstaaten müssen jedoch sicherstellen, dass der Zugang keine genauen Rückschlüsse auf das Privatleben der Inhaber der IP-Adressen zulässt (Rz 85 des Urteils). Dies bedeutet nach dem Kriterienkatalog des Gerichts (Rz 86–93 des Urteils), dass etwa Bedienstete, die Zugang haben, keine Informationen über den Inhalt der abgerufenen Dateien weitergeben, die von den IP-Adressen aus besuchten Webseiten nachverfolgen oder diese Adressen zu anderen Zwecken als der Identifizierung ihrer Inhaber verwenden dürfen. Dient der Zugang zu den Identitätsdaten ausschließlich der Identifizierung des Nutzers, so ist eine vorherige Kontrolle des Zugangs durch ein Gericht oder eine unabhängige Verwaltungsstelle nicht erforderlich, es sei denn, der Grundrechtseingriff kann als schwerwiegend angesehen werden (Rz 100 ff des Urteils). Eine solche Kontrolle muss jedoch vorgesehen sein, falls das nationale Verfahren durch die Verknüpfung der gesammelten Daten genaue Rückschlüsse auf das Privatleben der betroffenen Person zulässt, wodurch ein schwerer Grundrechtseingriff vorliegen würde (Rz 124 ff des Urteils). In diesem Fall muss die Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vor der Verknüpfung erfolgen, um die Wirksamkeit des Verfahrens zu gewährleisten, das insb dazu dienen muss, Wiederholungen des rechtswidrigen Verhaltens zu erkennen (Rz 130 ff).

Bemerkenswert an dem vorliegenden Urteil ist zunächst seine Form. Es handelt sich um eine der sehr seltenen Plenumsentscheidungen, dh, an diesem Urteil haben alle 27 Richter:innen des EuGH mitgewirkt. Abgesehen von den in Art 16 Abs 3 EuGH-Satzung vorgesehenen Fällen (zB zur Amtsenthebung des Europäischen Bürgerbeauftragten oder eines Mitglieds der Europäischen Kommission, das seine Amtspflichten verletzt hat) tagt das Plenum erst dann, wenn die zuständige Kammer zur Auffassung gelangt, dass eine Rechtssache von außergewöhnlicher Bedeutung iSv Art 16 Abs 4 leg cit zu entscheiden ist. Diese Ansicht wurde offenbar *in concreto* von dem übrigen EuGH-Kollegium geteilt.

In der Tat halten erste Kommentare in der Fachpresse das vorliegende Urteil für einen „Paradigmenwechsel“, da es festhielte, dass die Mitgliedstaaten durchaus Regelungen schaffen dürfen, die einer (Verwaltungs-)Behörde den Zugang zu gespeicherten Daten ermöglichen, um – privat zu verfolgende – Urheberrechtsverletzungen im Internet zu bekämpfen. Es bedürfe daher keiner „schweren Straftat“ mehr, um die – *nota bene* gesetzlich vorgesehene – Vorratsdatenspeicherung zu legitimie-

ren (vgl LTO, EuGH erlaubt Vorratsdatenspeicherung bei allen Straftaten, abrufbar unter <lto.de/recht/nachrichten/n/c47021-eugh-eropaeischer-gerichtshof-urteil-vorratsdatenspeicherung-daten-ueberwachung-hadopi/> [10. 7. 2024]).

Bei genauerer Analyse hat das Plenum stets den Anlassfall im Blick, sodass von einem „Freibrief“ für die Vorratsdatenspeicherung selbst bei geringsten Straf- oder Verwaltungsstraftaten keine Rede sein kann. Die französische Behörde erhielt gerade keinen (direkten) Zugang zu einem „Satz von Verkehrs- oder Standortdaten“ iSd bisherigen strengen Unions-Rsp (EuGH 6. 10. 2020, C-511/18 [La Quadrature du Net u.a.] Rz 108 und 167, jusIT 2020/86, 235; dazu Thiele, EuGH: Vorratsdatenspeicherung reloaded, jusIT 2020/84, 224 [226]). Die Behörde wurde gerade nicht in die Lage versetzt, genaue Schlüsse auf das Privatleben der betroffenen Personen ziehen zu können. Ein Zugang, der es nicht erlaubt, solche Schlüsse zu ziehen, stellt jedoch keinen schweren Eingriff in die durch die Art 7 und 8 GRCh garantierten Grundrechte dar (Rz 99 des Urteils). Damit dürfte zB die in Österreich übliche indirekte Datenweitergabe aus der Datenspeicherung von TK-Unternehmen zulässig bleiben.

Dient also der Zugang zu Identitätsdaten der Nutzer elektronischer Kommunikationsmittel allein zur Ermittlung des betreffenden Nutzers, ohne dass diese Daten mit Informationen über die erfolgte Kommunikation in Verbindung gebracht werden können, kann der mit einer solchen Verarbeitung dieser Daten verbundene Eingriff grds nicht als schwerwiegend eingestuft werden (Rz 133 des Urteils).

Das Plenum verkennt dabei nicht, dass in „atypischen Situationen“ diese Verkehrsdaten durchaus die Aspekte des Privatlebens einer Person offenbaren können, wenn diese in Peer-to-Peer-Netzen wiederholt oder in großem Umfang Aktivitäten setzt, die Urheberrechte oder verwandte Schutzrechte verletzen; dies insb im Zusammenhang mit geschützten Werken besonderer Arten, die sich anhand von Worten ihres Titels eingruppieren lassen, und dadurch Informationen, uU sensibler Art, enthüllen (Rz 111 und 112 des Urteils). Dies hat hierzulande bereits früh die Grundrechtsjudikatur erkannt: „Das Recht auf Achtung des Privatlebens iSv Art 8 MRK umfasst auch das Recht, die Gestaltung des Privatlebens dem Blick der Öffentlichkeit und des Staates zu entziehen. In einer von der Achtung der Freiheit geprägten Gesellschaft, wie sie die Präambel zur MRK voraussetzt, braucht der Bürger ohne triftigen Grund niemandem Einblick zu gewähren, welchem Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitungen er abonniert, was er isst und trinkt und wo er die Nacht verbringt“ (VfGH 14. 3. 1991, G 148/90). Diesem Gedanken trägt auch der EuGH Rechnung, indem er ausführt, dass die Intensität der Beeinträchtigung des Rechts auf Achtung des Privatlebens allmählich zunehmen kann (vgl Rz 140). Neben den ohnehin im französischen Recht vorgesehenen abgestuften Reaktionen der Behörde bedarf es daher auch bei der Weiterleitung an die Staatsanwaltschaft, dh im Verdachtsfall, einer Kontrollinstanz (Rz 143 ff des Urteils). Diese Kontrolle darf aber keineswegs „vollständig automatisiert“ ablaufen, sondern bedarf zwingend einer Überprüfung durch einen Menschen (deutlich Rz 151

des Urteils). Den Kontrollanforderungen wird die Behörde des Ausgangsfalles („Hadopi“) letztlich nicht gerecht (Rz 155 ff des Urteils). Schließlich bleibt es aber Sache des vorlegenden Gerichts, zu prüfen, ob diese nationalen Rechtsvorschriften *alle* durch die in der RL (EU) 2016/680 (des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89) vorgeschriebenen materiellen und prozeduralen Garantien vorsehen (Rz 163 des Urteils).

Ausblick: Aus dem vorliegenden Urteil wurde bereits politisches Kleingeld geschlagen. So äußerte sich die Deutsche Innenministerin, Nancy Faeser (SPD), eine Befürworterin der Vorratsdatenspeicherung, dazu wie folgt: „Der Europäische Gerichtshof hat durch das Urteil des Plenums aller 27 Richterinnen und Richter jetzt sehr deutlich entschieden, dass eine Pflicht zur Speicherung von IP-Adressen zur Verbrechensbekämpfung nicht nur ausdrücklich zulässig ist, sondern auch zwingend erforderlich“ (zitiert nach Heise-Online, abrufbar unter <heise.de/news/Faeserfordert-nach-EuGH-Urteil-Vorratsdatenspeicherung-9706221.html> [10. 7. 2024]). Ein oberflächlicher Blick auf Rz 119 des Urteils könnte diesen Befund stützen; der aufmerksame Rechtsanwender hat aber längst erkannt, dass das Plenum der bisherigen restriktiven Vorratsdaten-Rsp des Gerichtshofes treu geblieben ist (vgl Rz 122 des Urteils). Die französische Regelung ist voraussichtlich unionsrechtswidrig.

Zusammenfassend hat der EuGH die Vorgaben zur Vorratspeicherung von Daten und zum Zugang zu diesen konkretisiert. Nach der ePrivacy-RL darf eine nationale Regelung eine Vorratsdatenspeicherung zur Identifizierung von IP-Adressen erlauben, sofern (in wörtlicher Zitierung des umfangreichen Tenors [Rz 165])

- „diese Daten zu Bedingungen und unter technischen Modalitäten gespeichert werden, die gewährleisten, dass es ausgeschlossen ist, dass aus der Vorratsspeicherung genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen, zB durch Erstellung ihres detaillierten Profils, gezogen werden können, was insb dadurch erreicht werden kann, dass den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur Vorratsspeicherung der verschiedenen Kategorien personenbezogener Daten wie Identitätsdaten, IP-Adressen sowie Verkehrs- und Standortdaten auferlegt wird, die eine wirksame strikte Trennung dieser verschiedenen Datenkategorien gewährleistet, mit der im Stadium der Speicherung jede kombinierte Nutzung dieser verschiedenen Datenkategorien verhindert wird, und die Dauer der Speicherung das absolut notwendige Maß nicht überschreitet;
- der Zugang dieser Behörde zu solchen wirksam strikt getrennt auf Vorrat gespeicherten Daten ausschließlich dazu dient, die Person zu identifizieren, die im Verdacht steht, eine Straftat begangen zu haben, und dieser Zugang mit den erforderlichen Garantien versehen ist, um auszuschließen, dass er, abgesehen von

atypischen Situationen, genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen ermöglichen kann, zB durch die Erstellung ihres detaillierten Profils, was insbesondere impliziert, dass es den Bediensteten dieser Behörde, denen ein solcher Zugang gestattet worden ist, untersagt ist, Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zum alleinigen Zweck der Befassung der Staatsanwaltschaft, in welcher Form auch immer offenzulegen, die von diesen Personen besuchten Internetseiten nachzuverfolgen und allgemeiner die IP-Adressen zu anderen Zwecken als dem der Identifizierung ihrer Inhaber im Hinblick auf den Erlass etwaiger gegen sie gerichteter Maßnahmen zu nutzen;

- die Möglichkeit für die bei der betreffenden Behörde mit der Prüfung des Sachverhalts betrauten Personen, solche Daten mit Dateien zu verknüpfen, die Elemente enthalten, denen sich der Titel geschützter Werke entnehmen lässt, deren Bereitstellung im Internet die Sammlung der IP-Adressen durch Einrichtungen der Rechteinhaber gerechtfertigt hat, in Fällen der erneuten Entfaltung einer Aktivität, mit der dieselbe Person Urheberrechte oder verwandte Schutzrechte verletzt, von einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht wird, wobei die Kontrolle nicht vollständig automatisiert sein darf und vor einer solchen Verknüpfung erfolgen muss, da diese es in derartigen Fällen ermöglichen kann, genaue Schlüsse auf das Privatleben der Person zu ziehen, deren IP-Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen;
- das von der Behörde verwendete Datenverarbeitungssystem in regelmäßigen Abständen einer zur Überprüfung der Integrität des Systems, einschließlich wirksamer Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung, sowie seiner Wirksamkeit und Zuverlässigkeit bei der Aufdeckung etwaiger Verstöße dienenden Kontrolle durch eine unabhängige Stelle unterliegt, bei der es sich im Verhältnis zu dieser Behörde um einen Dritten handelt.“

Die im Anlassfall geprüfte französische Regelung, die ua die Weitergabe von elektronischen Daten zur Verfolgung von Urheberrechtsverstößen gestattet, dürfte diesen zwingenden Vorgaben des EuGH nicht entsprechen.

Bearbeiter: Clemens Thiele