Gerichtshof der Europäischen Union
PRESSEMITTEILUNG Nr. 58/22
Luxemburg, den 5. April 2022

Presse und Information

Urteil in der Rechtssache C-140/20
Commissioner of the Garda Síochána u. a.

Der Gerichtshof bestätigt, dass das Unionsrecht einer allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten, die elektronische Kommunikationen betreffen, zur Bekämpfung schwerer Straftaten entgegensteht

Ein nationales Gericht kann die Wirkungen einer Ungültigerklärung nationaler Rechtsvorschriften, die eine solche Speicherung vorsehen, nicht zeitlich begrenzen

Im März 2015 wurde G. D. wegen Mordes an einer Frau in Irland zu einer lebenslangen Freiheitsstrafe verurteilt. In der gegen seine Verurteilung beim Court of Appeal (Berufungsgericht, Irland) eingelegten Berufung warf der Betroffene dem erstinstanzlichen Gericht u. a. vor, es habe zu Unrecht Verkehrs- und Standortdaten im Zusammenhang mit Telefonanrufen als Beweismittel zugelassen. Um im Rahmen des Strafverfahrens die Zulässigkeit dieser Beweise in Abrede stellen zu können, leitete G. D. parallel beim High Court (Hoher Gerichtshof, Irland) ein Zivilverfahren mit dem Ziel ein, die Ungültigkeit bestimmter Vorschriften des irischen Gesetzes von 2011 über die Speicherung solcher Daten und den Zugang dazu mit der Begründung feststellen zu lassen, dass dieses Gesetz seine Rechte aus dem Unionsrecht verletze. Mit Entscheidung vom 6. Dezember 2018 gab der High Court dem Vorbringen von G. D. statt. Irland legte gegen diese Entscheidung ein Rechtsmittel beim Supreme Court (Oberster Gerichtshof, Irland), dem vorlegenden Gericht in der vorliegenden Rechtssache, ein.

Mit seinem Vorabentscheidungsersuchen hat der Supreme Court um Klärung bezüglich der Anforderungen des Unionsrechts im Bereich der Speicherung der genannten Daten zum Zweck der Bekämpfung schwerer Straftaten sowie bezüglich der erforderlichen Garantien im Bereich des Zugangs zu diesen Daten ersucht. Außerdem hat er Zweifel vorgebracht hinsichtlich der Tragweite und der zeitlichen Wirkung einer etwaigen Ungültigerklärung bezüglich des Gesetzes von 2011 wegen Unvereinbarkeit mit dem Unionsrecht, da dieses Gesetz zur Umsetzung der Richtlinie 2006/24/EG[1] – die der Gerichtshof später mit Urteil vom 8. April 2014, Digital Rights Ireland u. a.[2] für ungültig erklärt hat – erlassen wurde.

Mit seinem Urteil hat der Gerichtshof (Große Kammer) als Erstes seine ständige Rechtsprechung[3] bestätigt, wonach das Unionsrecht[4] **nationalen Rechtsvorschriften entgegensteht, die**

[1] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 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 Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54).
[2] Urteil vom 8. April 2014, Digital Rights Ireland u. a., C-293/12, (siehe Pressemitteilung Nr. 54/14).
[3] Urteile vom 8 April 2014, Digital Rights Ireland u. a., C-293/12, vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15 (siehe Pressemitteilung Nr. 145/16), vom 6. Oktober 2020, Privacy International, C-623/17, und La Quadrature du Net u. a., C-511/18, C-512/18, Ordre des barreaux francophones et germanophone u.a., C-520/18 (siehe Pressemitteilung Nr. 123/20) sowie vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation), C-746/18 (siehe Pressemitteilung Nr. 29/21).
[4] 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 (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Datenschutzrichtlinie für elektronische Kommunikation) im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten, die elektronische Kommunikationen betreffen, zum Zweck der Bekämpfung schwerer Straftaten vorsehen.

Die Datenschutzrichtlinie für elektronische Kommunikation beschränkt sich nämlich nicht darauf, den Zugang zu solchen Daten durch Garantien zu regeln, die Missbrauch verhindern sollen, sondern regelt insbesondere auch den **Grundsatz des Verbots der Vorratsspeicherung** von Verkehrs- und Standortdaten. Die Speicherung dieser Daten stellt somit zum einen eine Ausnahme von diesem Verbot der Vorratsspeicherung 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, dar.

Die Datenschutzrichtlinie für elektronische Kommunikation gestattet den Mitgliedstaaten zwar, diese Rechte und Pflichten u. a. zum Zweck der Bekämpfung von Straftaten zu beschränken, doch müssen solche Beschränkungen u. a. den Grundsatz der Verhältnismäßigkeit wahren. Dieser Grundsatz verlangt, dass nicht nur die Anforderungen der Geeignetheit und Erforderlichkeit, sondern auch die Anforderung bezüglich der **Verhältnismäßigkeit** dieser Maßnahmen im Hinblick auf das verfolgte Ziel erfüllt sein müssen. So hat der Gerichtshof bereits entschieden, dass das Ziel der Bekämpfung schwerer Kriminalität, so grundlegend es auch sein mag, für sich genommen die Erforderlichkeit einer Maßnahme der allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten – wie sie mit der Richtlinie 2006/24 geschaffen wurde – nicht rechtfertigen kann. Im selben Sinne können selbst die positiven Verpflichtungen der Mitgliedstaaten zur Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten keine so schwerwiegenden Eingriffe rechtfertigen, wie sie mit nationalen Rechtsvorschriften, die eine solche Speicherung vorsehen, für die Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen.

Der Gerichtshof hat außerdem darauf hingewiesen, dass die Behörden nach der Charta verschiedene Verpflichtungen haben, beispielsweise zum Erlass rechtlicher Maßnahmen betreffend den Schutz des Privat- und Familienlebens, den Schutz der Wohnung und der Kommunikation, aber auch den Schutz der körperlichen und geistigen Unversehrtheit der Menschen sowie das Verbot der Folter und unmenschlicher oder erniedrigender Behandlung. Sie müssen daher **die verschiedenen betroffenen berechtigten Interessen und Rechte miteinander in Einklang bringen**. Eine dem Gemeinwohl dienende Zielsetzung kann nämlich 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.

Aufgrund dieser Erwägungen hat der Gerichtshof u. a. das Vorbringen zurückgewiesen, wonach besonders schwere Kriminalität einer als real und aktuell oder vorhersehbar einzustufenden Bedrohung der nationalen Sicherheit gleichgestellt werden könne, die für einen begrenzten Zeitraum eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung von Verkehrs- und Standortdaten rechtfertigen kann. Eine solche Bedrohung unterscheidet sich nämlich 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.

Dagegen hat der Gerichtshof in Bestätigung seiner früheren Rechtsprechung als Zweites entschieden, dass das Unionsrecht Rechtsvorschriften nicht entgegensteht, die unter den in seinem Urteil genannten Voraussetzungen zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit

- anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums **eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen**;

- **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**;

- eine umgehende **Sicherung** (*quick freeze*) der Verkehrs- und Standortdaten vorsehen, die den Betreibern elektronischer Kommunikationsdienste zur Verfügung stehen.

Zu diesen unterschiedlichen Kategorien von Maßnahmen hat der Gerichtshof verschiedene Klarstellungen vorgenommen.

Zunächst können die zuständigen nationalen Behörden eine Maßnahme der gezielten Vorratsspeicherung auf der Grundlage eines geografischen Kriteriums wie u. a. der durchschnittlichen Kriminalitätsrate in einem geografischen Gebiet treffen, ohne dass sie zwingend über konkrete Anhaltspunkte für die Vorbereitung oder die Begehung schwerer Straftaten in den betreffenden Gebieten verfügen müssten. Zudem kann eine 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 es den zuständigen Behörden ermöglichen, zum Zweck der Bekämpfung schwerer Kriminalität Informationen über die Anwesenheit der Personen, die dort ein elektronisches Kommunikationsmittel benutzen, zu erlangen, und daraus Schlüsse über ihre Anwesenheit und ihre Tätigkeit an diesen Orten oder in diesen geografischen Gebieten zu ziehen.

Sodann hat der Gerichtshof darauf hingewiesen, dass weder die Datenschutzrichtlinie für elektronische Kommunikation noch irgendein anderer Unionsrechtsakt nationalen Rechtsvorschriften entgegensteht, 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.

Schließlich hat der Gerichtshof festgestellt, dass die Datenschutzrichtlinie für elektronische Kommunikation 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, d. h. ab dem Zeitpunkt, zu dem diese Behörden nach den einschlägigen Bestimmungen des nationalen Rechts solche Ermittlungen einleiten können, eine umgehende Sicherung anzuordnen. Eine solche Maßnahme kann 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.

Diese verschiedenen Maßnahmen können je nach der Wahl des nationalen Gesetzgebers und unter Einhaltung der Grenzen des absolut Notwendigen gleichzeitig Anwendung finden.

Der Gerichtshof hat auch das Vorbringen zurückgewiesen, wonach die zuständigen nationalen Behörden zum Zweck der Bekämpfung schwerer Kriminalität Zugang zu Verkehrs- und Standortdaten haben müssten, die gemäß seiner 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. Dieses Vorbringen macht diesen Zugang nämlich von Umständen abhängig, die mit dem Ziel der Bekämpfung schwerer Kriminalität nichts zu tun haben. Zudem könnte der Zugang nach diesem Vorbringen für ein Ziel von geringerer Bedeutung als das Ziel, das die Speicherung rechtfertigte, nämlich der Schutz der nationalen Sicherheit, gerechtfertigt sein, was gegen die Hierarchie der dem

Gemeinwohl dienenden Ziele verstoßen würde, in deren Rahmen die Verhältnismäßigkeit einer Maßnahme der Vorratsspeicherung zu beurteilen ist. Außerdem bestünde, würde man einen solchen Zugang gestatten, die Gefahr, dass das Verbot einer allgemeinen und unterschiedslosen Vorratsspeicherung zum Zweck der Bekämpfung schwerer Straftaten seine praktische Wirksamkeit verliert.

Als Drittes hat der Gerichtshof bestätigt, dass das Unionsrecht nationalen Rechtsvorschriften entgegensteht, nach denen die zentralisierte Bearbeitung von Ersuchen um Zugang zu von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, selbst wenn dieser von einer innerhalb der Polizei eingerichteten Einheit unterstützt wird, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt und deren Entscheidungen später gerichtlich überprüft werden können. Der Gerichtshof hat insoweit nämlich seine Rechtsprechung bestätigt, wonach, um in der Praxis die vollständige Einhaltung der strengen Voraussetzungen für den Zugang zu personenbezogenen Daten wie Verkehrs- und Standortdaten zu gewährleisten, der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle zu unterwerfen ist und dessen bzw. deren Entscheidung auf einen mit Gründen versehenen, von den zuständigen nationalen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag hin ergehen muss. Ein Polizeibeamter ist aber kein Gericht und bietet nicht alle Garantien der Unabhängigkeit und Unparteilichkeit, die erforderlich sind, um als unabhängige Verwaltungsstelle eingestuft zu werden.

Als Viertes und Letztes hat der Gerichtshof seine Rechtsprechung bestätigt, wonach das Unionsrecht dem entgegensteht, dass ein nationales Gericht die Wirkungen einer ihm nach nationalem Recht in Bezug auf nationale Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorschreiben, obliegenden Ungültigerklärung wegen Unvereinbarkeit dieser Rechtsvorschriften mit der Datenschutzrichtlinie für elektronische Kommunikation zeitlich begrenzt.

Der Gerichtshof weist allerdings darauf hin, dass die Zulässigkeit der durch eine solche Vorratsspeicherung erlangten Beweismittel nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität dem nationalen Recht unterliegt.

HINWEIS: Im Wege eines Vorabentscheidungsersuchens können die Gerichte der Mitgliedstaaten in einem bei ihnen anhängigen Rechtsstreit dem Gerichtshof Fragen nach der Auslegung des Unionsrechts oder nach der Gültigkeit einer Handlung der Union vorlegen. Der Gerichtshof entscheidet nicht über den nationalen Rechtsstreit. Es ist Sache des nationalen Gerichts, über die Rechtssache im Einklang mit der Entscheidung des Gerichtshofs zu entscheiden. Diese Entscheidung des Gerichtshofs bindet in gleicher Weise andere nationale Gerichte, die mit einem ähnlichen Problem befasst werden.

Der Volltext des Urteils wird am Tag der Verkündung auf der Curia-Website veröffentlicht.

Pressekontakt: Hartmut Ost ☎ (+352) 4303 3255

Filmaufnahmen von der Verkündung des Urteils sind verfügbar über „Europe by Satellite“ ☎ (+32) 2 2964106