

C-339/20 und C-397/20 - Vorratsdatenspeicherung wegen Hehlerei oder Insiderhandel unzulässig

Ein nationales Gericht kann die Feststellung, dass innerstaatliche Rechtsvorschriften, die eine solche Vorratsspeicherung der Verkehrsdaten vorsehen, ungültig sind, nicht in ihren zeitlichen Wirkungen beschränken.

Gegen VD und SR laufen in Frankreich Strafverfahren wegen Insiderhandels, Hehlerei im Zusammenhang mit Insiderhandel, [Beihilfe](#), Bestechung und Geldwäsche. Ausgangspunkt der Ermittlungen waren im Rahmen der Bereitstellung von Diensten der elektronischen Kommunikation generierte [personenbezogene Daten](#) betreffend Telefongespräche von VD und SR, die dem [Ermittlungsrichter](#) von der Finanzaufsichtsbehörde (Autorité des marchés financiers, AMF) nach entsprechenden Ermittlungen zur [Verfügung](#) gestellt worden waren.

VD und SR haben bei der Cour de cassation (Kassationsgerichtshof, Frankreich) gegen zwei Urteile der Cour d'appel de Paris (Berufungsgericht Paris) Kassationsbeschwerden eingelegt. Sie wenden sich dagegen, dass sich die AMF bei der Erhebung der [Daten](#) auf innerstaatliche Rechtsvorschriften gestützt habe, die, soweit sie eine allgemeine und unterschiedslose Vorratsspeicherung der Verbindungsdaten vorsähen, unionsrechtswidrig seien und in denen die Befugnis der Ermittler der AMF zur Anforderung gespeicherter [Daten](#) nicht begrenzt werde. Sie berufen sich insoweit auf die Rechtsprechung des Gerichtshofs¹.

Die Vorlagefragen der Cour de cassation betreffen innerstaatliche Rechtsvorschriften, nach denen die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten ab dem Zeitpunkt der Speicherung zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv ein Jahr lang allgemein und unterschiedslos auf Vorrat speichern. Es geht im Wesentlichen um das Zusammenspiel der einschlägigen Vorschriften der Datenschutzrichtlinie für elektronische Kommunikation² im Lichte der Charta der Grundrechte der Europäischen Union (im Folgenden Charta)³ und der einschlägigen Vorschriften der Marktmissbrauchsrichtlinie⁴ und der Marktmissbrauchsverordnung⁵ unionsrechtswidrig sein sollten, möchte das vorlegende Gericht wissen, ob ihre Wirkungen vorläufig. Für den Fall, dass die betreffenden innerstaatlichen Rechtsvorschriften

aufrechterhalten werden können, um Rechtsunsicherheit zu [vermeiden](#) und es zu ermöglichen, dass die auf ihrer Grundlage auf Vorrat gespeicherten [Daten](#) zur Aufdeckung und Verfolgung von Insidergeschäften [verwendet](#) werden.

Mit seinem heutigen Urteil stellt der Gerichtshof als Erstes fest, dass weder die Marktmissbrauchsrichtlinie noch die Marktmissbrauchsverordnung im Hinblick auf die Ausübung der den zuständigen Finanzaufsichtsbehörden durch sie übertragenen Befugnisse eine Rechtsgrundlage für eine allgemeine [Verpflichtung](#) zur Aufbewahrung der Datenverkehrsaufzeichnungen im [Besitz](#) der Anbieter von Diensten der elektronischen Kommunikation bilden können.

Als Zweites weist der Gerichtshof darauf hin, dass es sich bei der Datenschutzrichtlinie für elektronische Kommunikation um den Referenzrechtsakt im Bereich der Speicherung und allgemein der [Verarbeitung](#)

[personenbezogener Daten](#) in der elektronischen Kommunikation handelt. Die Datenschutzrichtlinie ist daher auch für die Datenverkehrsaufzeichnungen im [Besitz](#) der Anbieter von Diensten der elektronischen Kommunikation maßgeblich, die die zuständigen Finanzaufsichtsbehörden im Sinne der Marktmissbrauchsrichtlinie und der Marktmissbrauchsverordnung bei Letzteren anfordern können. Für die Beurteilung der Frage, ob die [Verarbeitung](#) der Aufzeichnungen im [Besitz](#) der Anbieter von Diensten der elektronischen Kommunikation zulässig ist, sind mithin die Voraussetzungen gemäß der Datenschutzrichtlinie für elektronische Kommunikation in der Auslegung durch den Gerichtshof maßgeblich.

Der Gerichtshof gelangt deshalb zu dem Schluss, dass es nach der Marktmissbrauchsrichtlinie und der

Marktmissbrauchsverordnung in Verbindung mit der Datenschutzrichtlinie für elektronische Kommunikation und im Lichte der Charta nicht zulässig ist, dass die Anbieter von Diensten der elektronischen Kommunikation die Verkehrsdaten ab dem Zeitpunkt der Speicherung zur Bekämpfung von Straftaten des Marktmissbrauchs, u.a. von Insidergeschäften, ein Jahr lang allgemein und unterschiedslos auf Vorrat speichern.

Als Drittes hält der Gerichtshof an seiner Rechtsprechung fest, wonach das Unionsrecht dem entgegensteht, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrs- und Standortdaten verpflichtet werden, wegen ihrer Unvereinbarkeit mit der Datenschutzrichtlinie für elektronische Kommunikation ungültig sind, in ihren zeitlichen Wirkungen beschränkt.

Der Gerichtshof stellt jedoch klar, 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 u. a. der Grundsätze der Äquivalenz und der Effektivität. Letzterer verpflichtet ein nationales Strafgericht 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 sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der [Tatsachen](#) maßgeblich zu beeinflussen.

EuGH-Urteil vom 20. Sept. 2022; [C-339/20 VD](#) und [C-397/20 SR](#); [EuGH PM 157/2022](#)

1 Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15 (vgl. auch PM 145/16).

2 Art. 15 Abs. 1 der 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.

3 Insbesondere Art. 7, 8, 11 und 52 Abs. 1.

4 Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) (ABl. 2003, L 96, S. 16).

5 Art. 23 Abs. 2 Buchst. g und h der [Verordnung \(EU\) Nr. 596/2014](#) des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (ABl. 2014, L 173, S. 1).

E-Learning Datenschutz

Datenschutz praktische
Lektion



[Zur Buchung \(EUR 7,00 / 1 Monat\)](#)

7 Min Datenschutz [juristi.e-Seminar](#)

Aus- und Weiterbildung