

USA: US Supreme Court gewährt bei Standortdaten Datenschutz

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius, Washington DC, und Mitherausgeber der ZD.

Der US Supreme Court hat am 22.6.2018 im Rechtsstreit *Carpenter v United States* (Az. US 16-404) entschieden, dass gesammelte Mobilfunk-Standortdaten Datenschutz nach dem Vierten Verfassungszusatz genießen. Das wichtige Urteil könnte allgemein die Art und Weise, wie US-Unternehmen mit personenbezogenen Daten umgehen, in den USA beeinflussen und den Zugriff der Strafverfolgungsbehörden auf diese Daten erschweren.

1. Vernünftige Erwartung des Schutzes der Privatsphäre

In dem mit fünf gegen vier Stimmen knapp ergangenen Urteil wies das *Oberste Gericht* das Argument der *US-Regierung* zurück, dass Einzelpersonen, wie der Antragsteller *Carpenter*, keine legitime Erwartungen in den Schutz ihrer Privatsphäre gem. dem Vierten Zusatzartikel der Verfassung haben können. Dieser Verfassungszusatz ist der Dreh- und Angelpunkt für die Privacy-Debatte in den USA. Er lautet: „Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines eidlich oder eidesstattlich erhärteten Rechtsgrunds ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen.“

Das Revisionsverfahren betraf die Aufzeichnungen, die Mobilfunkanbieter von Mobilfunkmasten über den Standort der Anrufer gewinnen und für Anrufe von und zu Mobiltelefonen nutzen. Die *US-Regierung* hatte vor dem Erwerb von *Carpenters* Standortdaten keinen detailliert zu begründenden Durchsuchungsbeschluss (warrant supported by probable cause) erhalten. Sie erlangte vielmehr diese Aufzeichnungen, wie üblich, durch eine gerichtliche Anordnung nach dem Stored Communications Act, der die *US-Regierung* dazu verpflichtete, „vernünftige Gründe“ darzulegen, die die Vermutung stützen, dass die Aufzeichnungen „relevant und für eine laufende Untersuchung wesentlich“ sind (18 U. C. § 2703 (d)). Die *Richter* entschieden aber, dass die *US-Regierung* generell einen Durchsuchungsbeschluss (search warrant) nach dem strikten Probable-Cause-Standard benötige, um Zugang zu historischen Mobiltelefon-Standortaufzeichnungen zu erhalten. Ein Zugang nach 18 U. C. § 2703 (d) sei als Rechtsgrundlage hierfür nicht ausreichend.

Das *Gericht* stellt fest, dass die Standortdaten einen strengeren Schutz als andere Kundeninformationen von Diensteanbietern verdienen. „Eine Mehrheit des *Gerichts* hat bereits erkannt, dass Einzelpersonen eine vernünftige Erwartung [des Schutzes] der Privatsphäre bei ihren

gesamten körperlichen Bewegungen haben", schrieb Chief Justice *Roberts* unter Berufung u. a. auf die Entscheidung des *Obersten Gerichtshofs* in *United States v. Jones* von 2012 (*Wittmann*, ZD-Aktuell 2012, ZDAKTUELL Jahr 30103) zum Zugang der Strafverfolgungsbehörden zu den Tracking-Daten eines Fahrzeugs mit einem GPS-Gerät. „Der Zugang der *US-Regierung* zu den Aufzeichnungen der Zellen widerspricht dieser Erwartung.“ Aber trotz dieses Fallrechts zog das Mehrheitsvotum vier getrennte abweichende Meinungen auf sich. Die Minderheitenvoten der Richter *Kennedy*, *Gorsuch*, *Thomas* und *Alito* kritisierten ihre Kollegen für ihre „krasse Abkehr von relevanten Präzedenzfällen und Prinzipien des Vierten Verfassungszusatzes.“

2. Allgemeine Auswirkungen auf die Privacy-Debatte

Experten in den USA erwarten, dass die *Supreme Court*-Entscheidung weitreichende Auswirkungen allgemein auf die Datenschutzdebatte hat. Die Entscheidung des *höchsten Gerichts* hat wahrscheinlich die unmittelbarste und offensichtlichste Auswirkung auf die *Bundespolizei*, die sich typischerweise für solche Standortdaten von Verdächtigen interessiert und das eingespielte Verfahren nach dem *Stored Communications Act* nutzt, um die Beteiligung an einer Straftat festzustellen und einen wahrscheinlichen Grund für weitere Durchsuchungen zu ermitteln. Die Schlussfolgerung der Mehrheit der *Richter*, dass Einzelpersonen das Recht haben, zu erwarten, dass ihre Standortdaten privat bleiben, könnte weitere Konsequenzen für Unternehmen nach sich ziehen, die solche Informationen für andere Zwecke sammeln. Es ist durchaus wahrscheinlich, dass das Urteil als Rechtsargument in verschiedenen laufenden Gerichts- und Regulierungsverfahren als Argument angeführt wird, dass private Unternehmen einen besseren Schutz der Privatsphäre bieten sollten als bislang. Die Gerichte werden voraussichtlich die *Carpenter*-Entscheidung zitieren, um die Unternehmen zu einem stärkeren Datenschutz anzuhalten. Auch wenn verfassungsrechtlich die Reflexwirkung des Vierten Verfassungszusatzes für Parteien außerhalb der *US-Regierung* umstritten ist, wird das Urteil wahrscheinlich dazu führen, dass die US-Gerichte in der Folge der *Carpenter*-Entscheidung den Zugang zu Drittdaten in privaten Rechtsstreitigkeiten strenger prüfen werden als bisher.

Die Entscheidung wird auch diejenigen in den *Parlamenten* stärken, die sich auf der Bundes- und Landesebene in den letzten Monaten in den USA für stärkeren Datenschutz einsetzen, soweit dies im Wahljahr 2018 möglich ist. In Kalifornien gibt es bereits eine Gesetzesinitiative zu einem der DS-GVO in vielerlei Hinsicht nachgestalteten *Consumer Privacy Protection Act*, über den im November 2018 i.R.e. „Ballot Initiative“ als Volksbegehren abgestimmt wird (vgl. *Spies*, ZD-Aktuell 2018, ZDAKTUELL Jahr 06156). Die *Carpenter*-Entscheidung dürfte die Diskussion befeuern, welche Grenzen den Unternehmen bei der Datenverarbeitung zu setzen sind. Die Gegner von neuen Gesetzesmaßnahmen argumentieren, dass die Entscheidung auf der Grundlage des Vierten Verfassungszusatzes eng ausgelegt werden müsse. Jedenfalls dürfte es in Zukunft schwierig sein, weiter vor einem US-Gericht zu argumentieren, dass freiwillig an Dritte von Personen übermittelte Daten keine vernünftigen Datenschutzerwartungen (*reasonable expectation of privacy*) auslösen.

Weiterführende Links

Vgl. auch ZD-Aktuell 2018, ZDAKTUELL Jahr 06184; *Spies*, ZD-Aktuell 2018, ZDAKTUELL Jahr 06156; *Bezirksgericht Northern California* ZD 2018, ZD Jahr 2018 Seite 76; *Metz/Spittka*, ZD 2017, ZD Jahr 2017 Seite 361; *Spies*, ZD-Aktuell 2018, ZDAKTUELL Jahr 04291 und *Revalidis*, ZD-Aktuell 2017, ZDAKTUELL Jahr 05598 sowie *Jansen*, ZD 2018, ZD Jahr 2018 Seite 149.