

von **Dr. Sebastian Kraska**

Datenschutz und Satellitenrecht: das deutsche Satellitendatensicherheitsgesetz (SatDSiG)

Seit dem 1.12.2007 ist die gewerbliche und somit nichtstaatliche Verbreitung hochwertiger Satelliten-Geodaten und die Zulassung und der Betrieb eines entsprechenden Systems erstmals gesetzlich geregelt. Auch der Datenschutz ist hiervon betroffen. Dieser Artikel soll Sie darüber informieren, was dieses Gesetz überhaupt regelt und welche Bedeutung dies in der Praxis hat.

Das Erfordernis einer rechtlichen Regelung

Die Qualität privater Satelliten entspricht mittlerweile der von militärisch und nachrichtendienstlich genutzten Satelliten des Staates und stellt damit auch ein potentielles Sicherheitsrisiko dar. Die USA haben bereits die Ausfuhr von Satellitenbauteilen an nationale gesetzliche Regelungen des Importlandes gebunden, die ihren Sicherheitsbedenken hinreichende Garantien geben. Auch der deutsche Gesetzgeber sah daher Handlungsbedarf, die Nutzung von Satelliten-Geodaten einer gesetzlichen Regelung zu unterwerfen.

Das Satellitendatensicherheitsgesetz

Mit dem „Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten“ ([kurz Satellitendatensicherheitsgesetz](#) oder [SatDSiG](#)) unternimmt der Gesetzgeber den Versuch, sicherheits- und außenpolitische Interessen des Staates einerseits und privatwirtschaftliche und wissenschaftliche Interessen andererseits in Einklang zu bringen.

Privater Betrieb eines Satelliten: Genehmigungsvorbehalt

Das SatDSiG stellt den privaten Betrieb eines hochwertigen Erdfernerkundungssystems vom Gebiet der Bundesrepublik aus gem. §§ 3,1 SatDSiG unter einen Genehmigungsvorbehalt des Staates. Vorab geprüft werden sollen hierbei vor allem die durch den Satelliten gesammelten Daten.

Was sind Satelliten-Geodaten?

§ 2 Abs. 1 Nr. 2 definiert Daten im Sinne des SatDSiG als

“

„Signale eines Sensors oder mehrerer Sensoren eines Orbital- oder Transportsystems und alle daraus abgeleiteten Produkte, unabhängig vom Grad ihrer Verarbeitung und der Art ihrer Speicherung oder Darstellung.“

Ein solcher Sensor ist nach § 2 Abs. 1 Nr. 5 SatDSiG

„ein Teil eines raumgestützten Erdfernerkundungssystems, das elektromagnetische Wellen aller Spektralbereiche oder gravimetrische Felder aufzeichnet.“

”

Sind Satelliten-Geodaten auch personenbezogene Daten im Sinne des BDSG?

Ob diese Daten auch personenbezogene Daten sind, richtet sich nach § 3 Abs. 1 Bundesdatenschutzgesetz („BDSG“). Danach sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Die Meinung des EuGH und BVerfG zu dieser Frage

Im Grundsatz können Geodaten v.a. Aussagekraft über eine Person bezüglich ihres Aufenthaltes, ihrer Nutzungsbeziehung zur abgebildeten Umwelt oder zum Eigentum haben. Sind Angaben jedoch zu großflächig und somit zu allgemein, könne kein Personenbezug mehr angenommen werden. Die Übermittlung von Art und Umfang der wirtschaftlichen Flächennutzung eines Zielgebiets hat der Europäischen Gerichtshof (EuGH, Urt. v. 14.2.2000, Rs. C-369/98) jedoch als personenbezogene Daten angesehen.

Nach der Rechtsprechung des Bundesverfassungsgerichts ([BVerfG, Beschluss vom 2.5.2006](#), 1 BvR 507/01) könne zudem die Abbildung von Grundstücken aus der Luft einen Eingriff in das allgemeine Persönlichkeitsrecht darstellen, wenn Bereiche des privaten Lebensbereichs gezeigt werden, die von öffentlichen Plätzen nicht einsehbar sind. Entscheidend ist insgesamt ob auf die Identität der betroffenen Personen geschlossen werden kann.

Übermittlung von personenbezogenen Daten

§ 27 SatDSiG ist nach der Systematik des Gesetzes Spezialnorm zu § 15 BDSG, der die Übermittlung von personenbezogenen Daten an öffentliche Stellen regelt. Von dieser Besonderheit abgesehen gilt das dem BDSG zugrunde liegende Verbot mit Erlaubnisvorbehalt einer jeden Verarbeitung von personenbezogenen Daten natürlich auch hier.

Gemäß § 27 SatDSiG wird die jeweils zuständige Behörde ermächtigt, zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland oder zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker oder einer erheblichen Störung der auswärtigen Beziehungen oder zur Verhütung oder Verfolgung von Straftaten personenbezogene Daten, die ihr bei der Erfüllung ihrer Aufgaben bekannt geworden sind, an eine andere Behörde zu übermitteln. Auch eine Übermittlung an den Bundesnachrichtendienst ist möglich, soweit der Zweckbindungsgrundsatz gewahrt wird.

§ 27 Abs. 2 SatDSiG enthält eine weitere Ermächtigungsgrundlage zur Datenübermittlung im Falle von Strafverfahren wegen eines Verstoßes gegen das SatDSiG. Gerichte und Staatsanwaltschaften dürfen hiernach aus denselben bereits zu Absatz 1 erwähnten Gründen an oberste Bundesbehörden personenbezogene Daten übermitteln. Eine Übermittlung ist nur zulässig, wenn das Interesse an der Verwendung der übermittelten personenbezogenen Daten das Interesse des Betroffenen an der Geheimhaltung erheblich überwiegt und der Untersuchungszweck des Strafverfahrens nicht gefährdet werden kann.

Das Verfahren zur Verbreitung von Daten

Soweit Daten verarbeitet werden, sieht das SatDSiG ein zweistufiges Prüfungsverfahren vor, bevor Daten von hochwertigen Erdfernerkundungssystemen erstmals verbreitet werden dürfen.

§ 17 SatDSiG legt dem Datenanbieter zunächst eine Vorabprüfung auf. Dieser hat die Anfrage auf ihre Sensitivität hin zu prüfen. Nach Absatz 2 ist eine Gesamtschau der aus den Daten zu entnehmenden Informationen sowie der antragenden Person vorzunehmen. Insbesondere die Person des Antragenden soll in geeigneter Weise durch den Datenanbieter überprüft werden. Den Datenanbieter ist nach § 18 SatDSiG umfassend zu Dokumentation von Anfragen verpflichtet.

Ziel ist es, die Möglichkeit eines Schadenseintritts für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik einschätzen zu können. § 17 Abs. 3 SatDSiG zusammen mit § 2 der vom Bundesministerium für Wirtschaft und Technologie erlassenen [Satellitendatensicherheitsverordnung](#) bestimmen, unter welchen Voraussetzungen die Möglichkeit eines Schadenseintritts vorliegt. Zu berücksichtigen sind regelmäßig zu aktualisierende Sicherheitsanforderungen und internationale Verpflichtungen der Bundesrepublik, insbesondere im Zusammenhang mit der NATO.

Schließlich stellt die Verordnung in § 2 Abs. 1 fest, dass Anfragen der Bundesrepublik, die in Fällen höchster Sicherheitsrisiken nach § 21 SatDSiG auch vorrangig zu bedienen wären, nicht als sensitive

Anfragen anzusehen sind. Anfragen von deutschen militärischen oder nachrichtendienstlichen Behörden sind grundsätzlich als nicht sensitiv anzusehen.

Zweite Stufe des Verfahrens: Erlaubnisvorbehalt nach § 19 SatDSiG

Die zweite Stufe des Verfahrens zur Verbreitung von Daten findet sich in einem Erlaubnisvorbehalt nach § 19 SatDSiG. Ein Datenanbieter muss jede Verbreitung von Daten hochwertiger Erdfernerkundungssysteme behördlich bestätigen lassen. Die zuständige Behörde muss innerhalb eines Monats entscheiden, ob die bereits erwähnte Möglichkeit eines Schadenseintritts nun auch im konkreten Einzelfall vorliegt.

Fazit zur Anreicherung der Diskussion, durch nationale Gesetzgebung globale Sachverhalte regeln zu wollen:

Der deutsche Gesetzgeber hat den rechtlichen Rahmen für die kommerzielle Verbreitung hochauflösender Satellitendaten geschaffen. Dies schließt datenschutzrechtliche Ermächtigungsgrundlagen im Bereich Sicherheit und Strafprävention und -verfolgung ein. Der Staat behält damit weitreichend die Kontrolle über hochauflösende Satellitendaten. Dazu gehört insbesondere das staatliche Interesse an Informationen über Personen, die Zugang zu sensitiven Daten oder eine entsprechende Anfrage getätigt haben.

Autor:

Dr. Sebastian Kraska

Rechtsanwalt