Spies: USA: US-Supreme Court befasst sich mit Abhörmaßnahmen für Gespräche und E-Mails aus dem Ausland (FISA) ZD-Aktuell 2012, 02957

USA: US-Supreme Court befasst sich mit Abhörmaßnahmen für Gespräche und E-Mails aus dem Ausland (FISA)

Dr. Axel Spies ist Rechtsanwalt bei Bingham McCutchen in Washington DC und Mitherausgeber der Zeitschrift ZD.

Der Zugang zu EU-Daten durch US-Behörden für Zwecke der Terroristenjagd oder zur Abwehr von Spionage ist seit geraumer Zeit Zielscheibe der Kritik aus Europa. Der US Patriot Act ist bei manchen in Brüssel oder Berlin geradezu ein Schreckgespenst. Eine Befürchtung der Europäer ist, dass z.B. in der Cloud gespeicherte Daten aus der EU ohne weitere Kontrolle in die USA abwandern und dort von Regierungsstellen gespeichert oder sonst wie genutzt werden. Der US-Supreme Court hat am 21.5.2012 einen Fall zur Entscheidung angenommen, in dem es um die Klagebefugnis bei der Prüfung der Rechtmäßigkeit (insb. der Verfassungsmäßigkeit) des Abhörens ohne vorherigen Richterbeschluss (warrant) nach dem Foreign Intelligence Surveillance Act (FISA) in der Fassung von 2008 (FAA) geht.

Viel Spielraum vor dem FISA-Court

Das Rubrum des Falls lautet: James R. Clapper Jr. v. Amnesty International USA Inc. (Az. 11-1025). Es geht im Kern darum, wer klagebefugt ist, um eine richterliche Überprüfung zu verlangen und ob die aus der Schlussphase der Regierung von Präsident *G.W. Bush* stammenden Ermächtigungen zum elektronischen Abhören von Kommunikation verfassungsgemäß sind. Nach dem FISA Amendments Act von 2008 (FAA) ist es möglich, aus dem Ausland kommende E-Mails und Telefongespräche ohne vorherige richterliche Einzelermächtigung (individual warrant) zu überwachen, sofern nur hinreichende Anhaltspunkte (probable cause) bestehen, dass das Individuum mit Terrorismus oder mit Agententätigkeit in Verbindung steht. Ein Memorandum des *Congressional Research Service* von 2006 führt zu diesem Standard aus: „FISA authorizes issuance of a surveillance or search order predicated upon the probability of a possibility; the probability to believe that the foreign target of the order may engage in spying, or the probability to believe that the American target of the order may engage in criminal spying activities."

Sec. 702 FISA (50 U.S. C. 1881a) bestimmt, dass der *US-Attorney General* und der *Director of National Intelligence* Überwachungsmaßnahmen von bis zu einem Jahr gegen Personen anordnen können, bei denen „vernünftigerweise anzunehmen" ist, dass sie sich im Ausland befinden." Die Ausnahmen von dieser Vorschrift im Gesetz sind recht vage und geben den Behörden einigen Anordnungsspielraum. Die *Regierung* darf z.B. nicht „absichtlich" US-Bürger, von denen vernünftigerweise anzunehmen ist, dass sie sich im Ausland aufhalten, zum Ziel solcher Ermittlungen machen (Sec. 702 (b) (3)). Zufallsfunde sind durchaus verwertbar. Für die Überwachung genügt eine allgemeine Ermächtigung (Certification) des sog. *FISA Court* – eines nicht öffentlich tagenden und entscheidenden Sondergerichts (ebd, Sec.1881a(a), (c)(2)). Allgemeine Versicherungen und Erklärungen (affidavits) sind als Beweis vor dem *FISA-Court* in der Regel ausreichend: Eines detaillierten Nachweises, dass es sich bei den Personen im Ausland wirklich um Terrorverdächtige oder ausländische Agenten handelt, bedarf es nicht. Es gibt keinen individuellen Beschluss des *FISA Court* zum Abhören. Es ist auch nicht nötig, dass die *Regierung* die betroffenen Telefonleitungen, E-Mailadressen oder Anlagen dem *FISA Court* gegenüber angibt. Die Vorschriften, wer zu diesen Daten Zugang hat, sind ebenfalls recht vage (§§ 1801(h)(1), 1821(4)(A)). Die Umsetzung der Ermächtigung des *FISA Court* wird von dem

Gericht nicht überwacht. Es gibt auch zahlreiche Vorwürfe, dass die Ermittler dem *FISA Court* zahlreiche Maßnahmen erst gar nicht zur Zertifizierung vorlegen.

Klagebefugnis schwierig nachzuweisen

Die Kritiker dieser Regeln behaupten seit langem, dass diese Ermittlungsmaßnahmen auch US-Bürger im In- und Ausland betreffen und nicht mit dem Fourth Amendment der US-Verfassung (Schutz vor Durchsuchungen) im Einklang stehen. *Amnesty International, Human Rights Watch* und eine Reihe von Anwälten, die Inhaftierte in Guantanamo Bay vertreten, hatten gegen die Vorschrift mehrfach geklagt. Ihr Standpunkt ist, dass sie jederzeit damit rechnen müssen, dass ihre schriftliche oder fernmündliche Kommunikation, die Inhaftierte in Guantanamo Bay betrifft, durch solche „Schleppnetzüberwachungen" beeinträchtigt wird. Der *FISA Court* komme seiner Rolle als Türhüter nicht nach, um einen hinreichenden Schutz nach dem Fourth Amendment zu gewährleisten. Bislang hatten sie vor Gericht wenig Erfolg, weil die US-Gerichte schon die Klagebefugnis der Parteien abgelehnt haben. Sie konnten keine konkreten Überwachungsmaßnahmen nach FISA gegen sie nachweisen.

Das hatte sich vor einigen Wochen geändert: Das *Bundesberufungsgericht (Federal Court of Appeals for the Second Circuit*) hatte in einem Musterverfahren einstimmig entschieden, dass die Kläger klagebefugt waren. Ein Antrag der *Regierung* auf Überprüfung der Entscheidung durch das Richterplenum des Gerichts (rehearing en banc) wurde im September 2011 vom *Gericht* abgelehnt. Die Kläger mussten nicht nachweisen, dass sie individuell das Ziel von Überwachungsmaßnahmen waren – der wesentliche Stolperstein bei den vorhergehenden Verfahren war mithin aus dem Weg geräumt. Die Kläger hatten nur behauptet, dass sie die „tatsächliche und gut begründete Befürchtungen" hegen, dass sie Zielscheibe einer solchen Überwachung sind. Diese Befürchtung erachtete das *Berufungsgericht* als ausreichend an. Es reiche aus, so die *Richter*, wenn die Kläger folgende zwei Tatbestände darlegten: (1) a sufficiently threatened "future injury" with an "objectively reasonable likelihood", dass Überwachungsmaßnahmen gegen sie vorgenommen werden und (2) a "present injury" – z. B. ein Vermögensschaden auf Grund der Auswahl von Maßnahmen, um sich dieser Überwachung nicht aussetzen zu müssen. Die Obama-Administration hat daraufhin diese Entscheidung angefochten, dem *US-Supreme Court* vorgelegt und die Klagebefugnis verneint. Eine bloße Furcht vor Anhörmaßnahmen reiche für eine Klage nicht aus – es sei „proof of injury" oder „imminent injury" erforderlich – so eines der Hauptargumente. Der *US-Supreme Court* nahm den Rechtsstreit kürzlich zur Entscheidung an.

Gag Orders und National Security Letters

Vor dem *US-Supreme Court* geht es im Wesentlichen um die Klagebefugnis gegen Maßnahmen nach Sec. 702 FISA (50 U. S. C. 1881a), wie oben beschrieben. Die Ermittlungsbehörden haben allerdings noch weitere rechtliche Pfeile im Köcher: Gem. Sec. 215 FISA kann das *FBI* auch die Vorlage von Unterlagen (Bücher, Aufzeichnung, Dokumente) für eine Untersuchung gegen internationalen Terrorismus oder heimliche Agententätigkeiten (clandestine intelligence activities) anordnen. Hierfür bedarf es jedoch einer richterlichen Ermächtigung. Möglich und durchaus üblich sind sog. „Gag Orders", wonach die Unternehmen, von denen Dokumente gem. Sec. 215 angefordert werden, zum Schweigen verpflichtet sind. Werden mithin E-Mails oder Telefondaten von Kunden eines Dienstleisters (ISP, TK-Anbieter) nach Sec. 215 FISA angefordert, wissen die Betroffenen in den meisten Fällen von dieser Maßnahme nichts. Allerdings könnte der Dienstleister, der so eine FISA Order erhält, diese vor dem *FISA Court* anfechten.

Eine weitere Möglichkeit für die US-Ermittlungsbehörden ist die Zusendung eines National Security Letters (NSL) an den Dienstleister, mit denen sie ohne Ermächtigung durch ein Gericht bestimmte Daten (wie Name, Adresse und Dauer des Gesprächs) in Erfahrung bringen dürfen (nicht aber den Inhalt der Information). Wo diese Daten belegen sind (Inland oder Ausland) macht bei der Anwendung dieser Vorschriften keinen

Unterschied, was besonders für die Anbieter von Cloud Computing wichtig ist. Das *FBI* bevorzugt NSLs, weil dann keine richterliche Ermächtigung erforderlich ist. Nach einem Bericht des *Kongresses* sollen rd. 25.000 NSLs im Jahre 2010 versandt worden sein. Da über die NSLs keine Inhalte der Kommunikation abgefragt werden dürfen, sind Abhörmaßnahmen gem. Sec. 702 FISA weiterhin für die US-Ermittlungsbehörden interessant. Eine weitere Option ist, dass die *US-Regierung* über die Regeln der zwischenstaatlichen Rechtshilfevereinbarungen für das Strafrecht (MLATs) sich die nötigen Informationen von den Ermittlungsbehörden aus dem Ausland beschafft. In diesem Fall stellt sich die weiterhin offene Frage, inwieweit der US-Datenschutz die Übermittlung von personenbezogenen Daten in die USA erlaubt. In der Praxis zwischen der EU und den USA kommen Beschränkungen auf Grund des Datenschutzes bei der Datenübermittlung nach dem US-EU MLAT, wie berichtet wird, nur selten zum Zuge. Das *US-Justizministerium* hat mehrfach die Auffassung vertreten, dass die aus der EU kommenden Daten hinreichend geschützt sind.

Der *US-Supreme Court* wird vermutlich erst in einigen Wochen über den Fall öffentlich verhandeln (oral argument). Es ist durchaus möglich, dass das höchste *US-Gericht* nur über die Klagebefugnis entscheidet und die Sache i. Ü. zur weiteren Klärung an das Untergericht zurückverweist. Die Diskussion über FISA dürfte allerdings so oder so in den USA weitergehen, insbesondere, was die Vorlage von Informationen nach FISA durch Anbieter von Cloud Computing betrifft.

Weiterführende Links

Vgl. auch ZD-Aktuell 2012, 02943.