Dokumentation

US-Datenrecht

Zugriff US-amerikanischer Behörden auf Daten

US-Datenrecht
Zugriff US-amerikanischer Behörden auf Daten

Aktenzeichen:	WD 3 - 3000 - 181/20
Abschluss der Arbeit:	3. August 2020
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Fragestellung

Diese Dokumentation befasst sich mit etwaigen nach US-Recht bestehenden Rechtsgrundlagen zur Erhebung von solchen Daten, welche von amerikanischen Firmen und deren europäischen Tochterfirmen verarbeitet, übermittelt und verwaltet werden. Die Dokumentation fasst neben den relevanten Rechtsquellen einschlägige deutschsprachige Fachbeiträge zusammen.

2. Überblick zu den Rechtsgrundlagen

In diesem Themenbereich sind folgende vier US-Gesetze von besonderer Relevanz: Der Foreign Intelligence Surveillance Act of **1978** (**FISA**)[1], der **USA Patriot Act of 2001**[2], **der USA Freedom Act of 2015**[3], sowie der Clarifying Lawful Overseas Use of Data Act von **2018** (**CLOUD Act**)[4]. FISA, Patriot Act und Freedom Act sind miteinander verknüpft. Die eigentliche Grundlage für nachrichtendienstliche Datenerhebungen durch US-Behörden im Ausland bildet FISA. Auf FISA beziehen sich Patriot Act und Freedom Act als in ihrer Geltung befristete Änderungsgesetze. Der Inhalt des Patriot Act gilt in weiten Teilen modifiziert durch den Freedom Act fort – dieser ist insoweit an die Stelle des Patriot Act getreten.

Durch die weitreichenden Änderungen an FISA durch den Patriot Act wurden die zuvor ohnehin nach FISA bestehenden **Eingriffsmöglichkeiten** stark **ausgeweitet**. Manches wurde durch den Freedom Act später wieder eingeschränkt. Zentral sind Section 215 Patriot Act bzw. Section 101 Freedom Act. Auf die dadurch geänderten Sections 501 und 502 FISA[5] stützte sich die U.S. National Security Agency (**NSA**) etwa bei ihren Anordnungen an Telefongesellschaften, Telekommunikationsdaten herauszugeben. Die maßgebliche Section 101 Freedom Act ist zwar am 15. März 2020 durch Fristablauf außer Kraft getreten, womit zurzeit Sections 501 und 502 FISA nur im vor dem Patriot Act geltenden, reduzierten Ausmaß als Rechtsgrundlage zur Verfügung stehen.[6] Nach

---

1 Publ. L. No. 95-511, 92 Stat. 1783 (abrufbar unter: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf#page=1, Stand: 31.7.2020); die aktuelle Version von FISA gilt als 50 U.S. Code Chapter 36 – "Foreign Intelligence Surveillance" (abrufbar unter: https://www.govinfo.gov/content/pkg/USCODE-1998-title50/pdf/USCODE-1998-title50-chap36.pdf, Stand: 31.7.2020).

2 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001 vom 26. Oktober 2001, H.R. 3162, Publ. L. No. 107–56, 115 Stat. 272 (abrufbar unter: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, Stand: 31.7.2020).

3 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 vom 2. Juni 2015, H.R. 2048, Publ. L. No. 114–23, 129 Stat. 268 (abrufbar unter: https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf, Stand: 31.7.2020).

4 Pub. L. No. 115-141, Stat. 2383 (abrufbar unter: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text, Stand: 31.7.2020).

5 Zugleich 50 U.S. Code §§ 1861, 1862 – Access to certain business records for foreign intelligence and international terrorism investigations.

6 Fandos, Savage, Senate, Bidding for Time, Tries to Temporarily Revive Spy Tools, New York Times vom 16. März 2020 (abrufbar unter: https://www.nytimes.com/2020/03/16/us/politics/surveillance-laws-fisa-senate.html, Stand: 31.7.2020).

einem aktuellen Gesetzesentwurf wird aber eine Verlängerung der Bestimmung bis zum 1. Dezember 2023 angestrebt.[7]

Darüber hinaus bestehen weitere Ermächtigungsgrundlagen in FISA, die nicht auf den Patriot Act zurückgehen. Hingewiesen sei an dieser Stelle bereits auf **Section 702 FISA**[8], welcher die Überwachung von Nicht-US-Bürgern außerhalb des US-Territoriums etwa durch die NSA regelt.[9]

Der **CLOUD Act** ist von den ersten drei genannten Gesetzen zu trennen. Er betrifft anders gelagerte Sachverhalte: Im Gegensatz zu nachrichtendienstlicher Überwachung wird die Erhebung von elektronischen Beweismitteln für Strafverfahren geregelt. Auch der CLOUD Act ist ein Änderungsgesetz und bezieht sich auf Section 2703[10] des Electronic Communications Privacy Act of 1986 (**ECPA**)[11]. Darauf gestützt werden können **strafverfahrensrechtliche Durchsuchungs- und Beschlagnahmebeschlüsse** einer US-Behörde zur Herausgabe von Daten als Beweismittel, auch wenn diese **außerhalb des US-Territoriums gespeichert** sind.

3. USA Patriot Act, USA Freedom Act und FISA

Mit diesen Rechtsgrundlagen haben sich mehrere Rechtswissenschaftler auseinandergesetzt.

Voigt gibt einen systematischen und umfassenden **Überblick** über die **Zugriffsrechte von US-Behörden** nach Patriot Act und FISA und deren extraterritoriale Anwendbarkeit zum **Stand 2014**. Er geht dabei auf Section 702 FISA, Section 501, 502 FISA[12], Section 2703 ECPA und auf die sog. National Security Letters ein.

Hervorgehoben wird zunächst **Section 702 FISA**.[13] Sie diene der Überwachung von Nicht-US-Bürgern, die sich außerhalb des US-Territoriums aufhalten. Danach dürfte **alle elektronische Kommunikation von und zu der Zielperson sowie über die Zielperson** abgefangen werden. Auch

---

7 USA FREEDOM Reauthorization Act of 2020, H.R.6172 (abrufbar unter: https://www.congress.gov/bill/116th-congress/house-bill/6172/all-info?r=3&s=5, Stand: 31.7.2020).

8 Zugleich 50 U.S. Code §§ 1881, 1881a; eingeführt durch FISA Amendments Act of 2008 vom 10. Juli 2008, H.R. 6304, Publ. L. No. 110–261, 122 Stat. 2437 (abrufbar unter: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf, Stand: 31.7.2020), zuletzt verlängert bis 31. Dezember 2023 durch FISA Amendments Reauthorization Act of 2017 vom 18. Januar 2018, Publ. L. No. 115–118, 132 Stat. 3 (abrufbar unter: https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.pdf, Stand: 31.7.2020).

9 Wissenschaftliche Dienste des Deutschen Bundestages, USA Freedom Act 2015, Überblick über die Änderungen der nachrichtendienstlichen Befugnisse, 17. Juni 2015 (WD3 - 3000 - 144/15), S. 4.

10 Zugleich 18 U.S. Code § 2703 – Required disclosure of customer communications or records.

11 Electronic Communications Privacy Act of 1986 vom 21. Oktober 1986, H.R. 4952, Pub. L. No. 99–508, 100 Stat. 1848 (abrufbar unter: https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf, Stand: 31.7.2020).

12 Bei *Voigt* als „Section 215 FISA" bezeichnet, wobei es sich nach hiesiger Ansicht um Section 502, 503 FISA handelt, welche auf Grundlage von Section 215 Patriot Act geändert wurden; zugleich 50 U.S. Code § 1861.

13 Zugleich 50 U.S. Code §§ 1881, 1881a.

die Kommunikation zwischen unbeteiligten Dritten, die sich auf die Zielperson bezieht bzw. deren Namen nennt, könne erhoben werden. Voraussetzung sei die Relevanz für Ermittlungen zur **Terrorismusabwehr**. Da keine materielle Einschränkung der Art der Daten erfolgt, sind auch Finanzdaten grundsätzlich erfasst.

Zudem erläutert *Voigt* kurz Section 215 Patriot Act bzw. Section 501, 502 FISA[14]. Auf dessen Grundlage könne die **Herausgabe jeglicher Unterlagen, inklusive Daten auf Servern,** verlangt werden. Materielle Voraussetzung von Section 215 Patriot Act bzw. Section 501, 502 FISA[15] sei, dass die herausverlangten Unterlagen relevant für eine Terrorismus- oder Spionageermittlung sein könnten. Formell sei ein Beschluss des speziell hierfür zuständigen Foreign Intelligence Surveillance Court (**FISC** bzw. **FISA-Court**) erforderlich. Wiederum wird nach hiesiger Ansicht davon ausgegangen, dass Finanzdaten grundsätzlich erfasst sein können.

Schließlich weist der Autor auf die sog. **National Security Letters** hin, welche auch auf den Patriot Act gestützt würden.[16] Sie machten die Herausgabe von genau bestimmten Metadaten – nicht aber vom Inhalt der Kommunikation – auch ohne richterlichen Beschluss möglich. Finanzdaten sind damit nicht erfasst.

Hierauf folgt eine Herausarbeitung der persönlichen und räumlichen Anwendbarkeit der US-Gesetze. Der Sache nach geht *Voigt* von einer potentiell **weltweiten Reichweite der Zugriffsrechte** von US-Behörden aus. Als Grundsatz könne eine auch nur lose Verbindung eines Adressaten zu den USA ausreichen, um den US-Regelungen zu unterfallen. Nicht nur **US-Unternehmen** fielen hierunter, sondern auch deren **Tochtergesellschaften im Ausland.** Umgekehrt könnten sogar US-amerikanische Tochter- oder Schwestergesellschaften von ausländischen Unternehmen verpflichtet werden, ihre Einflussrechte im Konzernverbund zur Erreichung einer Datenherausgabe auszuüben. Es könne als Anknüpfungspunkt sogar ausreichen, dass ein europäisches Unternehmen ein Büro in den USA unterhalte.

> *Paul Voigt, Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, MMR 2014, 158.*

Anlage 1

Knapper stellt *Spies* den Inhalt des **Patriot Act** dar. Auch er geht von einer potentiell **weltweiten Anwendbarkeit** der einschlägigen Eingriffsrechte aufgrund von persönlicher Anwendbarkeit („personal jurisdiction“) aus. Es sei dann unerheblich, wo die Daten gespeichert seien. Die Entwicklungen bis zum Jahr 2012 sind erfasst.

> *Axel Spies, Europa: Wer hat Angst vor dem US-Patriot Act?, in: ZD-Aktuell 2012, 03062.*

Anlage 2

---

14 Zugleich 50 U.S. Code § 1861.

15 Zugleich 50 U.S. Code § 1861.

16 Vgl. 18 U.S. Code § 2709.

Zum Verständnis vor allem der durch den **USA Freedom Act herbeigeführten Änderungen** im Vergleich zum ursprünglichen Patriot Act und damit zur aktuellen Rechtslage kann auf die folgende Ausarbeitung der Wissenschaftlichen Dienste vom 17. Juni 2015 verwiesen werden.

Geändert hätten sich unter Section 101 Freedom Act unter anderem die Voraussetzungen der massenhaften Abfrage von und der Bildung von Datenbanken mit Metadaten zu Telefongesprächen. Eine Abschaffung der Möglichkeit, nach Section 501, 502 FISA[17] auch Inhaltsdaten (wie etwa Finanzdaten) als „Geschäftsunterlagen" anzufordern, erwähnt der Sachstand jedoch nicht. Es ist nach hiesiger Ansicht davon auszugehen, dass es insoweit bei der von *Voigt* geschilderten alten Rechtslage geblieben ist. **Section 702 FISA**[18] zur nachrichtendienstlichen Auslandsüberwachung sei **nicht geändert** worden.

Zuletzt wird auf die „Roving Wiretap Clause"[19] und die „Lone Wolf Clause"[20] von FISA eingegangen. Die „Roving Wiretap Clause" regle **akustische Überwachung**. Die „Lone Wolf Clause" erlaube die umfassende **elektronische Überwachung** einer Zielperson, die im Verdacht steht, **terroristische Anschläge** verüben zu können und mit keiner terroristischen Organisation in Verbindung steht. Inhaltsdaten sind mithin erfasst.

> *Wissenschaftliche Dienste des Deutschen Bundestages, USA Freedom Act 2015, Überblick über die Änderungen der nachrichtendienstlichen Befugnisse, WD 3 - 3000 - 144/15 vom 17. Juni 2015.*

Anlage 3

Den Anwendungsbereich und die Bedeutung von Section 702 FISA[21] für die **Tätigkeit der NSA** durch die Ermöglichung des Zugriffs auf eine Schlüsseldatenbank mit Suchbegriffen zur Abfrage von personenbezogenen Daten umreißt *Spies.* Er erwähnt auch die **europäische Kritik** daran wegen Bedenken, US-Behörden würden Datenbanken von EU-Bürgern anlegen.

> *Axel Spies, USA: Repräsentantenhaus verlängert Spionagebefugnisse nach Sec. 702 FISA, in: ZD-Aktuell 2018, 05932.*

Anlage 4

---

17 Bzw. Section 215 Patriot Act; zugleich 50 U.S. Code § 1861.

18 50 U.S. Code §§ 1881, 1881a.

19 Section 105(c)(2)(B) FISA, zugleich Section 206 Patriot Act, zugleich 50 U.S.C. §1805(c)(2)(B).

20 Section 101(b)(1)(C) FISA, geändert durch Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 vom 17. Dezember 2004, Publ. L. No. 108–458, 118 Stat. 3742 (abrufbar unter: https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf, Stand: 31.7.2020); zugleich 50 U.S. Code § 1801 (b)(1)(C).

21 Zugleich 50 U.S. Code §§ 1881, 1881a.

Aktuell ist der Freedom Act im März 2020 außer Kraft getreten, womit ein Rückfall zur alten Rechtslage vor dem Patriot Act eingetreten ist (siehe oben unter 1.). Nach Sections 501, 502 FISA alter Fassung[22] konnte zur Terrorismus- und Spionageabwehr die Herausgabe von Geschäftsunterlagen von nur wenigen bestimmten Adressaten, wie Hotels oder Frachtunternehmen, verlangt werden.[23] Section 702 FISA ist von dem Wegfall des Freedom Act dagegen nicht betroffen.

4. CLOUD Act

Zum CLOUD Act kann vollumfänglich auf die beigefügte Dokumentation der Wissenschaftlichen Dienste des Deutschen Bundestages vom 20. August 2019 verwiesen werden.

> *Wissenschaftliche Dienste des Deutschen Bundestages, Datenübermittlung an US-Ermittlungsbehörden auf Grundlage des CLOUD Acts im Geltungsbereich des EU-Datenschutzrechts, WD 3 - 3000 - 205/19 vom 20. August 2019.*

Anlage 5

Zu **Hintergrund, Inhalt und Folgen** des CLOUD Act sowie möglichen Kollisionen mit Anforderungen der Europäischen Datenschutzgrundverordnung (**DSGVO**)[24], äußern sich *Gausling* sowie *Determann* und *Nebel*.

Der CLOUD Act habe klarstellen sollen, dass **ein dem US-Recht unterfallendes Unternehmen** einem Herausgabeverlangen bezüglich **elektronischer Beweismittel in Strafverfahren** nachkommen müsse, gleich wo sich die Daten befänden. Das Gesetz sei in Reaktion auf ein gegenteiliges Urteil des Berufungsgerichts im Fall *Microsoft Corp. v. United States* entstanden. Ein Beschlagnahmebeschluss kann sich folglich auf jegliche Daten – gegebenenfalls auch Finanzdaten – beziehen, die Beweismittel in einem Strafverfahren sind.

Der übliche Weg eines **Rechtshilfeersuchens** auf Basis von Rechtshilfeabkommen sei aus US-Sicht nach dem CLOUD Act nicht mehr erforderlich. Bei Rechtshilfeersuchen liege die Entscheidung über die Verpflichtung zur Herausgabe von Beweismitteln dagegen im Ermessen der jeweilig zuständigen ausländischen Behörde.

Gausling sowie *Determann* und *Nebel* beleuchten zudem die Bedeutung von **Verwaltungsabkommen** nach dem CLOUD Act. Diese hätten in zweierlei Hinsicht Bedeutung: Der **Widerspruch** des Adressaten zu einem Herausgabeverlangen aufgrund von ECPA bzw. CLOUD Act werde gericht-

---

22 In der durch Section 602 Intelligence Authorization Act for Fiscal Year 1999 geänderten Fassung, vgl. Intelligence Authorization Act for Fiscal Year 1999, Publ. L. No. 105–272, 112 Stat. 2396 (abrufbar unter: https://www.congress.gov/105/plaws/publ272/PLAW-105publ272.pdf. Stand: 31.7.2020).

23 Vgl. auch Spies, Europa: Wer hat Angst vor dem US-Patriot Act?, ZD-Aktuell 2012, 03062.

24 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. L 119 vom 4. Mai 2016, S. 1.

lich **nur berücksichtigt, wenn ein solches Verwaltungsabkommen vorläge**. Eine Berufung auf gegenteilige Pflichten nach der **DSGVO**, Daten nicht herauszugeben, setze demnach aus US-Sicht ein Verwaltungsabkommen voraus.

Zweitens sollten die Verwaltungsabkommen im Gegenzug den ausländischen Behörden des jeweiligen Staates die Möglichkeit geben, US-Unternehmen ebenfalls unmittelbar selbst zur Herausgabe von Daten als Beweismittel zu verpflichten. In beide Richtungen werde also der bis dato erforderliche Umweg über Rechtshilfeersuchen abgeschafft und stattdessen ein **Direktzugriff** von Behörden auf Daten eröffnet.

Lothar Determann/Michaela Nebel, U.S. CLOUD Act – Wolken über der Datenschutz- Grundverordnung? Neuigkeiten im Konflikt zwischen US-Recht und EU-Datenschutzrecht, in: CR 2018, S. 408.

Anlage 6

Tina Gausling, Offenlegung von Daten auf Basis des CLOUD Act. CLOUD Act und DS-GVO im Spannungsverhältnis, in: MMR 2018, S. 578.

Anlage 7

Rath und *Spies* verweisen auf das Modell einer **Datentreuhand**, welches möglicherweise den Zugriff von US-Behörden auf in Europa gespeicherte Daten ausschließen könne.

Michael Rath/Axel Spies, CLOUD Act: Selbst für die Wolken gibt es Grenzen, in: CCZ 2018, S. 229.

Anlage 8

Neue Entwicklungen bestehen vor allem im Bereich der **Verwaltungsabkommen**. Das Vereinigte Königreich und die USA haben das erste derartige Verwaltungsabkommen am 3. Oktober 2019 abgeschlossen.[25] Die Vorsitzende des **Europäischen Datenschutzausschusses** (**EDPB**) *Jelinek* meldet in einem Brief an die Mitglieder des Europäischen Parlaments aufgrund einer vorläufigen Analyse **Zweifel** an, ob dieses Abkommen mit **EU-Datenschutzrecht** zu vereinbaren ist. Der EDPB wünsche sich eine klarere Regelung der gerichtlichen Überprüfung der Datenerhebung in einem vergleichbaren Abkommen der EU mit den USA.

25 Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime vom 3. Oktober 2019 (abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf, Stand: 31.7.2020).

Andrea Jelinek, Brief an die Mitglieder des Europäischen Parlaments, 15. Juni 2020 (verfügbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf, Stand: 31.7.2020).

Anlage 9

Für ein **Abkommen zwischen der EU und den USA** wurden mittlerweile Verhandlungen aufgenommen.[26] Die *Bundesregierung* äußert sich in der BT-Drs. 19/15374 vom 22. November 2019 zum Status der Verhandlungen und zu der Bedeutung eines EU-US-Abkommens im Bereich „E-Evidence". Sie begrüßt das geplante Abkommen als sinnvolle Ergänzung des neuen europäischen Rechtsrahmens zu „E-Evidence" (der geplanten **Verordnung für elektronische Beweismittel in Strafsachen**[27] und einer ergänzenden Richtlinie[28]).

Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE, Verhandlungen der EU-Kommission zum Austausch elektronischer Beweismittel mit dem US-Justizministerium, 22. November 2019, BT-Drs. 19/15374.

Anlage 10

Bereits früher nahm die *Bundesregierung* in der BT-Drs. 19/5207 vom 22. Oktober 2018 zu dem **geplanten EU-US-Abkommen** Stellung. Sie stelle sich nicht gegen solche Verhandlungen, weil zu erwarten sei, dass sich damit eine „conflict of laws"-Situation vielfach vermeiden ließe. Dies liege auch im Interesse deutscher Strafverfolgungsbehörden.

Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Christine Aschenberg-Dugnus, Jens Beeck, weiterer Abgeordneter und der Fraktion der FDP, 22. Oktober 2018, BT-Drs. 19/4736.

Anlage 11

* * *

---

26 Europäische Kommission, Strafjustiz: Gemeinsame Erklärung zum Start der Verhandlungen zwischen der EU und den USA über die Erleichterung des Zugangs zu elektronischen Beweismitteln vom 26. September 2019 (abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_19_5890, Stand: 31.7.2020).

27 Vorschlag vom 17. April 2018 für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM/2018/225 final - 2018/0108 (COD) (abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52018PC0225, Stand: 31.7.2020).

28 Vorschlag vom 17. April 2018 für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, COM/2018/226 final - 2018/0107 (COD) (abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN, Stand: 31.7.2020).