



75 Jahre
Demokratie
lebendig



Deutscher Bundestag
Wissenschaftliche Dienste

Dokumentation

Zu grundrechtlichen Schutzpflichten gegen Datenübermittlungen an US-amerikanische Sicherheitsbehörden

Zu grundrechtlichen Schutzpflichten gegen Datenübermittlungen an US-amerikanische Sicherheitsbehörden

Aktenzeichen: WD 3 - 3000 - 026/24
Abschluss der Arbeit: 28.03.2024 (zugleich letzter Abruf der Internetseiten)
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Arbeiten der Wissenschaftlichen Dienste des Deutschen Bundestages	4
3.	Grundrechtlichen Schutzpflichten und mittelbare Drittwirkung von Grundrechten	5
3.1.	Rechtsprechung und rechtswissenschaftliche Literatur	6
3.2.	Grundrechtliche Schutzpflichten zugunsten von Abgeordneten?	9
3.3.	Schutzpflichten aus Art. 38 Abs. 1 Satz 2 GG?	9

1. Einleitung

Die vorliegende Dokumentation beschäftigt sich mit der Frage, ob der Staat verpflichtet ist, deutsche Staatsbürger, insbesondere Abgeordnete des Deutschen Bundestages, davor zu schützen, dass Unternehmen aufgrund von Herausgabeverpflichtungen durch US-amerikanische Sicherheitsbehörden personenbezogene Daten übermitteln.

In Bezug auf Abgeordnete ist fraglich, ob sich eine staatliche Schutzpflicht aus dem freien Mandat nach Art. 38 Abs. 1 Satz 2 des Grundgesetzes (GG)¹ ergeben könnte. Soweit ersichtlich, wurde diese konkrete Fragestellung in der Rechtsprechung noch nicht entschieden und auch im Übrigen in der rechtswissenschaftlichen Literatur nicht näher diskutiert. Allerdings wurden jedenfalls in der rechtswissenschaftlichen Literatur bereits im Allgemeinen staatliche Schutzpflichten diskutiert, die vor Eingriffen in das Recht auf informationelle Selbstbestimmung und in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) schützen sollen.

Zur Übersicht werden nachfolgend zuerst die bisherigen Arbeiten der Wissenschaftlichen Dienste zum Zugriff US-amerikanischer Sicherheitsbehörden auf Daten zusammengefasst (dazu unter 2.). Anschließend wird einschlägige Rechtsprechung und rechtswissenschaftliche Literatur zum Themenbereich möglicher staatlicher Schutzpflichten allgemein vor Eingriffen in Systeme der Informations- und Kommunikationstechnik und damit im Zusammenhang stehende Datenübermittlungen zusammengefasst (dazu unter 3.1.). Anschließend wird erörtert, ob sich die Abgeordneten auf die grundrechtlichen Schutzpflichten berufen können, und es wird der Schutzgehalt des freien Mandats von Abgeordneten gemäß Art. 38 Abs. 1 Satz 2 GG, insbesondere mit Blick auf den Schutz von Kommunikationsbeziehungen, cursorisch dargestellt (dazu unter 3.2.).

2. Arbeiten der Wissenschaftlichen Dienste des Deutschen Bundestages

Die folgenden Arbeiten der Wissenschaftlichen Dienste des Deutschen Bundestages erläutern näher, unter welchen Voraussetzungen US-amerikanische Sicherheitsbehörden die Herausgabe von Daten gegenüber US-amerikanischen Unternehmen und ihren europäischen Tochterfirmen fordern können. Insoweit gibt zunächst die Dokumentation

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

einen Überblick über die Diskussion der rechtswissenschaftlichen Literatur und von staatlichen Stellen über mögliche Kollisionen des im Mai 2018 vom US-Kongress erlassenen Clarifying Lawful Overseas Use of Data Act (sog. CLOUD Act)² mit europäischem Datenschutzrecht.

1 [Grundgesetz für die Bundesrepublik Deutschland](#) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert am 19.12.2022 (BGBl. I S. 2478).

2 Consolidated Appropriations Act (Division V–CLOUD ACT) [Pub. L. No. 115-141 Stat. 2383](#) vom 23.03.2018.

Die Dokumentation

Wissenschaftliche Dienste des Deutschen Bundestages, US-Datenrecht - Zugriff US-amerikanischer Behörden auf Daten, [WD 3 - 3000 - 181/20](#), vom 3. August 2020

fasst darüber hinaus die weiteren US-amerikanischen Rechtsgrundlagen zusammen, die den Zugriff durch US-amerikanische Sicherheitsbehörden auf Daten regeln.

Weiterhin befasst sich der Sachstand

Wissenschaftliche Dienste des Deutschen Bundestages, Herausgabepflichten von Daten und Informationen an US-amerikanische Sicherheitsbehörden, [WD 3 - 3000 - 105/23](#), vom 19. Januar 2024

ausführlich mit den wesentlichen Vorschriften des US-amerikanischen Rechts, nach denen Anbieter von Vermittlungsdiensten grundsätzlich verpflichtet werden können, Daten und Informationen auch von deutschen Kunden oder Vertragspartnern an US-amerikanische Sicherheitsbehörden herauszugeben. Unter Berücksichtigung des Umstands, dass Anbieter von Cloud-Diensten Adressaten dieser Herausgabepflichtung von US-amerikanischen Sicherheitsbehörden sein könnten, wird ferner allgemein die Gewährleistung der Datensicherheit durch staatliche Stellen betrachtet sowie die datenschutzrechtliche Zulässigkeit der Nutzung von Cloud-Diensten durch deutsche Behörden erörtert.

Im Kontext der Gewährleistung der Datensicherheit werden vor allem der aktuelle Stand der Diskussion zur sog. digitalen Souveränität der Verwaltung und die damit zusammenhängenden Pflichten des Staates dargestellt. Dies betrifft unter anderem die Problematik des IT-Outsourcing, also die Nutzung von privaten Anbietern für Informations- und Kommunikationsdienste im Bereich der hoheitlichen Aufgabenerfüllung. In der Arbeit wird in diesem Zusammenhang die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2010 zur Vorratsdatenspeicherung erörtert und damit einhergehende mögliche, aber nicht zwingende Einbußen an der Datensicherheit, wenn die Daten bei privaten Anbietern gespeichert werden. Im Ergebnis kann nach der Rechtsprechung des Bundesverfassungsgerichts IT-Outsourcing nicht pauschal ausgeschlossen werden, sondern muss für jede Informations- und Kommunikationstechnologie im Einzelfall unter Berücksichtigung der „Art der betroffenen Daten und [der] Art der hoheitlichen Aufgabe, für die die Daten verarbeitet bzw. die IT-Dienstleistung genutzt werden soll“, abgewogen werden.

3. Grundrechtliche Schutzpflichten und mittelbare Drittwirkung von Grundrechten

Das Bundesverfassungsgericht erkennt in ständiger Rechtsprechung an, dass Grundrechte neben der klassischen Abwehrfunktion grundsätzlich auch grundrechtliche Schutzpflichten für den Staat begründen können.³ Diese stehen außerdem im Zusammenhang mit der sog. mittelbaren Drittwirkung, wonach Grundrechte unter bestimmten Voraussetzungen auch eine Ausstrahlungswirkung auf privatrechtliche Verhältnisse haben. Allgemeine Ausführungen zu der mittelbaren

³ Vgl. dazu in Bezug auf den Schutz des Lebens und der körperlichen Unversehrtheit nach Art. 2 Abs. 2 Satz 1 GG, BVerfGE 39, 1 (42); 46, 160 (164); 56, 54 (73); 115, 118 (152).

Drittwirkung von Grundrechten sowie zu grundrechtlichen Schutzpflichten finden sich in dem Sachstand

Wissenschaftliche Dienste des Deutschen Bundestages, Drittwirkung von Grundrechten, [WD 3 - 3000 - 123/23](#), vom 9. November 2023.

Herausgabeverpflichtungen von US-amerikanischen Sicherheitsbehörden gegenüber privaten Unternehmen, personenbezogene Daten herauszugeben, berühren grundsätzlich das Recht auf informationelle Selbstbestimmung der Betroffenen nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.⁴ Sowohl zur mittelbaren Drittwirkung von Grundrechten als auch zu staatlichen Schutzpflichten im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG finden sich weitere Ausführungen in der Dokumentation

Wissenschaftliche Dienste des Deutschen Bundestages, Drittwirkung von Grundrechten – Gewährleistung des Rechts auf informationelle Selbstbestimmung bei ungleicher Machtverteilung zwischen den Vertragspartnern im Privatrecht, [WD - 3000 - 223/20](#), vom 5. Oktober 2020.

3.1. Rechtsprechung und rechtswissenschaftliche Literatur

Dass sich auch aus dem Recht auf informationelle Selbstbestimmung grundsätzlich eine grundrechtliche Schutzpflicht für den Staat ergeben könne, erläutert

Richter des Bundesverfassungsgerichts Prof. Dr. Peter M. Huber, Abweichende Meinung zum Beschluss des Bundesverfassungsgerichts vom 21. Juni 2016 - [2 BvR 637/09](#), Rn. 23 ff., BVerfGE 142, 234 (265 ff.).

Huber beschreibt in seinen Ausführungen des Weiteren die Rechtsprechungslinie des Bundesverfassungsgerichts, nach der grundrechtliche Schutzpflichten nicht nur bei der Bedrohung von Rechtspositionen deutscher Staatsbürger im Ausland greifen, sondern auch Maßnahmen einer fremden Hoheitsgewalt umfassen können, die gegenüber Einwohnern Deutschlands Wirkung entfalten. Demnach müssen die Verfassungsorgane grundsätzlich solchen Übergriffen, wenngleich nur im Rahmen des Möglichen, entgegentreten.

Auch in der rechtswissenschaftlichen Literatur wird die Bedeutung von grundrechtlichen Schutzpflichten des Staates vor allem im Zusammenhang mit dem ebenfalls aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgenden IT-Grundrecht diskutiert.⁵ Insgesamt werden insoweit überwiegend Schutzpflichten angenommen, allerdings ohne dass sich aus ihnen konkrete Handlungsvorgaben für den Staat ergeben sollen. So befasst sich

⁴ Zum Recht auf informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts vgl. BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, Ls. 1 und 2, BVerfGE 65, 1.

⁵ Zum IT-Grundrecht als Konkretisierung des allgemeinen Persönlichkeitsrechts vgl. BVerfG, Beschluss vom 30.04.2008 - [1 BvR 370/07](#), 1 BvR 595/07, Ls. 1, BVerfGE 120, 274.

Hoffmann-Riem, Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, JZ 2008, 1009 - 1022,

- Anlage 1 -

ausführlich mit dem Urteil des Bundesverfassungsgerichts zum IT-Grundrecht. Das Bundesverfassungsgericht habe mit der Entwicklung dieses Grundrechts auf moderne Gefahren der Informationstechnologien reagiert. Der Staat müsse seinen „IT-Schutzpflichten“ umso stärker nachkommen,

je mehr die realen Voraussetzungen der Freiheitsausübung der Bürger einerseits durch den Staat, andererseits aber auch durch Private oder im Zuge von Kooperationsakten zwischen Staat und Privaten geschaffen und erhalten werden [...].

Ferner setzt sich

Heckmann, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit in: Rüßmann, Festschrift für Käfer, 2009, S. 129 - 164,

- Anlage 2 -

mit der Frage der Ableitung einer staatlichen Schutzpflicht aus dem vom Bundesverfassungsgericht entwickelten IT-Grundrecht sowie dem Umfang einer etwaigen grundrechtlichen Schutzpflicht ausführlicher auseinander. Der Schutz- und Gewährleistungsauftrag des Staates ziele *Heckmann* zufolge auf die Bekämpfung und Vermeidung nichtstaatlicher Eingriffe ab. Das IT-Grundrecht schließe Schutzlücken, die die bisherigen grundrechtlichen Gewährleistungen nicht schließen könnten. Es eröffne seinen Schutzbereich in Bezug auf die Gewährleistung der IT-Sicherheit der grundrechtsberechtigten Bürger, nicht jedoch bezüglich der Gewährleistung der IT-Sicherheit des grundrechtsverpflichteten Staates.

Schliesky/Hoffmann/Luch/Schuls/Borchers, Schutzpflichten und Drittwirkung im Internet – das Grundgesetz im digitalen Zeitalter, 2014, S. 66 - 71,

- Anlage 3 -

zufolge seien Sachverhalte in einer digitalen Welt selten auf das territoriale Hoheitsgebiet eines Staates begrenzt. Die Autoren gehen insbesondere auf die Problematik ein, dass die mittelbare Drittwirkung nicht ohne Weiteres auf Sachverhalte mit Auslandsbezug angewendet werden könne. Dies gelte insbesondere mit Blick auf Privatunternehmen in der IT-Branche, die ihren Sitz in den USA haben. Die Grundvoraussetzungen für die Anwendung deutscher Grundrechte in privatrechtlichen Sachverhalten mit Auslandsbezug sei die Anwendbarkeit des deutschen Privatrechts auf den jeweiligen Sachverhalt. Zu beachten sei außerdem, dass das vom deutschen Staat zu gewährleistende Schutzniveau bei diesen Sachverhalten mit Auslandsbezug niedriger angesetzt werden müsse, was vor allem mit Blick auf den völkerrechtlichen Grundsatz der Territorialität der Staatsgewalt konsequent sei. In denjenigen Konstellationen, in denen Einzelne mit privaten Dritten Verträge schließen, bei denen kein deutsches Recht Anwendung finde, bestünde den Autoren zufolge die Möglichkeit, dass sie sich nicht auf das vom Grundgesetz gewährleistete Schutzniveau berufen können.

Neubert, Grundrechtliche Schutzpflicht des Staates gegen grundrechtsbeeinträchtigende Maßnahmen fremder Staaten am Beispiel der Überwachung durch ausländische Geheimdienste, AöR 140 (2015), 267 - 304,

- Anlage 4 -

zufolge sind bei einer Ausspähung und Abschöpfung von Daten durch ausländische Geheimdienste das Fernmeldegeheimnis, normiert in Art. 10 Abs. 1 GG, das Recht auf informationelle Selbstbestimmung und das sog. IT-Grundrecht, die Konkretisierungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, mögliche beeinträchtigte Grundrechte. Überwachungsmaßnahmen der ausländischen Geheimdienste oder privater Dritter stellen Eingriffe in die oben genannten Grundrechte dar, sodass eine schutzpflichtauslösende Gefährdungslage gegeben sein könne. Die deutsche Staatsgewalt habe insoweit wirksamen Schutz zu gewährleisten. *Neubert* führt aber auch aus, dass die grundrechtlichen Schutzpflichten keine totale Sicherheit garantieren könnten. Es sei ihm zufolge ausreichend, dass der Staat geeignete Maßnahmen ergreife, um die Gefährdung der Grundrechte zumindest „auf ein vertretbares Maß einzudämmen“.

Roßnagel, Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit, in: Fehling/Schliesky, Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 2016, S. 73 – 95,

- Anlage 5 -

vertritt ebenfalls, dass die Ausspähung von Kommunikationsvorgängen durch eigene als auch ausländische Geheimdienste Grundrechte verletzen oder gefährden könne. Dies gelte vor allem aufgrund einer etwaigen Pflicht der Internetdiensteanbieter, mit den Geheimdiensten zusammenarbeiten zu müssen. Der Staat habe *Roßnagel* zufolge auch in diesem Zusammenhang eine Schutzpflicht gegenüber Angriffen auf Grundrechte durch andere Staaten. *Roßnagel* ist daher der Auffassung, dass der Staat seinen Bürgern technische Schutzmöglichkeiten gegenüber ausländischen Geheimdiensten bieten müsse. In Bezug auf die Ausspähung durch Internetanbieter müsse der Staat seinen Bürgern „Schutz vor unfairen Allgemeinen Geschäftsbedingungen bieten“.

Zuletzt befasst sich auch

Papier, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, NJW 2017, 3025 (3026, 3029 f.),

- Anlage 6 -

mit Gefährdungen der Grundrechte in der heutigen globalen und digitalen Gesellschaft unter anderem durch fremde Staaten, aber auch durch global agierende, ausländische Privatunternehmen. Aus den staatlichen Schutzpflichten würden sich *Papier* zufolge keine unmittelbaren Handlungsansprüche ergeben. Dennoch müsse der Staat Schutzkonzepte aufstellen und diese normativ ausgestalten, um seinen grundrechtlichen Schutzpflichten zu genügen. Dabei habe der Gesetzgeber einen Ausgleich zwischen Freiheitsrechten und Privatautonomie herzustellen.

3.2. Grundrechtliche Schutzpflichten zugunsten von Abgeordneten?

Auch die diskutierten grundrechtlichen Schutzpflichten aus dem Recht auf informationelle Selbstbestimmung oder aus dem IT-Grundrecht dürften für Abgeordnete nur gelten, soweit sie sich als Privatperson auf diese berufen. Denn in der Rechtsprechung des Bundesverfassungsgerichts und der rechtswissenschaftlichen Literatur wird überwiegend vertreten, dass Abgeordnete sich im Rahmen ihrer Mandatstätigkeit nicht auf Grundrechte berufen können.⁶ Die Abgeordnetenrechte gemäß Art. 38 Abs. 1 Satz 2 GG schützen demnach nur die Mandatstätigkeit. Als Privatperson kann sich ein Abgeordneter hingegen selbstverständlich auf seine Grundrechte berufen und deren Verletzung gegebenenfalls im Rahmen einer Verfassungsbeschwerde geltend machen.⁷

3.3. Schutzpflichten aus Art. 38 Abs. 1 Satz 2 GG?

Aus Art. 38 Abs. 1 Satz 2 GG wurden letztlich, soweit ersichtlich, in der Rechtsprechung und in der rechtswissenschaftlichen Literatur bisher noch keine Schutzpflichten des Staates entnommen, weder allgemein noch speziell in Bezug auf die Nutzung von IT-Systemen und Datensicherheit.⁸

Zwar bezieht sich die Entscheidung des Bundesverfassungsgerichts

Bundesverfassungsgericht, Beschluss vom 17. September 2013 - [2 BvR 2436/10](#), BVerfGE 134, 141,

unmittelbar auf einen Eingriff in das freie Mandat durch Beobachtungen von deutschen Behörden des Verfassungsschutzes und nicht auf Datenübermittlungen von privaten Unternehmen an US-amerikanische Sicherheitsbehörden. Das Bundesverfassungsgericht führt allerdings allgemein zum Schutzgehalt des Art. 38 Abs. 1 Satz 2 GG aus, dass die Kommunikationsbeziehungen des Abgeordneten als Bedingung seiner freien Willensbildung zu schützen seien. Es müsse ferner gewährleistet werden, dass „die von ihm zu vertretenden, in die politische Willensbildung des Deutschen Bundestages einzuspeisenden Meinungen und Interessen ihn unverzerrt und ohne staatliche Beeinflussung erreichen können“. Der Gewährleistungsgehalt des Art. 38 Abs. 1 Satz 2 GG beziehe sich auf das gesamte politische Handeln des Abgeordneten und umfasse nicht nur dessen Tätigkeit im parlamentarischen Bereich, weil sich die Sphären des Abgeordneten als Mandatsträger, als Parteimitglied sowie als politisch handelnder Privatperson nicht strikt trennen ließen. Außerdem stelle dem Bundesverfassungsgericht zufolge

6 Vgl. dazu Morlok, in: Dreier, GG Bd. 2, 3. Aufl. 2015, Art. 38 Rn. 146 m.w.N.; Magiera, in: Sachs, GG, 9. Aufl. 2021, Art. 38 Rn. 52 m.w.N. A.A. in der Dissertation, Basakoglu, Die Beobachtung von Abgeordneten durch den Verfassungsschutz - Eine Untersuchung hinsichtlich der Verfassungsmäßigkeit unter Einbeziehung europarechtlicher Aspekte, 2017, S. 22.

7 Ausführlich dazu Klein/Schwarz, in: Dürig/Herzog/Scholz, GG, 102. EL August 2023, Art. 38 Rn. 266.

8 Zur Gewährleistung ihrer Unabhängigkeit sind indes die Indemnität und die Immunität nach Art. 46 GG, das Zeugnisverweigerungsrecht nach Art. 47 GG, der Anspruch auf angemessene Entschädigung nach Art. 48 Abs. 3 GG als verfassungsrechtliche „Schutzrechte“ der Abgeordneten anerkannt, vgl. dazu Magiera, in: Sachs, GG, 9. Aufl. 2021, Art. 38 Rn. 71.

[d]as freie Mandat [...] auch insoweit eine Vorkehrung zum Schutz der Integrität des Zustandekommens und der Willens- und Entscheidungsbildung der staatlichen Organe dar [...]. Durch eine Behinderung der parlamentarischen Arbeit des einzelnen Abgeordneten werden die vom Volke festgelegten Mehrheitsverhältnisse verändert [...]. Wird die Kommunikationsbeziehung zwischen Abgeordnetem und Bürgern gestört, so ist folglich die parlamentarische Willensbildung und infolgedessen die demokratische Repräsentationsfunktion des Parlaments berührt.⁹

Positive Schutzpflichten aus Art. 38 Abs. 1 Satz 2 GG statuiert das Bundesverfassungsgericht gleichwohl nicht.

* * *

9 BVerfG, Beschluss vom 17.09.2013 - 2 BvR 2436/10, Rn. 99, BVerfGE 134, 141.