

**05.02.20****Antrag**  
**der Länder Hamburg, Bremen**

---

**Entschließung des Bundesrates: „Effektivierung von Auskunftserteilungen durch ausländische Anbieter sozialer Netzwerke“**

Der Präsident des Senats  
der Freien und Hansestadt Hamburg

Hamburg, 4. Februar 2020

An den  
Präsidenten des Bundesrates  
Herrn Ministerpräsidenten  
Dietmar Woidke

Sehr geehrter Herr Präsident,

die Landesregierungen von Hamburg und Bremen haben beschlossen, dem Bundesrat die als Anlage mit Begründung beigefügte

**Entschließung des Bundesrates:**  
**„Effektivierung von Auskunftserteilungen durch**  
**ausländische Anbieter sozialer Netzwerke“**

zuzuleiten.

Ich bitte Sie, die Vorlage gemäß § 36 Absatz 2 der Geschäftsordnung des Bundesrates auf die Tagesordnung der 985. Sitzung des Bundesrates am 14. Februar 2020 zu setzen und sie anschließend den zuständigen Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen

Dr. Peter Tschentscher



## **Entschließung des Bundesrates: „Effektivierung von Auskunftserteilungen durch ausländische Anbieter sozialer Netzwerke“**

Der Bundesrat möge folgende Entschließung fassen:

Der Bundesrat bittet die Bundesregierung,

- auf nationaler Ebene durch eine Statuierung des Marktortprinzips dafür Sorge zu tragen, dass die jeweiligen Anbieter von Telemediendiensten sich bei der Erfüllung von Auskunftspflichten gegenüber den Strafverfolgungsbehörden nicht mehr darauf berufen können, dass die abgefragten Daten im Ausland gespeichert sind, da sie ihre Leistungen in Deutschland anbieten, und
- sich auf europäischer Ebene weiterhin für eine schnelle und zugleich grundrechts- und datenschutzsichernde Umsetzung der angedachten Maßnahmen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in Strafsachen einzusetzen und dabei darauf hinzuwirken, dass den Herausforderungen bei der Bekämpfung der Hasskriminalität im Internet im besonderen Maße Rechnung getragen wird.

### Begründung:

Die Bekämpfung der Hasskriminalität oder von anderen strafbaren Inhalten in den sozialen Netzwerken stellt die Strafverfolgungsbehörden vor eine große Herausforderung. Der in den sozialen Netzwerken geführte Diskurs hat sich stark verändert. Diese Netzwerke wachsen stetig und bilden eine zentrale Plattform für eine Vielzahl unterschiedlicher Gruppen und Menschen, die miteinander in Kontakt treten. Die Debatten und Kommentare werden dabei mehr und mehr aggressiv, verletzend, häufig hasserfüllt und oftmals außerhalb der Grenzen des durch Artikel 5 des Grundgesetzes geschützten Rechts auf freie Meinungsäußerung geführt. Straftaten wie Beleidigung, Verleumdung, Volksverhetzung, Bedrohung oder auch die öffentliche Verwendung von Kennzeichen verfassungswidriger Organisationen stehen an der Tagesordnung. Dabei können Täter mit einfachen Mitteln innerhalb kürzester Zeit eine Vielzahl von Personen erreichen. Dies hat neben einer Vergiftung des Diskurses im Internet auch Auswirkungen auf die politische Debatte und das gesellschaftliche Klima insgesamt, wodurch der Nährboden für Gewalttaten auch in der „analogen Welt“ gelegt wird.

Um dieses Phänomens Einhalt zu gebieten, bedarf es unter anderem einer konsequenten strafrechtlichen Verfolgung der Täter. Dies setzt voraus, dass die Strafverfolgungsbehörden die Urheber von strafrechtlich relevanten Nachrichten und Kommentaren ermitteln können.

Sofern die Täter bei der Veröffentlichung ihrer Hassnachrichten nicht unter ihrem Klarnamen, sondern unter einem Pseudonym auftreten, sind die Ermittlerinnen und Ermittler zumeist auf Auskünfte der jeweiligen Anbieter sozialer Medien angewiesen. So kann etwa die Übermittlung von Registrierungs- bzw. Bestandsdaten einen wichtigen und zusammen mit der zugeordneten IP-Adresse oftmals einzigen Ansatz für weitere Ermittlungen bieten.

Die Bundesregierung beabsichtigt, als Teil des Maßnahmenpakets zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, die gegenüber Erbringern von Telekommunikationsdiensten bestehenden strafprozessualen Befugnisse zur Datenerhebung auch auf Anbieter von Telemediendiensten zu erstrecken. Im Rahmen des anstehenden Gesetzgebungsverfahrens wird zu prüfen sein, ob diese Gleichstellung verfassungsrechtlich zulässig ist. Zudem bedarf es einer intensiven Prüfung, ob das Vorhaben geeignet und erforderlich ist, das mit dem Gesetz verfolgte Ziel zu erreichen. Unabhängig davon kann eine Verbesserung der jetzigen Situation nur durch legislative Maßnahmen erreicht werden, die sicherstellen, dass der Speicherort der abgefragten Daten für die Erfüllung etwaiger Auskunftspflichten unerheblich ist. Denn die größten und relevanten Internetdienstleister haben ihren Sitz im Ausland, insbesondere in den Vereinigten Staaten von Amerika. Oftmals werden die Strafverfolgungsbehörden bei jetzigen Auskunftsverlangen mit dem Hinweis, dass die angeforderten Daten auf Servern im jeweiligen Land des Geschäftssitzes gespeichert werden, auf den Rechtshilfeweg über die dort zuständigen Justizbehörden verwiesen. Entsprechende Ersuchen werden dann jedoch – wenn überhaupt – erst nach mehreren Monaten beantwortet.

Diese Problematik besteht nicht nur in Deutschland, sondern in der gesamten Europäischen Union.

Im Frühjahr 2018 hat die Europäische Kommission zwei Rechtsinstrumente zu elektronischen Beweismitteln („e-evidence“) vorgestellt. Kern der Initiative ist der Vorschlag einer Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, die durch eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren ergänzt werden soll. Die genannte Verordnung soll es den Behörden ermöglichen, Zugang zu gespeicherten digitalen Beweismitteln von Dienstleistern zu erhalten, ohne dass es auf den Ort der Speicherung ankommt. Mit der geplanten Herausgabeordnung könnten die Strafverfolgungsbehörden im grenzüberschreitenden Verkehr einen Anbieter von Online-Diensten in einem anderen Mitgliedstaat um direkten Zugang zu elektronischen Beweismitteln ersuchen. Die Anordnungen sollen alle Datenkategorien, also auch Teilnehmer- bzw. Bestandsdaten betreffen. Ergänzend hierzu soll die genannte Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern alle Anbieter, die ihre Dienste in der EU erbringen, dazu verpflichten, einen Vertreter in der EU zu bestellen. Letzterer soll für die Entgegennahme und Befolgung der Beschlüsse und Anordnungen zuständig sein.

Die Justizministerinnen und Justizminister der Länder haben sich bereits im Rahmen ihrer Frühjahrskonferenz 2018 auf Initiative der Freien und Hansestadt Hamburg und des Landes Rheinland-Pfalz mit diesen Vorschlägen der Europäischen Kommission befasst (TOP II.2). Sie haben die Bundesregierung gebeten, sich auch weiterhin intensiv für eine Lösung auf europäischer Ebene einzusetzen. Sie haben sich außerdem dafür ausgesprochen, den Anknüpfungspunkt nach dem Markortprinzip zu bestimmen und nicht nach dem Ort, an dem der jeweilige Dienstleister seinen Sitz hat oder an dem er die Daten speichert. Die Bundesregierung wurde darüber hinaus gebeten, sich bei den weiteren Beratungen und bei der Vorbereitung der Verhandlungen der Kommission mit Drittstaaten über Abkommen im Zusammenhang mit der grenzüberschreitenden Sicherung von elektronischen Beweismitteln für die Wahrung des geltenden Grundrechts- und Datenschutzniveaus einzusetzen.

Auch die von der Konferenz der Justizministerinnen und Justizminister bzw. von dessen Strafrechtausschuss eingesetzte Arbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht“ hat sich im Hinblick auf ausländische Internetdienste für die Einführung des Marktortprinzips stark gemacht.

Ferner ist auf die Bestrebungen über den Abschluss eines Abkommen zwischen der Europäischen Union und den Vereinigten Staaten hinzuweisen, das den direkten und schnellen Zugang zu elektronischen Beweismitteln bei grenzüberschreitenden strafrechtlichen Ermittlungen erleichtern und die genannten europäischen Legislativvorschläge flankieren soll. Die Vereinigten Staaten stützen dabei ihr Verhandlungsmandat auf das Gesetz zur Regelung der rechtmäßigen Verwendung von Daten im Ausland – „Clarifying Lawful Overseas Use of Data (CLOUD) Act“ – aus März 2018.

Vergleichbare Verhandlungen werden auf der Ebene des Europarates zum Abschluss eines zweiten Zusatzprotokolls zum Budapester Übereinkommen über Computerkriminalität geführt. Darin sollen Bestimmungen über eine effektivere und vereinfachte Rechtshilfe festgelegt werden, so dass künftig eine direkte Zusammenarbeit mit Diensteanbietern in anderen Vertragsstaaten des Übereinkommens und grenzüberschreitende Abfragen möglich wären.

Auf internationaler Ebene setzt sich demnach die Erkenntnis durch, dass es im digitalen Zeitalter nicht allein auf den Speicherort volatiler Daten im Rahmen strafrechtlicher Ermittlungen nicht ankommen darf. Der nationale Gesetzgeber ist dabei gehalten, diese Entwicklungen nicht nur durch die Teilnahme an den oder die Einflussnahme auf die jeweiligen Verhandlungen zu begleiten, sondern aktuellen gesetzgeberischen Handlungsbedarf wie bei der Bekämpfung der Hasskriminalität im Internet intensiv zu prüfen und erforderlichenfalls zügig und konsequent zu handeln.

Die Umsetzung bzw. das Inkrafttreten der Rechtsinstrumente der Europäischen Kommission oder eines Abkommens mit den Vereinigten Staaten sind nicht zeitnah zu erwarten. Zudem wird die Verordnung über Europäische Herausgabe- und Sicherungsanordnungen nicht für rein innerstaatliche Fälle gelten, in denen die ausländischen Anbieter von sozialen Netzwerken einen Vertreter in Deutschland benennen (vgl. Erwägungsgrund 15 des Verordnungsentwurfs). So sieht § 1 Absatz 2 Satz 2 des Verordnungsentwurfs explizit vor, dass die Verordnung nicht die Befugnisse der nationalen Behörden berührt, Diensteanbieter, die in dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zur Einhaltung ähnlicher nationaler Maßnahmen zu verpflichten.

Aufgabe der Bundesregierung ist es daher bereits jetzt, auch auf nationaler Ebene – unter Wahrung des geltenden Grundrechts- und Datenschutzniveaus – ein mit dem beabsichtigten europäischen Regelungsmodell vergleichbares System zu etablieren, in dem die Erfüllung etwaiger Auskunftspflichten der Anbieter von sozialen Netzwerken und von anderen Telemediendiensten nicht vom Speicherort der von den Strafverfolgungsbehörden abgefragten Daten abhängt, sondern vom Marktort der Diensteanbieter.